**T.C.**

**EGE ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

****

**KABLOLU, KABLOSUZ AĞLARDA GÜVENLİK VE GÜNÜMÜZDEKİ TEHDİTLER**

**LİSANS TEZİ**

**HAZIRLAYANLAR**

**Ufuk Atakan YÜKSEL**

**DANIŞMAN**

**Prof. Dr. Levent TOKER**

İçindekiler

[KISALTMALAR: xi](#_Toc472978329)

[ŞEKİLLER VE TABLOLAR xix](#_Toc472978330)

[ÖNSÖZ xxii](#_Toc472978331)

[BÖLÜM 1: GİRİŞ 1](#_Toc472978332)

[1.1 Tez Projesinin Konu ve Kapsamı: 1](#_Toc472978333)

[1.2 Tez Projesinin Amacı: 2](#_Toc472978334)

[1.3 Tez Projesinin Önemi: 2](#_Toc472978335)

[1.4 Wired and Wireless Network’lerde Fiziksel Güvenlik: 3](#_Toc472978336)

[1.5 Wired and Wireless Network’lerde Güvenlik İlkeleri ve Kavramları 4](#_Toc472978337)

[1.6 Wired and Wireless Network’lerde Bilişim Güvenliği 5](#_Toc472978338)

[1.7 Wired ve Wireless Network’lerde Güvenlik Teknolojileri ve Protokolleri 7](#_Toc472978339)

[1.8 Wired ve Wireless Network’lerde Çalışma Grupları, Uluslararası Standart Belirleyen Kurumlar 8](#_Toc472978340)

[1.9 Sonuç 9](#_Toc472978341)

[BÖLÜM 2: WIRED, WIRELESS NETWORKS ve FİZİKSEL GÜVENLİK 9](#_Toc472978342)

[2.1 WIRELESS NETWORKS 9](#_Toc472978343)

[2.1.1 Wireless Technologies 9](#_Toc472978344)

[2.1.1.1 Wireless Çeşitleri 11](#_Toc472978345)

[2.1.1.1.1 Wireless Personal Area Network (WPAN) 11](#_Toc472978346)

[2.1.1.1.1.1 ZigBee 12](#_Toc472978347)

[2.1.1.1.1.2 Ultra-Wideband (UWB) 12](#_Toc472978348)

[2.1.1.1.1.3 Bluetooth 12](#_Toc472978349)

[2.1.1.1.1.3.1 Bluetooth'un Genel Özellikleri 13](#_Toc472978350)

[2.1.1.1.1.3.2 Bluetooth Sürümleri 13](#_Toc472978351)

[2.1.1.1.1.4 Home RF 15](#_Toc472978352)

[2.1.1.1.2 Wireless Local Area Network (WLAN) 16](#_Toc472978353)

[2.1.1.1.2.1 Kablosuz Yerel Alan Ağ Standartları 19](#_Toc472978354)

[2.1.1.1.2.1.1 IEEE 802.11x Standartları 20](#_Toc472978355)

[2.1.1.1.2.1.2 IEEE 802.11a Standardı 20](#_Toc472978356)

[2.1.1.1.2.1.3 IEEE 802.11b Standardı 21](#_Toc472978357)

[2.1.1.1.2.1.4 IEEE 802.11g Standardı 21](#_Toc472978358)

[2.1.1.1.2.1.5 IEEE 802.11n Standardı 22](#_Toc472978359)

[2.1.1.1.2.2 HiperLAN 24](#_Toc472978360)

[2.1.1.1.2.3 Coding / Modulation Techniques 24](#_Toc472978361)

[2.1.1.1.2.4 Multiple Access and Duplication Methods 25](#_Toc472978362)

[2.1.1.1.2.5 Security and Encryption 26](#_Toc472978363)

[2.1.1.1.2.6 Wireless LAN Technologies 26](#_Toc472978364)

[2.1.1.1.2.6.1 RF Technology 27](#_Toc472978365)

[2.1.1.1.2.6.2 Infrared Technology 27](#_Toc472978366)

[2.1.1.1.2.7 Wireless LAN Systems 29](#_Toc472978367)

[2.1.1.1.2.7.1 Wireless LAN Systems Çalışma Esasları 30](#_Toc472978368)

[2.1.1.1.2.7.2 Wireless LAN System’lerde Kullanılan Frekanslar 30](#_Toc472978369)

[2.1.1.1.2.7.3 Wireless LAN System’inde Kullanılan Cihazlar 31](#_Toc472978370)

[2.1.1.1.2.7.4 Wireless LAN System’lerinin Mimari Yapısı 35](#_Toc472978371)

[2.1.1.1.2.7.5 Point-to-Point Wireless Connectivity 38](#_Toc472978372)

[2.1.1.1.2.7.6 Wireless LAN Uygulaması 39](#_Toc472978373)

[2.2 WIRED NETWORKS 42](#_Toc472978374)

[2.2.1 Yapılarına Göre Wired Computer Networks 44](#_Toc472978375)

[2.2.1.1 LAN (Local Area Network) 44](#_Toc472978376)

[2.2.1.1.1 Ethernet Kavramı ve Standartları 44](#_Toc472978377)

[2.2.1.1.2 Ethernet Ağ Elemanları 45](#_Toc472978378)

[2.2.1.1.3 CSMA/CD- Carrier Sense Multiple Access/Collision Detection 45](#_Toc472978379)

[2.2.1.1.4 MAC (Media Access Control) Adres Kavramı 46](#_Toc472978380)

[2.2.1.1.5 Ethernet Standartları 46](#_Toc472978381)

[2.2.1.1.6 Network Topologys 47](#_Toc472978382)

[2.2.1.1.6.1 Bus Topology 47](#_Toc472978383)

[2.2.1.1.6.2 Ring Topology 47](#_Toc472978384)

[2.2.1.1.6.3 Star Topology 48](#_Toc472978385)

[2.2.1.1.6.4 Mesh Topology 48](#_Toc472978386)

[2.2.1.2 MAN-Metropolitan Area Network 49](#_Toc472978387)

[2.2.1.3 WAN-Wide Area Network 49](#_Toc472978388)

[2.2.2 OSI (Open Systems Interconnection) 49](#_Toc472978389)

[2.2.2.1 Application Layer 51](#_Toc472978390)

[2.2.2.2 Presentation Layer 52](#_Toc472978391)

[2.2.2.3 Session Layer 52](#_Toc472978392)

[2.2.2.4 Transport Layer 52](#_Toc472978393)

[2.2.2.5 Network Layer 53](#_Toc472978394)

[2.2.2.6 Data Link Layer 53](#_Toc472978395)

[2.2.2.7 Physical Layer 54](#_Toc472978396)

[2.2.3 TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL) 54](#_Toc472978397)

[2.2.3.1 Uygulama Katmanı Protokolleri 55](#_Toc472978398)

[2.2.3.2 Taşıma Katmanı Protokolleri 56](#_Toc472978399)

[2.2.3.2.1 UDP (User Datagram Protocol) 59](#_Toc472978400)

[2.2.3.2.2 UDP ile TCP 'nin Farkları 60](#_Toc472978401)

[2.2.3.3 Network Layer Protocols 61](#_Toc472978402)

[2.2.3.3.1 ARP (Address Resulotion Protocol) 61](#_Toc472978403)

[2.2.3.3.2 ICMP (Internet Control Message Protocol) 62](#_Toc472978404)

[2.2.3.3.3 IP (Internet Protocol) 64](#_Toc472978405)

[2.2.3.3.4 IP Adresleme 65](#_Toc472978406)

[2.2.3.4 Data Link Layer 66](#_Toc472978407)

[2.2.3.4.1 PAKETLERİN FRAME YAPIYA DÖNÜŞTÜRÜLMESİ 69](#_Toc472978408)

[2.2.3.4.1 FRAME YAPISI 70](#_Toc472978409)

[2.2.3.5 Physical Layer 71](#_Toc472978410)

[2.3 WIRED ve WIRELESS NETWORK’LERDE FİZİKSEL GÜVENLİK 71](#_Toc472978411)

[2.3.1 Fiziksel Güvenlik 72](#_Toc472978412)

[2.3.1.1 Binalar 72](#_Toc472978413)

[2.3.1.2 Verinin Taşınması 73](#_Toc472978414)

[2.3.1.3 Veri Yedeklemeleri 73](#_Toc472978415)

[2.3.1.4 Diskler 74](#_Toc472978416)

[2.3.1.5 Dizüstü Bilgisayarlar 74](#_Toc472978417)

[2.3.1.6 Yazıcılar 74](#_Toc472978418)

[2.3.1.7 Bilgisayarlar 74](#_Toc472978419)

[2.3.1.8 Wired Network Hatları 75](#_Toc472978420)

[2.3.1.9 Bağlantı ve İletişim Elemenları 75](#_Toc472978421)

[BÖLÜM 3: WIRED ve WIRELESS NETWORK’LERDE GÜVENLİK İLKELERİ ve KAVRAMLARI 77](#_Toc472978422)

[3.1.“Bilişim Güvenliği”nden Ne Anlamalıyız? 78](#_Toc472978423)

[3.1.1 Bilişim Güvenliği Nedir? 78](#_Toc472978424)

[3.1.2 Güvenlik Prensipleri 80](#_Toc472978425)

[3.1.2.1 Confidentiality 80](#_Toc472978426)

[3.1.2.2 Data Integrity 81](#_Toc472978427)

[3.1.2.3 Availability 82](#_Toc472978428)

[3.1.2.4 Accountability 82](#_Toc472978429)

[3.1.2.5 Authentication 82](#_Toc472978430)

[3.1.2.6 Reliability- Consistency 83](#_Toc472978431)

[3.1.2.7 Non-Repudiation 83](#_Toc472978432)

[3.1.3 Threats 83](#_Toc472978433)

[3.1.4 Vulnerability 84](#_Toc472978434)

[3.1.5 Network Security Monitoring Süreçleri 85](#_Toc472978435)

[3.1.6 Risk 86](#_Toc472978436)

[BÖLÜM 4: WIRED ve WIRELESS NETWORK’LERDE BİLİŞİM GÜVENLİĞİ 89](#_Toc472978437)

[4.1 Bilişim Güvenliğinin Sağlanması 89](#_Toc472978438)

[4.1.1 Bilişim Güvenliği Süreç Alanları 89](#_Toc472978439)

[4.1.2 Bilişim Güvenliği Teknolojileri 91](#_Toc472978440)

[4.1.3 Eğitim 91](#_Toc472978441)

[4.2.Yönetsel Önlemler 93](#_Toc472978442)

[4.2.1 Risk Yönetimi 94](#_Toc472978443)

[4.2.1.1 Kurumsal Bilgi Kaynaklarına Değer Biçme 94](#_Toc472978444)

[4.2.1.2 Risk Analizi 95](#_Toc472978445)

[4.2.1.3 Tedbirlerin Seçimi 96](#_Toc472978446)

[4.2.2 Güvenlik Politikaları 96](#_Toc472978447)

[4.2.3 Standartlar, Yönergeler ve Prosedürler 98](#_Toc472978448)

[4.2.4 Güvenlik Yaşam Döngüsü 99](#_Toc472978449)

[4.2.5 Güvenlik Denetimleri 99](#_Toc472978450)

[4.3.Teknoloji Uygulamaları 100](#_Toc472978451)

[4.3.1 Kriptografi 101](#_Toc472978452)

[4.3.1.1 Simetrik Algoritmalar 102](#_Toc472978453)

[4.3.1.2 Asimetrik Algoritmalar 102](#_Toc472978454)

[4.3.1.3 Özetleme Fonksiyonları 103](#_Toc472978455)

[4.3.2 Sayısal İmza ve PKI 104](#_Toc472978456)

[4.3.3 Ağ Bölümlendirmesi ve Firewalls 105](#_Toc472978457)

[4.3.4 Yedekleme 107](#_Toc472978458)

[4.3.5. Saldırı Tespiti ve Saldırı Türleri 108](#_Toc472978459)

[4.3.5.1.Saldırı Türleri 108](#_Toc472978460)

[4.3.5.1.1 Sniffing 108](#_Toc472978461)

[4.3.5.1.1.1 Pasif Sniffing 108](#_Toc472978462)

[4.3.5.1.1.2 Aktif Sniffing 109](#_Toc472978463)

[4.3.5.1.1.3 ARP Poisoning 110](#_Toc472978464)

[4.3.5.1.2 Hizmet Dışı Bırakma (Denial Of Service) 112](#_Toc472978465)

[DoS Saldırı Çeşitleri 113](#_Toc472978466)

[4.3.5.1.2.1 Land Flood 115](#_Toc472978467)

[4.3.5.1.2.2 UDP Flood 115](#_Toc472978468)

[4.3.5.1.2.3 ICMP Flood 116](#_Toc472978469)

[4.3.5.1.2.4 Finger 117](#_Toc472978470)

[4.3.5.1.2.5 Ping of Death 118](#_Toc472978471)

[4.3.5.1.2.6 Smurf 118](#_Toc472978472)

[4.3.5.1.2.7 Fraggle 120](#_Toc472978473)

[4.3.5.1.2.8 DNS Poisoning 120](#_Toc472978474)

[4.3.5.1.2.9 Buffer Overflows 121](#_Toc472978475)

[4.3.5.1.2.10 HTTP Fragmentation 121](#_Toc472978476)

[4.3.5.1.2.11 Excessive VERB 122](#_Toc472978477)

[4.3.5.1.2.12 Faulty Application 122](#_Toc472978478)

[4.3.5.1.2.13 Media Data Flood 122](#_Toc472978479)

[DDos Savunma Yöntemleri 122](#_Toc472978480)

[4.3.5.1.3 IP Spoofing 126](#_Toc472978481)

[Genel Anlamda (Spoofing’den) Korunma Yöntemleri 127](#_Toc472978482)

[4.3.5.1.4 Kabloya saplama yapma 128](#_Toc472978483)

[4.3.5.1.5 Kriptografik Saldırılar 128](#_Toc472978484)

[4.3.5.1.5.1 Kriptanaliz ve Kriptosistemlere Saldırılar: 128](#_Toc472978485)

[4.3.5.1.5.2 Cipher-Text Only Saldırısı 128](#_Toc472978486)

[4.3.5.1.5.3 Known-PlainText Attack 129](#_Toc472978487)

[4.3.5.1.5.4 Selected Plaintext Attack 129](#_Toc472978488)

[4.3.5.1.5.5 Man in the Middle Attack: 129](#_Toc472978489)

[4.3.5.1.5.6 IPSec tanımı 130](#_Toc472978490)

[4.3.5.1.6 Sosyal Mühendislik 131](#_Toc472978491)

[4.3.5.1.7 SQL Injection 131](#_Toc472978492)

[4.3.5.1.8 Command Injection 131](#_Toc472978493)

[4.3.5.1.9 HTML Injection 132](#_Toc472978494)

[4.3.5.1.10 Backdoors 132](#_Toc472978495)

[4.3.5.1.11 Phishing 133](#_Toc472978496)

[4.3.5.1.11.1 Neler Çalınıyor? 133](#_Toc472978497)

[4.3.5.1.11.2 Bu dolandırıcılık işlemi nasıl gerçekleştirilmektedir? 133](#_Toc472978498)

[4.3.5.1.11.3 Phishingten Nasıl Korunulur? 134](#_Toc472978499)

[4.3.5.1.12 Rootkits 135](#_Toc472978500)

[4.3.5.1.13 Spyware 136](#_Toc472978501)

[4.3.5.1.14 Viruses 137](#_Toc472978502)

[4.3.5.1.15 Trojans 139](#_Toc472978503)

[4.3.5.1.16 Worms 140](#_Toc472978504)

[4.3.5.1.17 Bot 141](#_Toc472978505)

[4.3.5.1.18 Botnets 142](#_Toc472978506)

[4.3.5.1.19 Keyloggers 143](#_Toc472978507)

[4.3.5.2.Saldırı Tespiti 144](#_Toc472978508)

[4.3.6 Access Control 145](#_Toc472978509)

[4.3.6.1 Identification 146](#_Toc472978510)

[4.3.6.2 Authentication 146](#_Toc472978511)

[4.3.6.3 Authorization 147](#_Toc472978512)

[4.3.7 Anti-Virüs Sistemleri 148](#_Toc472978513)

[4.3.8 Eğitim 149](#_Toc472978514)

[4.3.9 Bilişim Güvenliği Standartları 150](#_Toc472978515)

[BÖLÜM 5: WIRED ve WIRELESS NETWORK’LERDE GÜVENLİK TEKNOLOJİLERİ ve PROTOKOLLERİ 152](#_Toc472978516)

[5.1 Wired ve Wireless Network’lerin Taşıdığı Riskler 152](#_Toc472978517)

[5.1.1 Wireless Network’e Sızma 152](#_Toc472978518)

[5.1.2 Trafiğin Dinlenip Verinin Çözülmesi 152](#_Toc472978519)

[5.1.3 Ağ Topolojisinin Ortaya Çıkması 153](#_Toc472978520)

[5.1.4 İstemcilerin Yetkisiz Access Point’lara Bağlanması 153](#_Toc472978521)

[5.1.5 İstenmeyen Yerlere Servis Verme 153](#_Toc472978522)

[5.1.6 Denial of service (DoS) 153](#_Toc472978523)

[5.2. Wireless Network’lerde Güvenlik Protokolleri 154](#_Toc472978524)

[5.2.1 WEP (Wireless Equivalent Privacy – 1999) 154](#_Toc472978525)

[5.2.1.1 WEP’te Asıllama Yöntemleri 154](#_Toc472978526)

[5.2.1.2 WEP’te Kullanılan Anahtarlar 156](#_Toc472978527)

[5.2.1.3 Şifreleme ve Şifre Çözme 156](#_Toc472978528)

[5.2.1.4 WEP Zayıflıkları 157](#_Toc472978529)

[5.2.1.4.1 Asıllama: 158](#_Toc472978530)

[5.2.1.4.2 Tekrar Saldırısı 158](#_Toc472978531)

[5.2.1.4.3 Bit Flapping 159](#_Toc472978532)

[5.2.1.4.4 IV’lerin Tekrar Kullanılması 159](#_Toc472978533)

[5.2.1.4.5 RC4 Zayıf Anahtarlar Üretmesi (Fluhrer et al 2001) (FSM attack) 160](#_Toc472978534)

[5.2.1.5 WEP Özet 160](#_Toc472978535)

[5.2.2 WPA (Wireless Protected Access -2002) 160](#_Toc472978536)

[5.2.2.1 TKIP- Temporal Key Integrity Protocol 161](#_Toc472978537)

[5.2.2.2 802.1x (EAP) ile Asıllama 161](#_Toc472978538)

[5.2.2.3 MIC (Message Integrity Code) 162](#_Toc472978539)

[5.2.2.4 Anahtar Yönetimi 163](#_Toc472978540)

[5.2.2.4.1 Oturum Anahtar Kümesinin Üretilmesi 164](#_Toc472978541)

[5.2.2.4.2 Grup Anahtar Kümelerinin Üretilmesi 165](#_Toc472978542)

[5.2.2.4.3 Farklı Anahtar Üretimi 166](#_Toc472978543)

[5.2.3 RSN (Robust Security Network, IEEE 802.11i, WPA2) 2004 168](#_Toc472978544)

[5.2.3.1 CCMP (Counter Mode –CBC MAC Protocol) 169](#_Toc472978545)

[5.2.3.1.1 Counter Mode: 169](#_Toc472978546)

[5.2.3.1.2 CBC- MAC Mode: 169](#_Toc472978547)

[5.3.1 Application Layer Güvenlik Protokolleri 171](#_Toc472978548)

[5.3.1.1 PGP (Pretty Good Privacy) 171](#_Toc472978549)

[5.3.1.1.1 PGP Nedir? 171](#_Toc472978550)

[5.3.1.1.2 PGP’nin Çıkışı 171](#_Toc472978551)

[5.3.1.1.3 PGP’nin Çalışma Prensibi 172](#_Toc472978552)

[5.3.1.1.4 PGP’nin Güvenliği 174](#_Toc472978553)

[5.3.1.2 S/MIME (Secure Multi-Purpose Internet Mail Extensions) 174](#_Toc472978554)

[5.3.1.3 S-HTTP (Secure HTTP) 174](#_Toc472978555)

[5.3.1.4 HTTPS (HTTP over SSL or HTTP Secure) 175](#_Toc472978556)

[5.3.1.5 Secure Electronic Transaction (SET) 176](#_Toc472978557)

[5.3.1.5 Kerberos 177](#_Toc472978558)

[5.3.1.5.1 Kerberos’un Çalışma Prensibi 178](#_Toc472978559)

[5.3.2 Transport Layer Security Protocols 179](#_Toc472978560)

[5.3.2.1 SSL VPN (Secure Sockets Layer Virtual Private Network) 179](#_Toc472978561)

[5.3.2.1.1 SSL Portal VPN: 179](#_Toc472978562)

[5.3.2.1.2 SSL Tunel VPN: 180](#_Toc472978563)

[5.3.2.2 Transport Layer Security (TLS) 180](#_Toc472978564)

[5.3.3 Network Layer Security Protocols 181](#_Toc472978565)

[5.3.3.1 IPsec (Internet Protocol Security) 181](#_Toc472978566)

[5.3.3.1.1 Authentication Header 181](#_Toc472978567)

[5.4.3.3.1.2 Encapsulating Security Payload(ESP) 182](#_Toc472978568)

[5.3.3.2 Virtual Private Network (VPN) 183](#_Toc472978569)

[5.3.4 Data Link Layer Güvenlik Protokolleri 185](#_Toc472978570)

[5.3.4.1 PPP (Point-to-Point Protocol) 185](#_Toc472978571)

[5.3.4.2 RADIUS (Remote Authentication Dial-In User Service) 185](#_Toc472978572)

[5.3.4.3 TACACS (Terminal Access Controller Access Control System) 186](#_Toc472978573)

[5.4. Diğer Authentication Protokolleri 186](#_Toc472978574)

[5.4.1 CHAP (Challenge-Handshake Authentication Protocol) 186](#_Toc472978575)

[5.4.2 Extensible Authentication Protocol (EAP) 187](#_Toc472978576)

[5.4.3 Password Authentication Protocol (PAP) 187](#_Toc472978577)

[5.4.4 Shiva Password Authentication Protocol (SPAP) 188](#_Toc472978578)

[5.4.5 Data Encryption Standard (DES) 188](#_Toc472978579)

[5.4.5.1 DES anahtar uzunluğu ve kaba kuvvet saldırıları 189](#_Toc472978580)

[5.4.5.2 DES için halefler 190](#_Toc472978581)

[5.4.6 S/Key Authentication 190](#_Toc472978582)

[5.4.7 MS-CHAP Authentication 190](#_Toc472978583)

[BÖLÜM 6: WIRED ve WIRELESS NETWORK’LERDE ÇALIŞMA GRUPLARI ve ULUSLARARASI STANDART BELİRLEYEN KURUMLAR 191](#_Toc472978584)

[6.1. ISO (International Organization for Standardization) 192](#_Toc472978585)

[6.1.1 ISO Nedir? 192](#_Toc472978586)

[6.1.2 ISO Tarihçe 192](#_Toc472978587)

[6.1.3 ISO Standartları Nelerdir? 193](#_Toc472978588)

[6.1.4 ISO Yönetim Standartları 193](#_Toc472978589)

[6.1.4.1 ISO 27001 Bilgi Güvenliği Yönetim Sistemi: 194](#_Toc472978590)

[6.1.4.2 ISO 27000 Serisi Standartları 194](#_Toc472978591)

[6.2. ANSI (American National Standards Institute) 195](#_Toc472978592)

[6.3. NIST (National Institute of Standards and Technology) 196](#_Toc472978593)

[6.3.1 Wired ve Wireless Network’lerde Güvenliğe Dair NIST’in Belirlediği SP 800 Seri Standartlar Listesi [127] 197](#_Toc472978594)

[3.2 Wired ve Wireless Network’lerde Güvenliğe Dair NIST’in Belirlediği SP 1800 Seri Standartlar Listesi [127] 220](#_Toc472978595)

[6.4. ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union) 220](#_Toc472978596)

[6.4.1 ITU TarafındanYayınlanmış Kilit Standartlar 221](#_Toc472978597)

[6.5. ISOC (internet society) 222](#_Toc472978598)

[6.5.1 Internet Engineering Task Force –IETF 223](#_Toc472978599)

[6.5.2 The Internet Architecture Board-IAB 223](#_Toc472978600)

[6.5.3 Internet Engineering Steering Group-IESG 223](#_Toc472978601)

[6.5.4 The Internet Research Task Force -IRTF 224](#_Toc472978602)

[6.5.5 RFC (Request for Comments) 224](#_Toc472978603)

[6.6 ETSI (European Telecommunications Standards Institute) 226](#_Toc472978604)

[6.6.1 ETSI Standartları 226](#_Toc472978605)

[6.6.1.1 European Standard, telecommunications series (EN): 226](#_Toc472978606)

[6.6.1.2 ETSI Standard (ES): 226](#_Toc472978607)

[6.6.1.3 ETSI Guide (EG): 226](#_Toc472978608)

[6.6.1.4 Special Report (SR): 226](#_Toc472978609)

[6.6.1.5 ETSI Technical Specification (TS): 227](#_Toc472978610)

[6.6.1.6 ETSI Technical Report (TR): 227](#_Toc472978611)

[6.6.1.7 ETSI Group Specification (GS): 227](#_Toc472978612)

[6.7 OMTP (Open Mobile Terminal Platform) 227](#_Toc472978613)

[6.8 GSMA (The GSM Association) 228](#_Toc472978614)

[6.9. TCG (Trusted Computing Group) 231](#_Toc472978615)

[6.9.1 Bir TCG Standardı: TPM 231](#_Toc472978616)

[6.9.1.1 TPM’nin İşlevi 232](#_Toc472978617)

[6.9.1.2 TPM’de Güvenliğin Sağlanması 234](#_Toc472978618)

[6.10. IEEE (Institute of Electrical and Electronics Engineers) 234](#_Toc472978619)

[6.10.1 Network and Information Security (NIS) Alanında IEEE Standart Faaliyetlerine Genel Bakış 235](#_Toc472978620)

[6.10.1.1 İlgili Standartlar Faaliyetleri 236](#_Toc472978621)

[6.10.1.1.1 Şifreleme 236](#_Toc472978622)

[6.10.1.1.2 Sabit ve Çıkarılabilir Depolama 236](#_Toc472978623)

[6.10.1.1.3 Yazılım Tanımlı Ağ ve Ağ İşlevleri Sanallaştırması için Güvenlik 236](#_Toc472978624)

[6.10.1.1.4 Hardcopy Aygıtları için Güvenlik 237](#_Toc472978625)

[6.10.1.1.5 Akıllı Şebeke için NIS 237](#_Toc472978626)

[BÖLÜM 7: SONUÇ 238](#_Toc472978627)

# KISALTMALAR:

WPAN :Wireless Personal Area Network

UWB :Ultra-Wideband

EDR :Enhanced Data Rate

HS :High Speed

Home R :Home Radio Frequency

WLAN :Wireless Local Area Network

LAN :Local Area Network

MAN :Metropolitan Area Network

FHSS :Frequency Hopping Spread Spectrum

DSSS :Direct Sequence Spread Spectrum

Wi*-*Fi :Wireless Fidelity

RF-Band :Radio Frequency Band

OFDM :Orthogonal Frequency Division Multiplexing

WEP  :Wired Equivalent Privacy

PDA :Personal Digital Assistant

FDMA :Frequency Division Multiple Access

TDMA :Time Division Multiple Access

CDMA :Code Division Multiple Access

FDD :Frequency Division Duplex

AP :Access point

VPN :Virtual Private Network

TDD :Time Division Duplex

PC :Personal Computer

PDA :Personal Digital Assistant

NIC :Network Interface Card

DSL :Digital Subscriber Line

FWA :Fixed Wireless Access

PCMCIA **:P**ersonal**C**omputer**M**emory**C**ard**I**nternational**A**ssociation

ISM :Industrial Scientific Medical band

ITU-RR :[International Telecommunication Union](https://en.wikipedia.org/wiki/International_Telecommunication_Union) -Radio Regulations

OFDM :Orthogonal frequency-division multiplexing

WDS  :Wireless Distribution System

ISA :Industry Standard Architecture

ATM :Asynchronous Transfer Mode

OSI :Open Systems Interconnection

ISO :International Standarts Organization

AL :Application Layer

http :Hypertext Transfer Protocol

FTP :File Transfer Protocol

NFS :Network File System

SMTP :Simple Mail Transfer Protocol

PL :Presentation Layer

ASCII :American National Standard Code for Information Interchange

EBCDIC :Extended Binary Coded Decimal Interchange Code

BCD :Binary-Coded Decimal)

SL :Session Layer

TL :Transport Layer

NL :Network Layer

PL :Physical Layer

DLL :Data Link Layer

CRC :Cyclic Redundancy Check

ECC :Error Correction Codes

PARC :Palo Alto Research Center

IEEE :Institute of Electrical and Electronics Engineers

CSMA :Carrier Sense Multiple Access

CD :Collision Detection

DTE :Data Terminal Equipment

DCE :Data Communication Equipment

UDP :User Datagram Protocol

TCP :Transmission Control Protocol

IP :Internet Protocol

ARP :Address Resolution Protocol

SNMP :Simple Network Management Protocol

TTL :Time to live

UTP  :Unshielded Twisted Pair

BNC :(Bayonet Neill–Concelman) connector

MAC :Media Access Control

IPX :Internetwork Packet Exchange

CSI :Computer Security Institute

NSM :Network Security Monitoring

CISSP :Certified Information Systems Security Professional

AES :Advanced Encryption Standard

DES :Data Encryption Standard

3DES :Triple Data Encryption Algorithm

IDEA :International Data Encryption Algorithm

RC4 :Rivest Cipher 4

SAFER :Secure And Fast Encryption Routine

RSA :Rivest, Shamir and Adleman Algorithm

ECC :Elliptic Curve Cryptography

SHA-1 :Secure Hash Algorithm 1

DSS :Digital Signature Standard

MD2 :Message-Digest Algorithm2

MD4 :Message-Digest Algorithm4

MD5 :Message-Digest Algorithm5

PKI :Public Key Infrastructure

NAT :Network Address Translation

IDS :Intrusion Detection System

IRC :Internet Relay Chat

DoS :Denial of Service

DDos :Distrubuted Denial of Service

DRDoS :Distrubuted Reflective Denial Of Service

RST :Reset Connection

FIN :Finish Connection

ACK :Acknowledgement

FACK :Fragmented Acknowledgement

ICMP :Internet Control Message Protocol

UDP :User Datagram Protocol

DNS  :Domain Name System

IDP :Intrusion Detection Prevention

IPSec :Internet Protocol Security

XSS :Cross-Site Scripting

SQL :Structured Query Language

 EULA :End User License Agreement

SMS :Short Message Service

URL :Uniform Resource Locator

RAt :Remote Management Tool

IDS :Intrusion Detection System

AC :Access Control

RSN :Robust Security Network

POP3 :Post Office Protocol 3

NTLM :NT LAN Manager

SSID :Service Set Identifier

RADIUS :Remote Authentication Dial-In User Service

MAC :Media Access Control

SSID :Service Set Identifier

ICV :Integrity Check Value

CRC :Cyclic Redundancy Check

TKIP :Temporal Key Integrity Protocol

EAP :Extensible Authentication Protocol

MIC :Message Integrity Code

WPA :Wi-Fi Protected Access

WEP IV :Wired Equivalent Privacy Initialization Vector

MPDU :Message Protocol Data Unit

TTAK :Temporal Transmitter Address Key

MSDU :MAC Service Data Unit

DA :Destination Address

SA :Source Address

SA :Sequence Number

TA :Transmitter Address

PGP :Pretty Good Privacy

DSA :Driving Standards Agency

S/MIME :Secure Multi-Purpose Internet Mail Extensions

SSL :Secure Sockets Layer

IETF :Internet Engineering Task Force

TLS :Transport Layer Security

HTTPS  :Secure Hypertext Transfer Protocol

SET :Secure Electronic Transaction

STT :Secure Transaction Technology

PKI :Public Key Infrastructure

MIT :Massachusetts Institute of Technology

KDC :Key Distribution Center

ISAKMP :Internet Security Association and Key Management Protocol

AH :Authentication Header

ESP :Encapsulating Security Payload

PPP :Point-to-Point Protocol

TACACS :Terminal Access Controller Access Control System

XTACACS:Extended Terminal Access Controller Access Control System

CHAP :Challenge-Handshake Authentication Protocol

PAP :Password Authentication Protocol

SPAP :Shiva Password Authentication Protocol

FIPS :Federal Information Processing Standards

LCP :Link Control Protocol

IEC :International Electrotechnical Commission

ANSI :American National Standards Institute

NIST :National Institute of Standards and Technology

SP-NIST :Special Publication International Organization for Standardization

ITU-T :Telecommunication Standardization Sector of the International Telecommunications Union

CCITT :Consultative Committee for International Telephony and Telegraphy

IETF :Internet Engineering Task Force

IAB :Internet Architecture Board

IESG :Internet Engineering Steering Group

IRTF :Internet Research Task Force

RFC :Request for Comments

ISOC :Internet Society

[DSL](https://en.wikipedia.org/wiki/DSL) :Digital Subscriber Line

ETSI :European Telecommunications Standards Institute

TMN :Telecommunications Management Network

ES :ETSI Standard

EG :ETSI Guide

SR :Special Report

TS :ETSI Technical Specification

TR :ETSI Technical Report

GS :ETSI Group Specification

OMTP :Open Mobile Terminal Platform

ADM :Advanced Device Management

GSMA :The GSM Association

TCG :Trusted Computing Group

AMD :Advanced Micro Devices

TNC :Trusted Network Connect

TPM :Trusted Platform Module

SWG :Standards Working Group

NIS :Network and Information Security

IEEE :Institute of Electrical and Electronics Engineers

ETI :Traffic Inspection Working Group

AMSS :Anti-Malware Support Service

IED :Intelligent Electronic Devices

# ŞEKİLLER VE TABLOLAR

[Şekil 2.1.1: Wireless Communication 32](#_Toc472971869)

[Şekil 2.1.1.1.1: Wireless Personal Area Network (WPAN) 33](#_Toc472971870)

[Şekil 3: Bluetooth Uygulamaları 34](#_Toc472971871)

[Şekil 4: Wireless Local Area Network (WLAN) 38](#_Toc472971872)

[Şekil 5: Wireless Local Area Network’ların kullanım alanları 39](#_Toc472971873)

[Şekil 6: 802.11b, g standardı ve 802.11n standardı radyo sinyal yayılımı 43](#_Toc472971874)

[Şekil 7: MIMO teknolojisi ile radyo sinyallerinin akışı 44](#_Toc472971875)

[Şekil 8: ISM Frekans Bant 51](#_Toc472971876)

[Şekil 9: Wired LAN ve Wireless LAN’ların access point’ları ile birleştirilmesi 52](#_Toc472971877)

[Şekil 10 :Erişim Cihazı 52](#_Toc472971878)

[Şekil 11: Bit PCI slot 54](#_Toc472971879)

[Şekil 12: Bir üniversite kampüsünde uygulanan wireless LAN’da kullanılan antenler 55](#_Toc472971880)

[Şekil 13: Ad Hoc modeli 56](#_Toc472971881)

[Şekil 14: Infrastructure, Client/Server Çalışma Modeli 57](#_Toc472971882)

[Şekil 15: Point-to-Point Wireless Connectivity 58](#_Toc472971883)

[Şekil 16: Bilgisayar Wired Network Yapısı Örnek 62](#_Toc472971884)

[Şekil 17: Computer Networks 65](#_Toc472971885)

[Şekil 18: Veriyolu Topoloji 66](#_Toc472971886)

[Şekil 19 : Ring Topology 66](#_Toc472971887)

[Şekil 20: Star Topology 67](#_Toc472971888)

[Şekil 21: Mesh Topology 67](#_Toc472971889)

[Şekil 22: Computer Networks 68](#_Toc472971890)

[Şekil 23: TCP/IP ve OSI karşılaştırması 73](#_Toc472971891)

[Şekil 22.2.3.4.1: Frame Yapısı/Frame formatı genel olarak şu alanlardan oluşmaktadır. 86](#_Toc472971892)

[Şekil 25: Temel Güvenlik Prensipleri 96](#_Toc472971893)

[Şekil 26: Temel Güvenlik Kavramlarının Birbirleri İle Olan İlişkileri 103](#_Toc472971894)

[Şekil 27: Bilgi Güvenliğinin Sağlanmasında Bütünleşik Yaklaşım 104](#_Toc472971895)

[Şekil 28: Kurumun Sahip Olduğu Değerli Varlıkların Korunması 105](#_Toc472971896)

[Şekil 29: Risk Yönetiminin Adımları 109](#_Toc472971897)

[Şekil 30: Temel Kriptogtafi Mekanizması 114](#_Toc472971898)

[Şekil 31: Kullanışı 115](#_Toc472971899)

[Şekil 32: Bir Mesajın Sayısal İmzasıʹnın Oluşturulması gönderilmesinde kullanılabilir. Sayısal sertifikalar için ISO tarafından X.509 standardı yayınlanmıştır ve bu standart yaygın olarak kullanılmaktadır. 118](#_Toc472971900)

[Şekil 33: Pasif Sniffing 122](#_Toc472971901)

[Şekil 34: Aktif Sniffing 122](#_Toc472971902)

[Şekil 35: ARP Zehirlenmesi 123](#_Toc472971903)

[Şekil 36: DDos Saldırısı 125](#_Toc472971904)

[Şekil 37:TCP three handshake 126](#_Toc472971905)

[Şekil 38:TCP SYN Flood Saldırısı 126](#_Toc472971906)

[Şekil 39: ICMP Flood Saldırısı 129](#_Toc472971907)

[Şekil 40: Ölüm Pingi 130](#_Toc472971908)

[Şekil 41: Smurf Saldırısı 131](#_Toc472971909)

[Şekil 42: DNS Poisoning 132](#_Toc472971910)

[Şekil 43: Anonymous LOIC Saldırı Yazılımı Arayüzü 134](#_Toc472971911)

[Şekil 44: IP Aldatması 138](#_Toc472971912)

[Şekil 45: IP Aldatması 2 138](#_Toc472971913)

[Şekil 46: Kabloya Saplama 139](#_Toc472971914)

[Şekil 47: Selected Plaintext Attack Görseli 140](#_Toc472971915)

[Şekil 48: Man in the Middle Attack 141](#_Toc472971916)

[Şekil 49: Sosyal Mühendislik 142](#_Toc472971917)

[Şekil 50: Basit Bir Bot-Net 152](#_Toc472971918)

[Şekil 51: Açık Güvenlik Asıllama Yöntemi 163](#_Toc472971919)

[Şekil 52: Ortak Anahtarlı Asıllama 164](#_Toc472971920)

[Şekil 53: MAC Adresi ile Asıllama 164](#_Toc472971921)

[Şekil 54: WEP’te kullanılan Anahtar 165](file:///C:\Users\ufukatakan\Desktop\TEZ\Tez-son%202%202%20(1).docx#_Toc472971922)

[Şekil 55: WEP Şifreleme ve Şifre Çözme 166](#_Toc472971923)

[Şekil 56: WEP Çerçeve Yapısı 166](file:///C:\Users\ufukatakan\Desktop\TEZ\Tez-son%202%202%20(1).docx#_Toc472971924)

[Şekil 57: Ortak Anahtarlı Asıllamadaki Zayıflık 167](#_Toc472971925)

[Şekil 58: Bit Flapping 168](#_Toc472971926)

[Şekil 59: 802.1x ile Asıllama 171](#_Toc472971927)

[Şekil 60: MIC Mesaj Bütünlük Kontrolu 171](#_Toc472971928)

[Şekil 61: Oturum ve Grup Anahtarları Hiyerarşik Yapısı 172](#_Toc472971929)

[Şekil 62: Oturum Anahtarı Kümesi Eldesi 173](#_Toc472971930)

[Şekil 63: Grup Anahtarı Kümesi Eldesi 174](#_Toc472971931)

[Şekil 64: Farklı Anahtar Üretimi 174](#_Toc472971932)

[Şekil 65: TKIP Yapısı 175](#_Toc472971933)

[Şekil 66: AES counter (sayaç) çalışma modu 177](#_Toc472971934)

[Şekil 67: CCMP Çalışma Yapısı 178](#_Toc472971935)

[Şekil 68: PGP’nin Çalışma Prensibi 180](#_Toc472971936)

[Şekil 69: Authentication Header 188](#_Toc472971937)

[Şekil 70: ESP 189](#_Toc472971938)

[Şekil 71: OMTP Standard Örneği 232](#_Toc472971939)

[Şekil 72: TPM’nin işletim sistemi mimarisindeki yeri [155]. 237](#_Toc472971940)

[Şekil 73.: TPM içyapısı [155]. 237](file:///C:\Users\ufukatakan\Desktop\TEZ\Tez-son%202%202%20(1).docx#_Toc472971941)

[Tablo 1: Home RF Frekans Aralık Tablosu 36](#_Toc472108445)

[Tablo 2: IEEE’nin 802.11x standartlarının karşılaştırılması 41](#_Toc472108446)

[Tablo 3: Yaygın IEEE WLAN standartları 44](#_Toc472108447)

[Tablo 4: Multiple Access and Duplication Methods 46](#_Toc472108448)

[Tablo 5: Şifreleme tekniğine göre kullanılabilecek anahtar uzunlukları 47](#_Toc472108449)

[Tablo 6: Infrared teknolojisinin üstünlük ve mahzurları 49](#_Toc472108450)

[Tablo 7: Duvarın yapısına göre sinyallerin zayıflama değerleri 60](#_Toc472108451)

[Tablo 8: Ethernet standartları 65](#_Toc472108452)

[Tablo 9: OSI Katmanları 69](#_Toc472108453)

[Tablo 10: TCP paket formatı 75](#_Toc472108454)

[Tablo 11: UDP paket formatı 77](#_Toc472108455)

[Tablo 12: TCP ile UDP farkları 78](#_Toc472108456)

[Tablo 13: ICMP mesaj tipleri 80](#_Toc472108457)

[Tablo 14: ICMP formatı 81](#_Toc472108458)

[Tablo 15: Tehdit Kaynağı- Güvenlik Boşluğu- Risk İlişkisine örnekler 101](#_Toc472108459)

[Tablo 16: WEP ve WPA karşılaştırması 176](#_Toc472108460)

[Tablo 17: WEP, WPA ve RSN Karşılaştırması5.3. Kablolu Ağlarda Güvenlik Protokolleri 178](#_Toc472108461)

[Tablo 18: Wired ve Wireless Network’lerde NIST SP 800 Güvenlik Standartları 224](#_Toc472108462)

[Tablo 19: Wired ve Wireless Network’lerde NIST SP 1800 Güvenlik Standartları 225](#_Toc472108463)

[Tablo 20: GSM Güvenlik standartları 235](#_Toc472108464)

# ÖNSÖZ

Bu tez çalışmasına, bilgisayar kablolu ve kablosuz ağ sistemlerindeki güvenlik mekanizmalarının işleyişine duyduğum merak ve konunun artık günümüzde her alanda hayati öneme sahip olması sebep olmuştur. Bilimsel çalışmaların kaynağını oluşturan merak beni de bu konuda geniş bir araştırma yapmaya sevk etmiştir. Geleneksel bilgi teknolojileri güvenliğini araştırmaya başlayıp, her alanda en çok ihtiyaç duyulan kıstas olan güvenlik mekanizmaları ve konusunu, kablolu ve kablosuz ağlarda güvenlik ve günümüzdeki tehditler gibi geniş bir kapsamda tutarak araştırmaya devam ettim. Sonuçta tam olarak çalışan bir sistem üzerinde araştırmalarımı test etmeye zamanım yetmese de yaptığım bu çalışmanın bu tip çalışmalara ön ayak olmasını, kaynak teşkil etmesini umduğum bu belgeyi ortayta çıkarabildim.

Bu belge içerisinde, bilgi güvenlik teknolojilerini, bilgilerin güvenliğinin sağlanması için kullanılan yöntemleri, yapılan çalışmaları, bilinen günümüz tehditlerini ve bilgisayar çağında kablolu ve kablosuz ağların bütününde güvenliğin gelişim ve önemini açıklamaya çalıştım.

Sonuç olarak bu çalışmanın, bu konudaki araştırma eksikliğini bir nebze olsun kapatmasını umduğum gibi gelecek çalışmalara kaynak teşkil etmesini ümit ediyorum.

**Teşekkür**

Tez çalışması sırasında, sahip olduğu insani değerlerle bana örnek teşkil eden ve tezde dâhil olmak üzere her türlü çalışmamda yakın ilgi ve desteğini üzerimden eksik etmeyen tez danışmanım **Prof. Dr. Levent TOKER’**e teşekkürü bir borç bilirim. Ayrıca bu tezi hazırlarken gereksinim duyduğum bilgi birikimini bana kazandıran bölümdeki tüm öğretim görevlilerine, arkadaşlarıma ve destek aldığım kaynak kitapların eşsiz yazarlarına teşekkür ederim.

# BÖLÜM 1: GİRİŞ

## 1.1 Tez Projesinin Konu ve Kapsamı:

Günümüzde bilgiye her yerden kolayca erişebilme istek ve arzusu, wired ve wireless network teknolojileri ve bunların güvenliği konusunun aslında ne kadar önemli olduğunu bizlere göstermektedir. Neredeyse artık hiçbir işin günümüzde internetsiz olmadığı gerçeği de düşünüldüğünde wired ve wireless network’lerdeki güvenliğin aslında ne kadar hayati bir öneme sahip olduğu açıkça görülmektedir.

Günümüzde wireless network teknolojilerinin kullanımda sağladığı pratik kullanımı gibi nedenler wireless network teknolojilerine olan talebi wired network’e olan talebe oranla sürekli olarak artırmakta, bu alanın sektörel olarak büyümesine, yaygınlaşmasına ve çeşitliliğine neden olmaktadır. Bu gelişmelerin bir sonucu olarak bilgiye her yerden erişim kolaylaşmakta bilgiler merkezi olmaktan çıkıp, daha kolay paylaşılabilir ve erişilebilir hale gelmektedir. Bilginin bu denli kolay erişilebilir olması, sistemsel ya da insana dayalı pek çok zafiyeti de ne yazık ki beraberinde getirmektedir. Bu zafiyetleri kullanan tehditler ise bilgi güvenliği açısından büyük riskleri doğurabilmektedir.

Wireless network risklerinin yanında wired network, e-posta ve web üzerinden gelebilecek tehditlerin de eklenmesi sonucu, bilgi güvenliği çok daha önemli hale gelmiştir. Bu riskleri önlemenin en etkin çözümlerinden biri kurumsal bilgi güvenliği politikalarını etkin işletmek yani sistemsel kontrol ve önlemleri almaktan diğeri ise bilgi güvenliği farkındalık çalışmalarını yürütmekten geçmektedir. Bu tez çalışması konu ve kapsam olarak, ilk başta, her geçen gün hızla yaygınlaşan ve gelişen kablosuz ağ teknolojileri ve genel var olan wired teknolojiler, türleri, standartları, yapıları, bunları sağladığı yaşamsal kolaylıklar hakkında temel bilgilendirme sağlamayı amaçlayan kritik bilgileri içermektedir. Daha sonra ise wired ve wireless network’lerde çok kritik, hayati öneme sahip olan güvenlik konusu, tehditler, bilgi güvenliği riskleri, bu riskleri asgari seviyeye çekmede bilgi güvenliği farkındalığının önemi ve nasıl daha güvenli ağ teknolojilerine sahip olabileceğimiz yöntemi konusunda belirli düzeyde araştırma çalışması içerecektir.

## 1.2 Tez Projesinin Amacı:

Günümüz dünyasında her iş internet üzerinden yürütülmektedir. Banka işlemleri, resmi kurum ve kuruluşlardaki işlemler, hastane işlemler vs. neredeyse hiçbir şey artık internet olmadan işler halde değildir. İnternetin, bilgi işlemin bu denli hayati bir hal aldığı günümüz şartlarında da wired ve wireless network’lerde güvenlik ve günümüzdeki tehditler konusu şu halde büyük bir önem arz etmektedir. Gelişmekte olan küresel dünya, artık bilgi temelli olarak şekillenmekte ve bilgi işlem üzerine kurulmaya devam etmektedir. Tam da bu noktada, bütün küresel ağlarımızın temelindeki wired ve wireless network’lerin güvenliği ve bunlara yönelik günümüz tehditleri artık bugünün en temel sorunlarından biri haline gelmiş ve üzerinde büyük çalışmalar yürütülen kritik bir konu olmuştur.

Bu bağlamda, bu tez projesi, ilk olarak bizim için bu kadar kritik önem arz eden bir konuda farkındalığı arttırmayı, belirli bir düzeyde bilinçlendirmeyi, bu konudaki güvenliğin önemini vurgulamayı amaçlamaktadır. Daha sonra wired ve wireless network’lerdeki güvenlik konusundaki esasları kapsamlı bir araştırmaya dayanarak belirtmeyi, bu konuya dair günümüzdeki tehdit unsurları ve bunlara karşı nasıl, ne çeşit önlemler alınabileceğini konusunda bir kaynak olmayı, bilgilendirmeyi amaçlamaktadır.

## 1.3 Tez Projesinin Önemi:

Wired ve wireless networks’lerin güvenliği, hayatın neredeyse her noktasının artık internet ve bilgi-bilişim üzerine kurulu olduğu düşünüldüğünde, kritik, hatta çok hayati bir önem arz etmektedir. Wired, wireless networks’lerin güvenliği demek, günümüzde aslında tam anlamıyla her şeyin güvenliği demektir. Devletler, bireyler, kısacası hayatın reel faaliyette olan neyi varsa artık bilgi üzerinden işlevsel faaliyet yürütmekte ve wired, wireless networks’leri da bu bilgileri taşımak, göndermek vs. gibi kritik işlemler için kullanmaktadır. Bu yüzden günümüzde güvensiz bir kablolu, kablosuz ağ teknolojisi düşünülemez.

Günümüzde, wired, wireless networks’lere yönelik tehditler, güvenliği tahrip eden ve etmeye çalışan en kritik unsurlardır. Hırsızlıklar, kritik devlet bilgileri ve kişisel bilgilere sızma gibi ciddi zarar verici eylemler, bu tehditler kullanılarak gerçekleştirilmekte ve ne yazık ki bu tehditler gün geçtikçe hem yöntemsel hem de şekilsel olarak daha kompleks hale getirilerek art niyetli kişilerce geliştirilmektedir.

Hem diğer bölümlerde hem de yukarıda birçok kez bahsedildiği gibi, bu kadar hayati vasıflara sahip olan wired, wireless networks’lerin güvenliği ve onlara yönelik tehditler açısından şu günün dünyasında çok kritiktir. Bu tez de araştırma konusu olarak bu konuyu ele aldığı için, gerek farkındalık yaratma adına, gerek bilgi kaynağı olmak adına kritik esaslar içermektedir. Dünya, artık bilgisayar, internet ve bilgi üzerine kurulu olduğu için, tüm bu bilgi ağının alt yapısı olan wired-wireless networks’lerin güvenliği ve onlara yönelik tehditler konulu bu tez birçok anlamda faydalı ve hayati bir araştırma projesidir.

## 1.4 Wired and Wireless Network’lerde Fiziksel Güvenlik:

Günümüzde, wireless network’lerin wired network’lerden çok daha fazla rağbet gördüğü ve hızla büyüdüğü bir dönemi yaşıyoruz. Wireless network erişim cihazlarının maliyetlerinin düşmesi, wireless network’lerin performansının kablolu ağlara yaklaşması, kullanımı daha da artıyor.  
 Ancak wireless network’lerde fiziksel bir bağlantı olmadığı için güvenlik boyutu da değişiyor. Wireless Network’lerdeki en temel güvenlik problemi, verilerin havada uçuşmasıdır. Konumlandırılan erişim noktalarının dağıtık ve bir yapıda olması, fiziksel güvenliğin sağlanmasının zor olması nedeniyle kablolu ağ ekipmanlarına göre daha fazla tehdit altındadır. Kullanıcılara, bu bağlamda wireless area networks’lerin sağladığı esneklikten daha verimli ve güvenli bir şekilde yararlanabilmesi için çok katmanlı güvenlik çözümleri sunulmaktadır.

Wired ve wireless network’lerde fiziksel güvenlik konusu kapsamında ayrıca, bilgisayar veya aktif cihazlara fiziksel olarak erişebilen saldırganın cihazın kontrolünü kolaylıkla ele alabileceği gerçeği de unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan, kabloya özel ekipmanla erişerek (tapping) hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal güvenlik önlemlerinin hiç bir kıymeti bulunmamaktadır. Kurumun ağını oluşturan ana cihazlar ve hizmet sunan sunucular için alınabilecek fiziksel güvenlik politikaları kurum için belirlenmelidir.

Bu bölüm kapsamında, wired ve wireless network’lerin öncelikle ayrıntılı yapısı ele alınacak, daha sonra fiziksel güvenlik konusu üzerinde durularak alınabilecek önlemler ele alınacak, sonrasında ise ayrıntılı fiziksel güvenlik kavramlarından bahsedilerek bölüm sonlandırılacaktır. [48][47]

## 1.5 Wired and Wireless Network’lerde Güvenlik İlkeleri ve Kavramları

Bir organizasyonun güvenlik gereksinimlerini, kavram ve ilkelerini tanımlamak önemlidir. Güvenlik ihtiyaçlarının üç ana kaynağı vardır;

- Birinci kaynak organizasyon için risklerin değerlendirilmesinden sağlanır. Risk değerlendirmesi ile varlıklar için riskler belirlenir ve tehditler tanımlanır.

- İkinci kaynak firmaların ve servis sağlayıcıların ticari ortakları ile yerine getirmesi gereken yasal, resmi, düzenleyici şartlar ve bir organizasyonun sözleşme şartlarıdır.

- Üçüncü kaynak bir organizasyonun faaliyetlerini desteklemek amacıyla bilgi işleme için hedefler, şartlar ve ilkelerin özelleştirilmesidir.

Saldırılar ve zafiyetler karşısında, bilgi güvenliğini sağlamak için bu güvenliği oluşturan unsurların belirlenmesi gereklidir. Bu unsurların yokluğu veya bu unsurlarda oluşabilecek zafiyetler, doğrudan oluşturulmak istenen güvenliğin etkinliğini belirleyecektir.

Bilgilerin, istenmeyen hasarlardan korunması için, en temel açıdan atılması gereken adımlar, güvenlik unsurlarının yerine getirilmesi ile sağlanmaktadır.

Bilgi güvenliği çerçevesinde kurulacak güvenlik sistemi altyapısının ve politikasının doğru bir şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik yönetiminin doğru ve eksiksiz bir şekilde yapılması gerekir. Güvenlik yönetimi, bilgi ve bilgisayar güvenliğini olumsuz yönde etkileyecek faktörlerin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.

Confidentiality, integrity, availability, authentication venon-repudiation bilgi güvenliğinin en temel unsurlardır. Bunun dışında accountability, access control, reliability, Network Security Monitoring (NFC) ve safety etkenleri de bilgi güvenliğini destekleyen unsurlardır. Bu unsurların tamamının gerçekleştirilmesiyle ancak bilgi güvenliği tam olarak sağlanabilecektir. Şekilden de görülebileceği gibi, bu unsurların bir veya birkaçının eksikliği, güvenlik boyutunda aksamalara sebebiyet verebilecektir. Bu unsurların birbirini tamamlayıcı unsurlar olduğu hiçbir zaman unutulmamalıdır.

**Accountability**, belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirleme yeteneğidir. Tipik olarak etkinliklerin kayıtlarını tutmak için bir logging sistemine ve bu kayıtları araştıracak bir hesap auditing sistemine ihtiyaç duyar.**Access Control**, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir. **Reliability**, bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir. **Safety**, bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda, kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları önleme tedbirlerini içermektedir. **Network Security Monitoring(NSM)**,  ağ üzerindeki bir sunucuya gelen ve sunucudan giden paketleri yakalayarak bu paketlerin istatistiklerini çıkartır. Bunun yanında, Network Monitor yardımıyla ağ trafiğinizi analiz edip, meydana gelen problemlerin sebeplerini bularak sorunları çözer. Şimdilik basit ve genel anlamda ön bilgileri verilen bu kavram ve ilkeler ilerde ayrıntılı biçimde bu bölümünde ele alınacaktır.[46][45]

## 1.6 Wired and Wireless Network’lerde Bilişim Güvenliği

Bilgi, günümüzde haberleşme kanalları olan wired ve wireless olarak ağlar üzerinden paylaşılabilmekte ve iletilebilmektedir. Wireless iletişim kanallarının kullanımı oldukça yaygınlaşmakla birlikte bilginin istenilmeyen kişiler tarafından kötü amaçlı kullanımı da yaygınlaşmakta, güvenlik zafiyetleri ise artmaktadır.

Wireless network yapıları itibariyle wired network’e göre daha güvensiz olup çeşitli zafiyetleri de beraberinde taşımaktadır. Wired network’de ise bilgiler kablolar vasıtasıyla iletildiğinden daha güvenli iletilebilmektedir. Kullanımda ise wireless network’lerde verilerin erişim noktasından aktarılıyor olması nedeniyle bilgiye erişimi kolaylaşır. Wireless network’ün kullanımın kolay ve yaygın olması bununla birlikte barındırdığı zafiyetlerin çeşitli bilgi güvenliği tehditleri ile karşı karşıya kalması kaçınılmazdır. Kurum ve bireyler için önemli ve sürekli korunması gereken varlık olan bilgi ise olası kötü amaçlı saldırılar karşısında savunmaya muhtaç hale gelir.

Wireles networks’de, bilgi güvenliğinin üç temel prensibi olan gizliğin, bütünlüğün ve erişilebilirliğin sağlanması noktasında öncelikle; SSID kullanımı, kimlik doğrulama mekanizmaları, MAC adres filtreleme ve kablosuz 5 şifreleme teknolojileri gibi sistemsel özel güvenlik kontrolleri uygulanmalıdır.

Bu güvenlik tedbirlerine paralel olarak güvenlik en zayıf halkasını oluşturan insan faktörü hiçbir zaman unutulmamalı ve bireyler üzerinde belirli bir bilgi güvenliği farkındalığı sağlanmalıdır. Her ne kadar sistemler üzerinde gerekli güvenlik önlemleri alınsa bile kullanıcılar bu konuda bilinçlendirilmedikçe gerçek anlamda güvenlik hiçbir zaman sağlanmayacaktır.

TÜBİTAK Türkiye’de kablosuz internet ağı kullanan 30 bin bilgisayar üzerinde yaptığı araştırmaya göre, kullanıcıların yüzde 5’nin şifre kullanmadığı ve bilgisayarların yarısında ADSL modemlerin yönetim ara yüzüne dışarıdan ulaşılabildiği görülmüştür.

Bu tür araştırmalar ya da günümüzde her geçen gün artan bilgi güvenlik olayları kullanıcılarda farkındalık oluşturulmasının gerekliliği gösterir. Bu doğrultuda, kurumlar öncelikli olarak kurumsal bilgi güvenlik politikalarını oluşturmalı, kurumun en üst düzey yönetiminin onayından geçirmeli, güvenlik kural ya da yönergelerini hazırlamalı, bilgi güvenliği farkındalığını arttırmaya yönelik belirli aralıklarla eğitimler, seminerler düzenlemeli ve işleyişi gözlemleyerek sürekli iyileştirmeler yapmalıdır.

Düzenlenen bu farkındalık eğitimlerde; bilgi güvenliği temel kavramları, kurum beklentileri, yaşanılmış ya da yaşanması muhtemel tehditler, riskler ve bu riskleri önleyici kontroller, bilgi güvenliği olayları ve bunların kurumlara ya da bireylere verebileceği zararlar hakkında güncel örneklerle örneklendirilerek anlatılmalı ve sürekli farkındalık seviyesi yükseltilmelidir. Bireyler uğrayabilecekleri bilgi güvenlik saldırıları hakkında da bilgilendirilmelidir.

Bu bölümde, tüm bu durum ve etkenler göz önüne alınarak Risk Yönetimi, Security politika ve standartlar, Kriptografi, Sayısal İmza, Firewall, Backup, Saldırı türleri ve tespitleri, Access Control ve Virus/Trojan/Worm, Sosyal Mühendislik ve Güvenlik önlemleri gibi konular spesifik olarak ayrıntılı biçimde bu bölümde ele alınarak işlenecektir.[44] [43] [42][41]

## 1.7 Wired ve Wireless Network’lerde Güvenlik Teknolojileri ve Protokolleri

Günümüzde gelişen ağ iletişim teknolojilerine paralel, kablosuz iletişim sistemlerinin kullanımları da hızla artmaktadır. Buna bağlı olarak kablosuz iletişim sistemlerindeki veri güvenliğini sağlamak önem kazanmaktadır. Bu çalışmanın temel amacı, kablosuz iletişim sistemlerindeki güvenlik protokollerini karşılaştırarak farklı uygulamalar için en uygun olanlarını tespit etmektir.

Wireless Sensor Networks (WSN), sınırlı kapasiteli, kısa mesafede kablosuz ortam üzerinden haberleşebilen düşük güçlü ve düşük maliyetli algılayıcı düğümlerinden meydana gelmektedir ve bu özellikleriyle genel kablosuz sistemler içerisinde ayrı bir öneme sahiptir. Gözlem yapılacak ortama rasgele dağıtılabilen bu düğümler, birbirlerini tanıyabilmekte ve ortak gayret sarf ederek geniş bir alanda ölçüm vazifesini gerçekleştirebilmektedir. Bu avantajlarından dolayı sağlıktan askeri uygulama alanlarına, bir binanın güvenliğinin sağlanmasından orman yangınlarının önceden tespitine kadar çok çeşitli şekillerde kullanılabilmektedirler. Güvenlik teknolojileri ve protokolleri, kablolu veya kablosuz her türlü ağ için oldukça önemli bir konudur. Klasik bir kablolu ağ üzerinden iletişim, fiziksel kablolar üzerinden sağlanır ve güvenlik, genellikle fiziksel altyapıda dahili olarak bulunur. Wireless Network’lerde  ise çoğunlukla RF sinyalleri kullanılır ve bu nedenle aynı güvenlik önlemlerinin uygulanması mümkün olmayabilir. Wireless kullanıcılarının ve verilerinin, bilgisayar korsanlarının saldırılarına, kurumsal casusluğa karşı daha güvenli hale getirilmesi için çeşitli güvenlik özelliklerinden yararlanılır.

Wireless network’lere özgü çeşitli güvenlik tedbirleri bulunmaktadır. Bunların başlıcaları, SSID kullanımı, cihaz kimlik doğrulama mekanizmaları, MAC adresi filtreleme ve şifreleme teknolojisi olan WEP şeklinde sıralanabilir. Wireless Sensor Networks (WSN) düğümlerinin sınırlı donanımsal kaynaklara ve güç birimlerine sahip olması, bazı çözüm bekleyen güvenlik açıklarını da beraberinde getirmektedir. Ortam erişim protokolünün açıklarından faydalanarak algılayıcı düğümlerin iletişimlerinin kesilmesine ya da anormal durumların oluşmasına ve böylece ağ ömrünün kısalmasına sebep olan hizmet engelleme (Denial of Service-DoS) saldırıları, kablosuz algılayıcı ağ güvenliği için önemli bir tehdit unsuru oluşturmaktadır. Wireless Sensor Networks (WSN) için tasarlanan ortam erişim protokolleri arasında en yaygın olarak bilinen S-MAC (Sensor Medium Access Control ) ve türevleri (T-MAC, D-MAC v.b.) bu tür saldırılara karşı savunmasızdır. Dolayısıyla güvenlik protokollerine ihtiyaç duyulmaktadır.

Tez çalışmasının bu bölümde, wired ve wireless network’lerde, güvenlik teknoloji ve protokolleri üzerinde durulacak, Authentication, IEE-802.11 protokolleri, WEP, WPA, RSN, LEAP, LISP, SNEP, MIC, TKIP, SSL, CBC MAC protokol ve TLS gibi teknolojik/protokol kavramları üzerine spesifik bir araştırma ele alınacaktır.

## 1.8 Wired ve Wireless Network’lerde Çalışma Grupları, Uluslararası Standart Belirleyen Kurumlar

Son 20-30 yıl içerisinde bilgisayarlardaki gelişmenin yanı sıra bilgisayar ağlarında da çok büyük gelişmeler yaşandı. İlk yıllarda her üretici kendine ait bir standart geliştiriyordu. Bu da birbiriyle uyumsuz birçok bilgisayar ağının oluşmasına sebep oldu. Böyle problemleri ortadan kaldırmak amacıyla ISO (International Standarts Organization) tarafından bir ağ modeli geliştirme çalışmaları başlatıldı ve bu çalışmalar sonucunda OSI (Open System Interconnection ) referans modeli yayınlandı. Bütün ağ protokollerinde bu modelin kullanılması zorunlu kılındı.  
Ağ protokollerinde genel olarak aşağıdakiler tanımlanır;

* Fiziksel arayüzler, sinyal düzeyleri ve kodlama
* Ağ adresleri, bağlantı kurma/kesme
* Ağ veri birimlerinin büyüklüğü ve yapısı
* Hata kontrolü
* Başarılı alındı belgesi
* Akış denetim mekanizmaları
* Veri tabanı alanları ve formatları
* Uygulamaya özgü anlamlar

Ağ standartları da bazı kurum ve komiteler tarafından oluşturulmaya başlandı ve genel anlamda bu standartlar kabul edildi. Bu bölümde, wired, wireless network’lerde çalışma gruplarını, uluslararası düzeyde standart belirleyen kurumları ele alıp, belirledikleri standartlar üzerinde durulacaktır.

## 1.9 Sonuç

Bu bölümde, artık tez ile ilgili genel bir değerlendirmede bulunulup, eksik görülen ve ya çalışma bazında yetersiz olduğu düşünülen konular ele alınacaktır. Bu çalışma, bundan sonra bu konu üzerine çalışacak olan kurum ve ya kişilere bir alt kaynak oluşturacak, bu bölümde eksiklikleri saptanan konularla çalışmanın geliştirilerek kapsamlaştırılması adına bir temel araştırma projesi olarak sunulacaktır.

# BÖLÜM 2: WIRED, WIRELESS NETWORKS ve FİZİKSEL GÜVENLİK

## 2.1 WIRELESS NETWORKS

### 2.1.1 Wireless Technologies

Kablosuz iletişim, kablolu iletişimin yanı sıra bir noktadan başka bir noktaya kablo hattı kullanmadan veri, ses veya görüntü taşınmasına denir. Buna göre kablosuz iletişimi kablolu iletişimden ayıran önemli nokta, iletim ortamı olarak havanın kullanılmasıdır.

Modern kablosuz iletişim, Heinrich Rudolph Hertz’in radyo dalgası olarak bilinen elektromanyetik dalgaları keşfetmesiyle 1800’lü yılların sonunda başlar. Guglielmo Marconi 1901 yılında radyo dalgalarını kullanarak Atlantik Okyanusu’nun karşısına kablosuz telgraf ile mesaj göndermiştir. 1920’de radyo, telgraf ve radyo telefonlar kullanılmaya başlanmıştır.

1940’lı yıllarda yapılan gelişmiş radar sistemiyle kısa dalga boyları kullanılarak radyo mesajlarının taşınması gerçekleşmiştir. Dalga boyu küçük olan bu dalgalar günümüzde mikrodalga olarak bilinir. Mikrodalgalar, daha çok bilgiyi daha büyük hızla ve daha güvenilir taşımayı mümkün kılar. Daha sonra geliştirilen “Spread spectrum” teknolojisi ile veriler daha güvenli olarak taşınmaya başlanmıştır. 1950’li yıllarda radyo tabanlı “paging system” ile radyo teknolojisi kullanarak kıtalar arasında ses ve telgraf alışverişi gerçekleştirilir.

1983 yılında hücresel telefonların çıkması ile kablosuz ağ teknolojileri kullanıp gruplar hâlinde bilgisayarların birbirlerine bağlanması için yeni sistemler geliştirilir. Bununla birlikte “IEEE” standartları ortaya çıkar.

Her yeni teknolojinin gelişmesiyle kişilerin yaşama şekillerini değiştiren ilerlemeler meydana gelmiş. Bu bağlamda günümüzde kablosuz erişim teknolojisi ile çalışan taşınabilir bilgisayar, masaüstü bilgisayar, el bilgisayarı, PDA (Personel Digital Assistant), cep telefonu, kalemli bilgisayar ve çağrı cihazları gibi aygıtlar kullanılır hâle gelmiştir. [1][2]



Şekil 2.1.1: Wireless Communication

#### 2.1.1.1 Wireless Çeşitleri

Wireless networks kullanım amaçları ve büyüklüklerine dört kategoriye göre ayrılmıştır fakat wireless networks, wired networks gibi net bir biçimde tanımlanmış sınırları yoktur. Wireless iletimin aralığı birçok etmene bağlı olarak değişiklik göstermektedir. Hava koşulları ve girişimler kablosuz ağın kapsamını büyük ölçüde değiştirebilir.[14][22][4]

##### 2.1.1.1.1 Wireless Personal Area Network (WPAN)

İletişim gereksinimlerinin karşılanması birçok alanda büyük önem taşımaktadır. Bu gereksinimlerin karşılanması amacıyla iletişim teknolojileri geliştirilmektedir. IEEE (Institute of Electrical and Electronics Engineers) iletişim teknolojilerinin oluşturulması ve geliştirilmesi konusunda çalışmalar yapmaktadır. WPAN (Wireless Personal Area Network) IEEE organizasyonunun veri iletişimi standartlarından biridir ve 802,15 standardı olarak bilinir.

WPAN, temel olarak kablosuz bağlantı kullanılarak oluşturulan kablosuz kişisel alan ağıdır. WPAN, 10 metreye kadar olan mesafelerde veri iletişimine olanak tanıyan bir iletişim teknolojisi standardıdır. IEEE 802,15 (WPAN) standardı tüm sıradan bilgisayar ve iletişim cihazlarının birbirlerine kablosuz olarak bağlanabilmesine olanak sağlar, buradaki temel nokta cihazlar arası uzaklığın yeterli olması ve cihazların aynı kablosuz kişisel ağda olmaları gerektiğidir.

WPAN standardı kullanılarak kablosuz veri iletişimi şekildeki gibi gerçekleştirilebilir.



Şekil 2.1.1.1.1: Wireless Personal Area

WPAN standardının kullanıldığı teknolojilerin başlıcaları ZigBee, Ultra-Wideband(UWB), Bluetooth ve Home RF’dir. [3] [32] [4]

###### 2.1.1.1.1.1 ZigBee

ZigBee, WPAN oluşturmak için kullanılan bir iletişim teknolojisidir.  Bu iletişim teknolojisi, WPAN oluşturulurken 868 Mhz, 902-928 MHz ve 2,4 GHz hızlarda kullanılır. ZigBee kullanımında; veri haberleşmesi yapan cihazlar arası uzaklık en fazla 50 metre olmalıdır. Veri aktarım hızı en fazla 250 kbps (kilobit per second) olmaktadır. ZigBee, IEEE 802.15.4 standartı olarak bilinmektedir. ZigBee görev döngüsü düşük olduğu için uygulamalarda yüksek veri aktarımı sağlar. Bu durum ZigBee kullanımını, kontrol cihazlarının ve sensörlerin yaygın olarak kullanıldığı ev, iş ve endüstriyel otomasyon alanlarında ideal kılar. ZigBee peer-to-peer, star ve mesh ağ topolojilerine uyumludur. ZigBee bir kablosuz kişisel alan ağında 255 adete kadar cihaz iletişimi sağlayabilir. [3] [32]

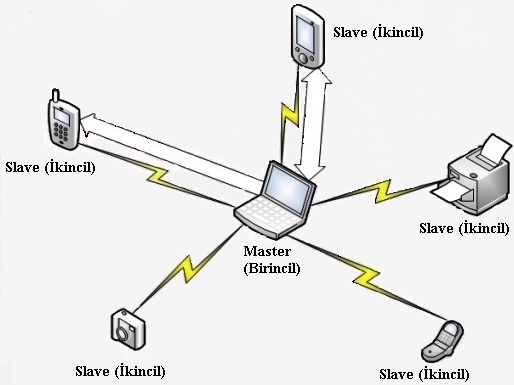
###### 2.1.1.1.1.2 Ultra-Wideband (UWB)

UWB kısa bir mesafe için frekans bandı çok geniş bir yelpaze üzerinden, düşük güç ile büyük miktarda dijital veri aktarımı için kullanılan kablosuz veri aktarım teknolojisidir. UWB teknolojisi ile veri aktarım hızı başlangıçta 40-60 mbps hızında iken veri aktarımı sırasında 1 gbps hızına kadar çıkabilmektedir. UWB, çok kısa bir elektrik akımı ile düşük güçte radyo sinyalleri yayar. UWB alıcıları vericiler tarafından gönderilen tanımlanmış darbe dizilerine bakarak, alınan sinyalleri verilere çevirebilmektedir. [3] [32]

###### 2.1.1.1.1.3 Bluetooth

Bluetooth kısa mesafelerde güvenlik düzeyi yüksek olan kişisel alan ağları yaratarak sabit ve mobil cihazlar arasında veri alışverişi için kullanılan özel bir açık kablosuz teknoloji standartıdır. Bluetooth, kablo bağlantısını ortadan kaldıran kısa mesafe RF teknolojisi esasına dayanır. Bluetooth; bilgisayar, çevre birimleri ve diğer cihazların birbirleri ile kablo bağlantısı olmadan görüş doğrultusu dışında bile olsalar haberleşmelerine olanak sağlar. Bluetooth teknolojisi 2.402-2.480 ghz ISM (Industrial Scientific Medical) frekans bandında çalışmakta olup, ses ve veri iletimi yapabilmektedir. 721 kbps'a kadar veri aktarabilen bluetooth destekli cihazların etkin olduğu mesafe yaklaşık 10 ile 100 metredir. Bluetooth teknolojisi ilk olarak 1994 yılında kullanılmıştır. Bluetooth teknolojisi başlangıçta kablosuz olarak RS-232 veri kablosuna alternatif olarak tasarlanmıştır. Bluetooth, frekans atlamalı yaygın spektrum denilen radyo dalga teknolojisini kullanır ve master-slave yapıya sahip paket tabanlı bir protokoldür. [3] [32]

Bluetooth uygulamaları şekildeki gibi gösterilebilir



Şekil 2.1.1.1.1.3: Bluetooth Uygulamaları

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1.1.1.1.3.1 Bluetooth'un Genel Özellikleri |  |  |  |

* Frekans Aralığı 2.402-2.480 gHz
* Veri Oranı 1 mbps
* Kanal Band Genişliği 1 mHz
* Menzil 10-100 Metre
* Frekans Atlama 1600 kez / sn
* Şifreleme 48bit cihaz ID ve Eo 128bit şifreleme
* IEEE Standartları 802.15.1-802.15.2-802.15.3-802.15.4

2.1.1.1.1.3.2 Bluetooth Sürümleri

2.1.1.1.1.3.2.1 Bluetooth Sürüm 1.1 ve Öncesi

Bluetooth teknolojisi, 1998 yılında tanıtıldığından bu yana birkaç bluetooth sürümü yayımlanmıştır. Sürüm 1,0 ve 1.0B, üreticilerin bluetooth cihazları başarılı bir şekilde geliştirmelerine engel olacak problemler ve sınırlamalar içeriyordu. Temel sorun cihazların birlikte çalışabilirliklerinin eksikliğiydi. Bluetooth sürüm 1,1 bluetooth teknolojisinin gerçek anlamda ilk başarılı işletim sürümüdür. Bluetooth sürüm 1,1’de önceki sürümlerinde bulunan sorunların çoğunu düzeltilmiştir.

2.1.1.1.1.3.2.2 Bluetooth Sürüm 1. 2

Sürüm 1,2, sürüm 1,1 ile uyumludur ve ek özellikleri aşağıdaki gibidir;

* + Daha hızlı bağlantı ve cihaz bulma özelliği
  + Adaptif Frekans Atlamalı Yaygın Spektrum
  + Daha hızlı veri aktarım hızı (1 Mbps)
  + Alınan Sinyal Gücü Göstergesi
  + Genişletilmiş Senkron Odaklı Bağlantılar

2.1.1.1.1.3.2.3 Bluetooth Sürüm 2.0 +EDR (Enhanced Data Rate)

Bluetooth sürüm 2,0 + EDR özelliği üç kat kadar daha hızlı transfer hızı sağlar. Bluetooth sürüm 2,0 + EDR çok bağlantı imkânı sağlar. Sürüm 2,0 + EDR özellikleri aşağıdaki gibidir;

* Önceki Bluetooth sürümleriyle uyumlu
* Üç kat daha hızlı aktarım hızı (bazı durumlarda 10 kat)
* Improved data rate (3 Mbps)
* Azaltılmış görev döngüleri nedeniyle daha düşük güç tüketimi
* Broadcast/multicast desteği
* Media access control protocols
* Daha gelişmiş bit hata oranı özelliği
* Çoklu bağlantıların daha fazla kullanılabilir bant genişliğiyle basitleştirilmesi

2.1.1.1.1.3.2.4 Bluetooth Sürüm 2.1 +EDR (Enhanced Data Rate)

Bluetooth sürüm 2,1 + EDR ile uyumludur. Gelişmiş özellikleri aşağıdaki gibidir;

* + Gelişmiş eşleştirme özelliği
  + Gelişmiş güç optimizasyonu

2.1.1.1.1.3.2.5 Bluetooth Sürüm 3.0 +HS (High Speed)

Bluetooth sürüm 3.0 + HS önceki sürümlerle uyumludur. Kullanıcıların Bluetooth sürüm 3.0 + HS kullanarak yararlanacakları önemli özellikler şunlardır;

* Unicast Bağlantısız Veri. (Gecikmeyi en aza indirir ve daha hızlı daha güvenilir deneyimler sunar)
* Enhanced Power Control.  (Bluetooth kullanıcılar arasında bağlantı kopmalarını en aza indirir.)
* Alternatif MAC / PHY. (Bluetooth profil verisi taşımak için alternatif  
   MAC ve PHY kullanımını sağlar)
* Wi-Fi hızı ile veri aktarma
* Düşük enerji tüketimi

2.1.1.1.1.3.2.6 Bluetooth Sürüm 4.0 +HS (High Speed)

Bluetooth teknolojisi son sürümü olan 4.0 önceki sürümlerle uyumludur. Son sürüm özellikleri aşağıdaki gibidir;

* + Genişletilmiş çekim alanı (100 metreye kadar)
  + Wi-Fi tabanlı yüksek veri iletim hızı (24 Mbps)
  + Oldukça düşük güç gereksinimi
  + AES-128 (Advanced Encryption Standard)   
     güvenlik desteği getirilmiştir.

###### 2.1.1.1.1.4 Home RF

HomeRF, genel olarak küçük ofis ve ev ihtiyaçları için düşünülmüş kablosuz erişim standardıdır. 2.4 GHz ISM bandında çalışmaktadır. HomeRF’nin IEEE 802.11x standartlarına göre güçlü yanı veri aktarımının yanı sıra ses desteğinin de olmasıdır. Tablo 2.1.1.1.1.4’ de homeRF’ nin genel özellikleri verilmiştir. Bakınız. [3] [32]

|  |  |
| --- | --- |
| **Frekans Aralığı** | 2.402 – 2.480 GHz |
| **VERİ ORANI** | 10 Mbps (v.2 için) |
| **MESAFE** | ~100 metre |
| **RF ATLAMA** | 50 kez/s |
| **TX ÇIKIŞ GÜCÜ** | Azami 20 dBm (01.W) |

Tablo 2.1.1.1.1.4: Home RF Frekans Aralık Tablosu

HomeRF’ in katmanlı bir mimarî yapısı vardır. Fiziksel katmanın üzerinde ethernet, ses ve veri akışı için ayrı ayrı teknikler vardır. Ethernet için CSMA/CD, veri akışı için CSMA ve ses için TDMA kullanır.

HomeRF 2.0 sistemlerinde FHSS modülasyon tekniği kullanılmaktadır. Bu teknikte veri kanalı bir frekanstan diğerine saniyede 50 defa atlamaktadır. Bu teknoloji iletişimin izlenmesini ve verilerin çalınmasını oldukça zorlaştırmaktadır. Ayrıca ağa giriş için “ağ şifresi” istenerek güvenlik artırılmaktadır.

HomeRF ne için kullanılabilir sıralayalım:

* Bilgisayarlar arası kablosuz ağ kurulabilir.
* Evin içinde ve etrafında taşınabilir aygıtlar ile internete bağlanılabilir.
* Çok bilgisayarlı ortamda dosya, modem, yazıcı paylaşımı sağlanabilir.
* Sadece PC uyumlu el setine konuşarak ev elektronik sistemi aktif hâle getirilebilir.

##### 2.1.1.1.2 Wireless Local Area Network (WLAN)

WLAN (Wireless Local Area Network), iki yönlü geniş bant veri iletişimi sağlayan, iletim ortamı olarak kablo yerine RF veya IR ışınları kullanan ve bina, kampüs gibi sınırlı alanda çalışan iletişim ağlarıdır.

Kablosuz yerel alan ağları genellikle kablolu yerel alan ağın sınırlarını genişletmek için kullanılır. Bu ağlar IEEE 802.11 standartlarına göre çalışır. WLAN sistemleri kullanıcılara kablosuz geniş bant internet erişimi, sunucu üzerindeki uygulamalara ulaşım, aynı ağa bağlı kullanıcılar arasında elektronik posta hizmeti ve dosya paylaşımı gibi çeşitli imkânlar sağlamaktadır.

WLAN sistemlerinin mesafesi 25-100 metre civarındadır. Dünyada yaygın olarak kullanılan iki tür WLAN teknolojisi mevcuttur. Bunlardan birisi Amerika tabanlı IEEE 802.11x, diğeri ise Avrupa tabanlı HiperLAN sistemleridir. [3] [10] [11] [32]



Şekil 2.1.1.1.2: Wireless Local Area Network (WLAN)

Wireless Local Area Network, Avrupa düzenlemelerinde RLAN (Radio Local Area Network), ABD ve birçok ülkede Wi-Fi (Wireless Fidelity), Wireless Local Area Networks, WLAN olarak isimlendirilir.

Wired Local Area Network’ların tüm özelliklerine sahip olan Wireless Local Area Network sistemleri Wired Network’ların devamı ya da alternatifi olarak kullanılmaktadır. Wireless Local Area Network sistemleri işletmeler, kafeler, kütüphaneler, okullar ve kampüs gibi birçok alanda bireysel kullanıcılara ağa bağlanma imkânı sağlamaktadır.

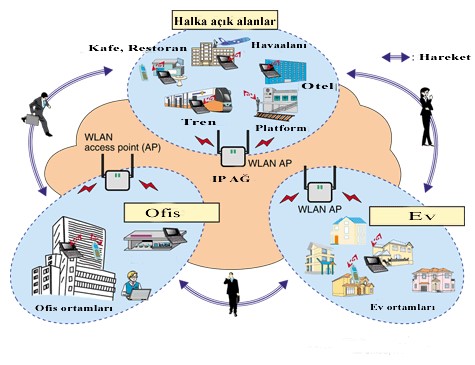
Wireless Local Area Network’ların kullanımıyla birçok avantaj elde edilir. Bu avantajlar bina içi ve binalar arası avantajlar olarak ayrılabilir.

Bina içinde;

* **Hareketlilik:** Wireless Local Area Network sisteminde bilgisayarları sabitlemeye ihtiyaç duyulmaz. Dolayısıyla kullanıcıların hareket özgürlüğü sağlanır ve iş verimliliği artar.
* **Kurulum hızı ve esnekliği:** Wired Network kurulumundan önce gerekli olan kablolama planı ve kablolama işlemi için belli bir zaman harcanır. WLAN sisteminde bu işlemlere gerek olmadığı için zamandan tasarruf edilmiş olup sistemin kurulumu hızlandırılmış olur. Ayrıca kablo çekmenin zor olduğu yerlerde ağa kolay erişim imkânı sağlar.
* **Düşük maliyet:** Wireless Local Area Network kurulacak sisteme göre değişmekle birlikte genellikle Wired Network’a göre daha düşük maliyetlidir. Çünkü kablo maliyeti ve kablolama işçiliği ücreti yoktur.
* **Ölçeklenebilirlik:** Kullanıcı sayısının sabit olmadığı ortamlarda (kampüs, kütüphane, restoran, konferans salonu vb.) her yerden internet erişimi sağlanabilir. Sisteme kullanıcıların katılımı sırasında ilave malzeme ve iş yükü gerektirmediğinden istenilen sayıda ağ genişletilebilir.

Binalar arasında;

* 11 Mbps hızında hızlı bağlantılarla kablolu ağlara alternatif olmaktadır.
* Sabit iletişim/bakım giderleri en az düzeydedir.
* 128 bit şifreleme ile iletişim güvenliği sağlar.
* Dağınık yapıya sahip işletmeler veya kampüsler için binalar arası kablosuz bağlantı gerçekleştirilebilir.



Şekil 2.1.1.1.2.a: Wireless Local Area Network’ların kullanım alanları

Wireless bağlantının esnekliğine ve avantajlarına rağmen bazı sınırlamaları ve riskleri vardır. Wireless Local Area Network’ların dezavantajları şunlardır:

* **Girişim (enterferans):** Wireless Local Area Network teknolojileri elektromanyetik tayfın lisanssız bölgelerini kullanır yani bu bölgeler düzenlenmemiş nitelikte olduğundan birçok farklı sinyal bu bölgeleri kullanır. Sonuç olarak bu bölgeler tıkanır ve kablosuz telefonlar, mikrodalgalar gibi farklı aygıtlardan gelen sinyaller ağa girişimde bulunabilir.
* **Ağ ve veri güvenliği:** Wireless Local Area Network teknolojisi, iletilmekte olan verilerin güvenliğini sağlamak için değil o verilere erişimi sağlamak için tasarlanmıştır. Wireless bağlantının bu özelliği, istenmeyen alıcıların (istemci) da iletişim akışına müdahale etmesine dolayısıyla güvenlik tehditlerinin oluşmasına neden olur. Wireless Local Area Network’larda güvenlik tehditlerini önlemek amacıyla encryption ve authentication gibi teknikler geliştirilmiştir.
* **Teknoloji:** Wireless Local Area Network teknolojisi gelişmeye devam etmektedir. Wireless Local Area Network teknolojisi şu an için Wired Network’ların sağladığı hızı ve güvenirliliği sağlamamaktadır. [3] [10] [17] [19] [11]

###### 2.1.1.1.2.1 Kablosuz Yerel Alan Ağ Standartları

Kablosuz teknik standartların oluşturulmasından sorumlu olan ana kuruluş IEEE (Institute of Electrical and Electronics Engineers)’dir. IEEE, LAN ve MAN ağlar için 802.x adı altında bir seri standart yayınlamıştır. Wireless Local Area Network, ağlar için ise 1997 yılında 802,11 standardı yayınlanmıştır.

802.11 standardı, 2,4 GHz bandında FHSS (Frequency Hopping Spread Spectrum) ve DSSS (Direct Sequence Spread Spectrum) tekniklerinde 2 Mbps’e kadar veri iletişimi sağlamaktadır. Bu ilk standardın amacı var olan wired LAN’ların, wireless olarak genişlemesini sağlamaktır.

IEEE, bu temel standardı daha yüksek veri iletim hızı, daha iyi servis kalitesi vb. ihtiyaçları karşılamak üzere geliştirmeye devam etmiştir. Geliştirilen yeni standartlar, 802.11x adı ile tanımlanmış olup x bir harfi temsil etmektedir. 1999 yılında sırasıyla 802.11a ve 802.11b standartlarını duyurmuştur. Daha sonra 2003’te 802.11g ve 2009’da 802.11n standartları yayınlanmıştır. Bu standartlar farklı şekilde, farklı alanlarda kullanılmaktadır.

802.11b, g ve n standartlarına genel olarak Wi-Fi denir. Wi-Fi Alliance olarak bilinen bir kuruluş da farklı üreticilerin Wireless Local Area Network aygıtlarının test edilmesinden sorumludur. Bir cihazdaki Wi-Fi logosu, o ekipmanın standartları karşıladığı ve aynı standartlara sahip diğer cihazlarla birlikte çalışabileceği anlamına gelir. [3] [10] [17] [24] [35] [22] [12]

2.1.1.1.2.1.1 IEEE 802.11x Standartları

8021.11x ailesi IEEE tarafından Wireless Local Area Network uygulamaları için tanımlanmış standartlar kümesidir. 802.11x standardında ilk olarak 1 veya 2 Mbps’lik çalışma hızları ön görülmüşse de daha sonra geliştirilen 802.11b ve 802.11a standartlarında çalışma hızları 11 Mbps, 54 Mbps’e kadar çıkarılmıştır.

Verilen bu hızların, Wireless Local Area Network için brüt hızlar olduğu aslında veri aktarımının daha az olduğu unutulmamalıdır. Yani, yararlı veri aktarım miktarı da önemlidir. Bu sebeple wireless cihazları birbirleriyle karşılaştırılırken aktarım başarımı da göz önüne alınmalıdır. Tablo 2.1.1.1.2.1.1’de 802.11x standartlarının fiziksel aktarım oranı (brüt aktarım oranı) ve veri aktarım oranı (net aktarım oranı) verilmiştir. [28] [35] [12]

|  |  |  |  |
| --- | --- | --- | --- |
| **Özellik** | **802.11** | **802.11a** | **802.11b** |
| Brüt Aktarım Oranı | 2 Mpbs | 54 Mpbs | 11 Mpbs |
| Net Veri Oranı | 1,2 Mpbs | 32 Mpbs | 5 Mpbs |
| Frekans | 2,4 GHz | 5 GHz | 2,4 GHz |
| Ortalama Erişim | CSMA/CA | CSMA/CA | CSMA/CA |
| Şifreleme | 40 bit RC4 | 40 bit RC4 | 40 bit RC4 |
| Modülasyon Yöntemi | FHSS veya DSSS | Tek taşıyıcı | DSSS |
| Kesişmeyen Kanal Sayısı | 3 (dahili/harici) | 4 (dahili, U-NII1)  4 (dahili, U-NII2)  4 (dahili, U-NII3) | 3 (dahili/harici) |

Tablo 2.1.1.1.2.1.1: IEEE’nin 802.11x standartlarının karşılaştırılması

2.1.1.1.2.1.2 IEEE 802.11a Standardı

802.11a, 1999 yılında geliştirilen bir standarttır. Veri aktarımında 5 GHz (Gigahertz) RF bandını kullanır. Bu frekans aralığı’nda, 12 kanal kullanan OFDM modülasyon tekniğini kullanır. OFDM (Orthogonal Frequency Division Multiplexing), radyo sinyallerini farklı frekanslarda, aynı anda yollanmak üzere daha kısa sinyallere böler ve böylece iletim boyunca oluşabilecek çapraz karışmaları önler. Bu modülasyon tekniği ev aletlerinden gelen girişimleri azaltmıştır. 802.11a standardı veri iletiminde saniyede 6, 9, 12, 18, 36, 48, 54 Mbps (Megabit) hızında yaklaşık 50 m’ye kadar iletişimi destekler.

802.11a standardı 5 GHz RF tayfını kullandığı için 2.4 GHz RF tayfı (802.11 b/g/n standards) ile uyumlu değildir. 802.11a uyumlu ekipman bulmak gittikçe zorlaşmaktadır. Diğer standartlara göre yüksek maliyetlidir. 802.11a standardının iletişim mesafesi diğer standartlara göre kısıtlıdır.

Bu teknoloji yüksek veri iletim hızına ihtiyaç duyan kullanıcılar tarafından veya video dağılım sistemlerinde aktif olarak kullanılmaktadır. Daha pahalı cihazlarda bulunmasına rağmen iş hayatında kurumsal kullanıcılar tarafından tercih edilmektedir. [24] [35] [12] [13]

2.1.1.1.2.1.3 IEEE 802.11b Standardı

802.11a ile aynı tarihlerde yayınlanmasına rağmen 802.11b standardı kullanıcılar arasında büyük kabul görmüştür. 802.11b standardı Wi-Fi olarak adlandırılmış ve Wi-Fi logosu bulunan ürünler uyumlu olarak çalışır. 802.11a standardına göre 802.11b standardının maliyeti düşüktür.

802.11b, veri aktarımında 2.4 GHz RF bandını kullanır ve 1, 2, 5.5, 11 Mbps hızında 100 m’ye kadar veri iletimini destekler. 802.11b standardı DSSS modülasyon tekniğini kullanır. 802.11b standardını kullanan bileşenlerin 2.4. GHz RF bandında çalışan diğer cihazlardan (bluetooth, kablosuz telefon, bebek monitörü vb.) girişime maruz kalması nedeniyle iletişimi kesilebilir.

802.11b ofis ortamları, hastaneler, depolar ve fabrikalar gibi ortamlarda kullanılmaya oldukça uygundur. Özellikle konferans salonları, çalışma alanları ve kablo çekmenin tehlikeli olduğu noktalarda ağ bağlantısı sağlanması için uygun bir teknolojidir. Kısaca 802.11b, taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulan alanlarda kullanılır. [35] [12]

2.1.1.1.2.1.4 IEEE 802.11g Standardı

802.11a ile aynı modülasyon tekniğini (OFDM) kullanır ama 2.4 GHz RF bandında çalışır. Maksimum veri hızı 54 Mbps’dir. 802.11g’nin sahip olduğu en önemli özellik 802.11b ile ulaşılan kapsama alanını (100 m) koruyarak veri iletim hızını 802.11a’ da olduğu gibi 54 Mbps’e ulaştırmasıdır. 802.11g istemci 802.11b erişim noktası ile uyumlu çalışabilir. Aynı şekilde 802.11b istemci 802.11g erişim noktası ile uyumlu çalışabilir.

802.11g standardının zaman zaman 802.11b ile çalışan cihazlarla uyum sorunu yaşamasından dolayı kullanımı çok fazla yaygınlaşmamıştır. Aynı zamanda fiyatının 802.11b’den yüksek olması da dezavantajıdır.

Yüksek hız gerektiren video ve çoklu ortam uygulamalarında hızı ve kapsadığı alanın genişliği nedeniyle 802.11g standardı tercih edilebilir. [35] [12]

2.1.1.1.2.1.5 IEEE 802.11n Standardı

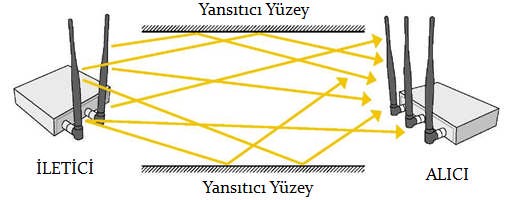
Ekim 2009 yılında yayınlanan 802.11n standardı 802.11b ve 802.11g wireless network’lerin geliştirilmesiyle oluşturulmuştur. Bu teknoloji ile wireless cihazların geniş bir alanı kapsaması ve wired network kadar hızlı veri iletimi hedeflenmiştir. 802.11n teknolojisiyle yüksek çözünürlükte video izlenebilir, kablosuz olarak sesli ve görüntülü görüşmeler yapılabilir. Wired LAN sistemlerin sunduğu kararlılık, performans ve güvenirlilik 802.11n standartlarıyla da sağlanmaktadır.

802.11n standardı ile sağlanan veri hız 144,4 Mbps’dir. Ancak bazı değişiklikler ile veri aktarım hızı 300 Mbps’ye kadar çıkabilir. Bu değişikliklerden en önemlisi 802.11n standardı ile MIMO teknolojisinin kullanılmasıdır. 802.11n standardına göre üretilen AP (Access Point)’ler hem 2,4 GHz hem de 5 GHz frekansında haberleşebilmektedir. Bu şekilde 802.11a, b, g standartları ile üretilmiş cihazlarla uyum içinde çalışabilecektir. [35] [12]

* **MIMO (Multiple Input Multiple Output):** Birden fazla anten kullanarak iletimin sağlandığı teknolojiye verilen addır. Bu teknolojide kullanılan çok yollu yayılım ile bant genişliğinin verimi artırılır. [6][7]

Şekil 2.1.1.1.2.1.5: 802.11b, g standardı ve 802.11n standardı radyo sinyal yayılımı

AP (Acces point) ve Wireless Network arayüz kartı üzerinde bulunan birden fazla anten ile veri parçalar hâlinde gönderilir ve karşı tarafta da birden fazla anten tarafından algılanır. Her bir anten tarafından alınan veri, DSP (Digital Signal Processor) kullanılarak birleştirilir.



Şekil 2.1.1.1.2.1.5.a: MIMO teknolojisi ile radyo sinyallerinin akışı

MIMO teknolojisi iki alıcı ve iki gönderici (2X2) anten kullanılarak gerçekleştirilir. Aynı zamanda daha yüksek veri hızı ve daha kaliteli bir sinyal için (2X3), (3X3), (2X4) veya (4X4) şeklinde anten bağlantıları yapılabilir. [6][7]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Standart** | **Modülasyon Tekniği** | **Frekans bandı** | **Veri hızı**  **(Maksimum)** | **Maksimum**  **sinyal aralığı** | **Yayın tarihi** |
| **802.11** | FHSS  DSSS | 2.4 GHz | 2 Mbps | Tanımlanmamış | 1997 |
| **802.11a** | OFDM | 5 GHz | 54 Mbps | 50 m | 1999 |
| **802.11b** | FHSS | 2.4 GHz | 11 Mbps | 100 m | 1999 |
| **802.11g** | OFDM | 2.4 GHz | 54 Mbps | 100 m | 2003 |
| **802.11n** | OFDM DSSS | 2.4 GHz 5 GHz | 144.4 Mbps (300 Mbps) | 250 m | 2009 |

Tablo 2.1.1.1.2.1.5: Yaygın IEEE WLAN standartları

###### 2.1.1.1.2.2 HiperLAN

HiperLAN (High Performance Radio LAN), ETSI tarafından tanımlanmış, OFDM kodlama ve modülasyon yöntemi kullanılan, 5 GHz bandında çalışan kablosuz LAN standardıdır. [35] [3]

###### 2.1.1.1.2.3 Coding / Modulation Techniques

IEEE 802.11x ailesi standartlarında genel olarak DSSS, FHSS ve OFDM kodlama/modülasyon yöntemleri kullanılmaktadır. Kodlama/modülasyon yöntemi, kullanıldığı standardın veri oranı, kanal sayısı gibi temel özelliklerini belirlemektedir.

DSSS (Direct Sequence Spread Spectrum) düz sıralı dağınık spektrum tekniği 802.11b standardında kullanılan kodlama ve modülasyon yöntemidir. 11 Mbps veri oranına kadar kodlama yapabilmektedir.

FHSS (Frequency Hopping Spread Spectrum), frekans atlamalı dağılmış spektrum 802.11’ de tanımlanmıştır, ancak üreticiler tarafından pek rağbet görmemiştir.

OFDM (Orthogonal Frequency Division Multiplexing) yani dikey frekans bölümleme çoğullama 802.11a standardında kullanılmakta ve dağılmış spektrum (spread spectrum) sağladığı tüm getirileri kullanmaktadır. Bu getiriler veri aktarım oranı ve kanal sayısıdır. Özellikle kanal sayısı büyükçe kablosuz ağ kurulumunda önem kazanır. Çünkü her bir kanal aslında bağımsız bir iletişim ortamıdır. OFDM’de 20 MHz’lik 8 tane çakışmayan kanal tanımı yapılmıştır. Kanalların her biri 52 alt taşıyıcıya bölünmüştür. Böylece aynı anda yapabilecek bağımsız aktarım sayısı artırılmıştır. Her bir alt-taşıyıcı aynı anda yapabilecek bağımsız aktarıma karşılık düşmektedir. 54 Mpbs hıza ulaşmak için 64QAM adlı mekanizma kullanılmaktadır. [22] [3]

###### 2.1.1.1.2.4 Multiple Access and Duplication Methods

Wireless Network’ların radyo frekansını kullanarak iletişimi sağlamakta olduğunu önceki konularda söylemiştik. Radyo frekansı spektrumu sonlu bir kaynaktır. Bu sebeple, aynı anda aktarım yapmak isteyen farklı uç sistemler kaçınılmaz olarak belirli frekans aralıklarını paylaşmaları gerekir. Frekans spekturumunun bölünmesi ve birçok kullanıcının arasında paylaştırılmasının birçok yöntemi vardır. Tablo 2.1.1.1.2.4’ te kısaca bu yöntemler anlatılmaktadır. [3]

|  |  |
| --- | --- |
| ***Yöntem*** | ***Yöntemin Çalışma Şekli*** |
| **FDMA (Frekans**  **Bölmeli Çoklu**  **Erişim) Yöntemi** | **Frekans, alanında birbiri üzerine taşmayan bölmelere ayrılır.**  **Bu bölmeler, uç sistemlerin belirli bir çağrısı için sistemlere atanır.**  **Her bir çağrı için, frekans ayrı bir taşıyıcı işaret bulunur.**  **Yaygın olarak analog sistemlerde kullanılır.** |
| **TDMA (Zaman**  **Bölmeli Çoklu**  **Erişim) Yöntemi** | **Kullanacağı spekturum zaman alanında bölmelere ayrılır.**  **Uç sistemler birim zamanda kendilerine ait bölümüne sırayla erişebilir.**  **Eğer çerçeveler yeterince hızlı tekrar edilirse, uç sistemler haberleşme sırasında bir kesilme ve gecikme hissetmezler.**  **HiperLAN/2 standardı tarafından kullanılıyor.** |
| **CDMA (Kod**  **Bölmeli Çoklu**  **Erişim) Yöntemi** | **Bu yöntemde çağrılar frekans ve zaman akanında kanallanmaz. Bu yaklaşımda iletimde bulunan her uç, her bir ayrı çağrı için benzersiz bir dağıtma kodunu, bilgi işaretini eldeki frekans aralığına yaymak için kullanılır.**  **Alıcı aynı benzersiz kodu kullanarak bilgi işaretini ayıklar; alıcı için diğer işaretler arka alan gürültüsü olarak algılanır.**  **Bu yolla aynı spektrum bloğunda aynı anda birden fazla çağrı gerçekleşebilir.**  **802.11x standartları bu yöntemi kullanır.** |
| **FDD ( Frekans**  **Bölmeli Çift Yönlü**  **Erişim) Yöntemi** | **İki yönlü aktarım anlamına gelir.**  **Var olan spektrum alışveriş yönünde birbiriyle etkileşimde bulunmayacak şekilde ayrılmasıdır.** |
| **TDD (Zaman**  **Bölmeli Çift Yönlü**  **Erişim) Yöntemi** | **İki yönlü aktarım anlamına gelir.**  **Sayısal ortamda iki yönlü iletimin gerçekleştirilmesi için kullanılıyor.**  **HiperLAN/2 standardı tarafından kullanılıyor.** |

Tablo 2.1.1.1.2.4: Multiple Access and Duplication Methods

###### 2.1.1.1.2.5 Security and Encryption

Wireless Network’larda güvenlik üzerinde en çok durulması gereken unsurlardan birisidir. Radyo frekans dalgalarının havadan iletilmesi istenmeyen kişilerce izlenebilme ve takip edilebilme imkânı sağlar. Güvenliği artırmak için en basit yaklaşım VPN yapılandırmasının, kablosuz haberleşme sistemleriyle birlikte kullanılmasıdır, ancak bu yaklaşım maliyetlerin artmasına sebep olur. 802.11x ailesi standardlarında kablolu ağ düzeyinde fiziksel koruma imkânı sağlanabilmesi amacıyla WEP adlı mekanizma önerilmiştir. Amaç, fiziksel anlamda kablolu ağların doğal olarak sağladığı mahremiyeti sağlamaktır.

WEP (Wired Equivalent Privacy) kısaltması kablolu düzeyde gizlilik/mahremiyet anlamına gelmektedir. Öyle ki, kapsama alanı içersinde herkes tarafından alınabilen radyo frekans dalgalarından, yalnızca haberleşme yetkisi olanların veri aktarımında bulunabilmesini sağlamaktadır. Bu yöntem, anahtar yöntemini kolaylaştırır ve gizli kalması gereken anahtarların öğrenilmesini engeller. Tablo 2.1.1.1.2.5’ ten şifre oluştururken yararlanabilirsiniz. [16] [38] [5] [20] [18] [39] [3]

|  |
| --- |
| **Şifreleme Tekniğine Göre Kullanılabilecek Anahtar Uzunlukları** |
| **WEP (Wired Equivalent Privacy)** |
| **Onaltılık ASCII** |
| **64bit (40+24)** 0-9 ve A-F arası 10 karakter A-Z ve 0-9 arası 5 karakter |
| **128bit (104+24)** 0-9 ve A-F arası 26 karakter A-Z ve 0-9 arası 13 karakter |
| **152bit (128+24)** 0-9 ve A-F arası 32 karakter A-Z ve 0-9 arası 16 karakter |
| **256bit (232+24)** 0-9 ve A-F arası 58 karakter A-Z ve 0-9 arası 29 karakter |
| **128bit-256bit** 0-9 ve A-F arası 64 karakter A-Z ve 0-9 arası 63 karakter |

Tablo 2.1.1.1.2.5: Şifreleme tekniğine göre kullanılabilecek anahtar uzunlukları

###### 2.1.1.1.2.6 Wireless LAN Technologies

Wireless Network’larda veri iletimi için kullanılan birkaç teknoloji bulunmaktadır. Bunların en önemlileri elektromanyetik dalgaları kullanılan RF ve çıplak gözle görülebilen ışığın altındaki frekansları kullanan kızıl ötesi teknolojisidir. RF ve kızıl ötesi teknolojileri WLAN sistemlerinde kullanılmakta olup, her birinin kendine özgü üstünlükleri ve mahzurları bulunmaktadır. Kullanıcıların kendi ihtiyaçlarına göre doğru teknolojiyi seçmeleri sistem verimliliğini ve memnuniyeti artırmaktadır. Günümüzde artan çoklu ortam uygulamaları sonucunda oluşan yüksek veri hızı talebi sebebiyle teknolojiler arasındaki rekabette veri hızı en önemli ölçüt olarak görülmektedir.

Uygulamada yüksek veri hızları ve fiziksel engelleri geçebilme özellikleri sebebiyle RF teknolojisi yaygın olarak kullanılmaktadır. WLAN sistemlerinde kullanılan RF ve kızıl ötesi teknolojisi aşağıda verilmiştir. [35] [34] [22] [21] [18] [3]

2.1.1.1.2.6.1 RF Technology

RF teknolojisinde, kablo yerine elektromanyetik dalgalar kullanılarak kablosuz iletişim gerçekleştirilmekte ve WLAN sistemlerinde yaygın olarak kullanılmaktadır.

Ekonomik sebeplerden dolayı WLAN sistemleri için lisans ve kullanım ücreti gerektirmeyen ISM frekans bantları esas alınmıştır. Bu bantlar öncelikle diğer telsiz servislerinin kullanımı için tahsisli olduklarından WLAN sistemleri muhtemel enterferansı baştan kabul etmek zorundadır. Bu durum WLAN sistemleri için karışım olaylarına (enterferans) karşı dayanaklı teknolojilerin geliştirilmesini ve kullanılmasını zorunlu hâle getirmiştir.

"Enterferans" terimi, ilgili kanun ve tüzüklere uygun olarak sağlanan her türlü haberleşme hizmetini engelleyen, haberleşmede kesinti doğuran veya kalitesini bozan her türlü yayın veya elektromanyetik etkiyi ifade etmektedir. [8] [22] [3]

2.1.1.1.2.6.2 Infrared Technology

Infrared teknolojisi elektromanyetik spektrumda gözle görülebilen ışığın altındaki frekansları (3x10 14 kHz / 850-950 nm) veri iletiminde kullanan bir teknolojidir. Alıcı ile verici cihaz arasında açık görüş hattının bulunduğu ortamlarda ve kısa mesafeler için çok uygundur.

Infrared teknolojisini iki tür kullanmak mümkündür. Birincisi direct beam, line of sight, ikincisi ise diffused beam yöntemidir. Doğal olarak görüş hattı yöntemi diğerine oranla daha fazla veri iletişimi sağlamaktadır. Ancak uygulamada geniş alan kaplamak ya da çok kullanıcıya ulaşabilmek için yansıma yöntemi tercih edilmektedir. Infrared teknolojisi büyük oranda uzaktan kumanda cihazlarında kullanılmaktadır. Profesyonel olarak infrared teknolojisi geçici ağ kurma ihtiyacı duyulan toplantılarda veya gezici satış elamanları tarafından kullanılmaktadır. Bu tür kullanımda yerel wired network ile bağlantı kurarak bilgi alışverişinde bulunmak ve sunucuya bağlı faks ve yazıcı gibi cihazlardan faydalanmak mümkündür. Aynı ortamda çalışan bir grubun yazıcı, faks ve benzeri donanımları ortaklaşa kullanabilmeleri için bir ağ oluşturmaları da mümkündür. Benzer şekilde kullanım örneklerini artırmak mümkündür. Kısa mesafe iletişim için uygun olan infrared teknolojisinin üstünlük ve mahzurları Tablo 2.1.1.1.2.6.2’da verilmiştir. [3]

|  |  |
| --- | --- |
|  | **Kızılötesi (infrared-ırda)** |
| **Üstünlükleri** | Serbest kullanıma açıktır. Bir lisans ve ücret gerektirmez. |
| RF sinyallerinden etkilemez. |
| Güç tüketimi düşüktür. |
| Kapalı ortamlarda yetkisiz dinlemeye ve bozucu etkilere karşı tam bir güvenlik sağlar. |
| **Mahzurları** | İletişim mesafesi kısadır. İdeal şartlarda 10-15 m’ dir. |
| Sinyaller katı cisimleri geçemez. Bu sebeple kapalı alanlarda duvar, kapı ve büro malzemeleri tarafından kullanım için uygundur. |
| Sinyaller kar, sis, toz ve ışık gibi hava şartlarından etkilenir. Bu sebeple açık alanlarda kullnım için uygun değildir. |
| Kirlilik sinyalleri etkiler. |

Tablo 2.1.1.1.2.6.2: Infrared teknolojisinin üstünlük ve mahzurları

###### 2.1.1.1.2.7 Wireless LAN Systems

WLAN, veri iletimini hava üzerinden elektromanyetik dalgalar hâlinde taşıyarak kablo bağlantılarını azaltan bir çözümdür. WLAN uygulamaları, kullanıcının hareket imkânını kolay bir kurulumum rahatlığı ile birleştirirler. Temel olarak wireless LAN (WLAN) sistemi iki ana unsurdan oluşmaktadır. Birincisi AP (Access point,), ikincisi ise kablosuz cihazlardır. Ancak cihazdan cihaza (peer to peer) çalışma modelinde AP’ye ihtiyaç duyulmaz. Bu durumda kablosuz ağ kartına sahip bilgisayarlar, kendi aralarında ilave bir cihaz veya kabloya ihtiyaç olmadan bir ağ oluşturabilir. Kablosuz cihazlar genellikle bir dizüstü bilgisayar, kişisel bilgisayar (PC), cep bilgisayarı (PDA, Personal Digital Assistant), veya kablosuz ağ ünitesi (NIC, Network Interface Card) ile donatılmış benzeri bir cihaz olabilir. NIC’ler RF veya infrared kullanarak takılı bulunduğu cihaz ile AP arasındaki bağlantıyı sağlar. AP’ler ihtiyaca göre bir eve, iş yerine, toplantı salonuna veya bir binaya kurulabilir. Halka açık kullanımı sağlamak üzere ise şehir merkezlerine (Taksim, Kızılay gibi), büyük alışveriş merkezlerine, hava alanı, tren istasyonu, otobüs terminali veya restoran gibi kamuya açık alanlara AP kurulabilir. Bu durumda AP’nin oluşturduğu kablosuz internet bağlantısı sağlanan fiziksel alan, Erişim Alanı olarak adlandırılmaktadır. Kablosuz cihazlarda bulunan NIC’ler otomatik frekans tarama özelliğine sahip olduklarından kendilerine ulaşan WLAN sinyalini algılayabilir. NIC tarafından doğru frekans kanalı bulunduktan sonra AP ile kablosuz cihazlar arasında bağlantı kurulumu başlatılır.

WLAN sistemleri aslında tamamen kablosuz değildir. Çünkü sistemde bulunan AP’nin geniş bant erişim hizmeti veren DSL, Fiberoptik veya benzeri bir kablolu altyapı üzerinden şebekeye bağlanması gerekebilir. Bu sebeple, WLAN sistemleri ile tamamen kablosuz olmaktan ziyade kablolama ihtiyacı en az düzeye indirilmiş olmaktadır. Bu açıdan bakılınca WLAN sistemlerinin artışı geniş bant erişim hizmetinin artışına bağlıdır ya da WLAN sistemlerinin artışı geniş bant erişim hizmetinin yaygınlaşmasını desteklemektedir. Ancak cihazdan cihaza kullanımda herhangi bir kablolamaya ihtiyaç olmadığından tam bir kablosuz ağ kurulumu gerçekleşmektedir. Benzer şekilde şebekeye erişim hizmetinin kablo yerine sabit telsiz erişim (FWA) veya uydu terminali ile sağlanması durumunda da tam bir kablosuz ağ kurulumu gerçekleşmektedir. [9] [8] [30] [27] [3]

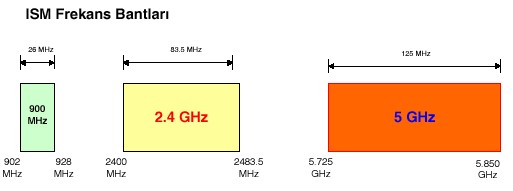
2.1.1.1.2.7.1 Wireless LAN Systems Çalışma Esasları

WLAN sistemleri havada yayılan elektromanyetik dalgalarla bir noktadan başka bir noktaya fiziksel bağlantı olmaksızın bilgi iletişimini sağlar. Tipik bir kablosuz yerel ağ kurulumunda, AP olarak isimlendirilen hem alıcı hem verici konumundaki cihaz, wired network’e bağlanır ve wired network omurgası ile kablosuz cihazlar arasında veri alışverişi işlemini gerçekleştirir. Bir AP, kullanılan ortama bağlı olarak dâhili uygulamalarda 25-100 metre, harici kullanımda ise 200 metreye kadar yarıçaplı bir alanı kapsayabilir. WLAN sistemlerinde kullanılan yüksek frekanslı RF sinyali (2.4 GHz ve 5 GHz) temel özelliği sebebiyle katı cisimlere nüfuz edebilir ve geçebilir. Bu özellik görüş hattının sağlanamadığı bina içi kullanımlarda fayda sağlar. Ancak katı cisimler kullanılan maddeye (tahta, çelik, beton gibi) bağlı olarak sinyal zayıflamasına sebep olur. Bu da sonuçta erişim mesafesini kısaltır.

Lisansız kullanımlar için çıkış gücü düzenlemeler ile sınırlandırılmış (genellikle 100 mW) olduğundan mesafe artırımı için güç yükseltilmesi söz konusu değildir. Bu sebeple iyi bir kapsama alanı için fiziksel ortam iyi etüt edilmeli ve AP montaj yerleri iyi seçilmelidir. AP veya kullanılıyorsa AP’ye bağlı harici anten, genellikle yüksek bir noktaya montaj edilir. Bu sadece kapsama alanını genişletmek için gereklidir. Eğer yeterli kapsama alanı sağlanıyor ise AP’ler istenilen her noktaya konulabilir. Kullanıcılar ise kablosuz erişim özelliğine sahip cihazlar ile ağa bağlanabilir. Bu özelliği bulunmayan bilgisayarlar için hariçten takılan kablosuz ağ adaptörleriyle, dizüstü bilgisayarda PCMCIA kartlarla, masaüstü bilgisayarlarda ise ISA/PCI kartlarla kablosuz erişim gerçekleştirilir. Ayrıca dizüstü ve masaüstü bilgisayarlarda USB girişinden Wireless LAN Adapter ile wireless connection yapılmaktadır. Bir başka ifade ile wireless access özelliği bulunmayan cihazlar hariçten takılan Wireless LAN Adapter’leri ile WLAN sistemlerinde kullanılabilmektedir. [8] [35] [15] [27]

2.1.1.1.2.7.2 Wireless LAN System’lerde Kullanılan Frekanslar

RF bantlarının belirli alanları, wireless LAN, kablosuz telefon ve bilgisayar çevresel aygıtları gibi lisanssız aygıtların kullanımına ayrılmıştır. Bu alanlar, 900 MHz, 2.4 GHz ve 5 GHz frekans aralıklarıdır. Bu aralıklar Endüstriyel, Bilimsel ve Tıbbi (ISM) bantlar olarak bilinir ve çok az bir kısıtlamayla kullanılabilir. Bu bantlardan teknik olarak WLAN uygulamasına uygun olan ISM bantları Şekil 2.1.1.1.2.7.2’de verilmiştir. [27]



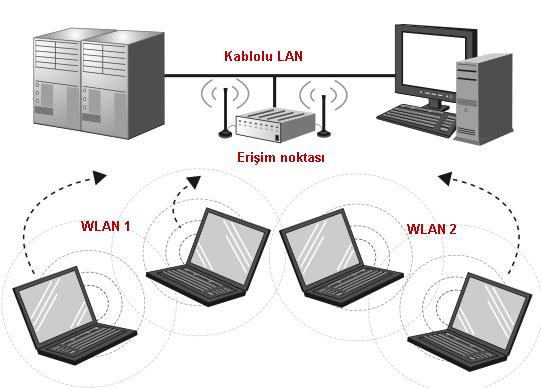
Şekil 2.1.1.1.2.7.2: ISM Frekans Bant

Ancak, 900 MHz bandı sadece ITU-RR ikinci bölge için ISM bandı olarak belirlenmiştir. Bu sebeple, ITU-RR birinci bölgede yer alan Türkiye’de GSM sistemleri için tahsis edilmiş olup WLAN sistemlerinde kullanılmamaktadır. [27]

2.1.1.1.2.7.3 Wireless LAN System’inde Kullanılan Cihazlar

2.1.1.1.2.7.3.1 Erişim Cihazı

Access Point wireless LAN kurulması için merkezi konumda olan ve kapsama alanı içerisindeki tüm trafiği yöneten erişim cihazı köprüleme mantığıyla çalışır. Wireless access üzerinde bulunan antenlerle havadan, wired network’e bütünleştirilmesi de ethernet gibi LAN teknolojisiyle yapılır. Uç sistemlerden daha yükseğe monte edilmesi yararlıdır. Access point cihazları kuruluma ve teknolojiye dayanarak 10 metrelerden 500 metreye kapsama alanına sahip olabilmekteyken, 10 ile 250 arasında kullanıcıyı desteklemektedir. Bir access point cihazının kapsama alanındaki uç sistemlerin sayısı arttıkça tıkanma olasılığı artar ve wireless network’ün başarımı düşer. Bu sebeple, Şekil 2.1.1.1.2.7.3.1’de görüldüğü gibi hem kapsama alanını genişletmek hem de erişim cihazı başına düşün kullanıcı sayısını azaltmak için aynı ağ içerisinde birden çok erişim cihazı kullanılabilir. [27]



Şekil 2.1.1.1.2.7.3.1: Wired LAN ve Wireless LAN’ların access point’ları ile birleştirilmesi

Piyasada kullanılan erişim cihazlarına bir örnek aşağıda gösterilmiştir ve erişim cihazı alırken dikkat edilecek özellikler ile ilgili bilgiler aşağıda verilmiştir. Kuracağınız wireless LAN’ın yapısına uygun erişim cihazı almanız ağınızın sağlıklı çalışması için hayati önem taşır.



Şekil 2.1.1.1.2.7.3.1 a : Erişim Cihazı

* **Standartlar:** Cihazın desteklediği wireless LAN standartları
* **Modülasyon:** Cihazın desteklediği modülasyon yöntemleri (OFDM)
* **Veri transfer değerleri:** Veri transferi yapabildiği hız değerleri
* **Ağ bağlantısı tipi:** Desteklediği ağ bağlantı tipi (Infrastructure ve Ad-hoc)
* **Çalışma modları:** Çalışabildiği wireless connection modları **(**Erişim Noktası, APto-AP Bridge, Point-to-MultiPoint Bridge (köprü, Wireless Repeater (WDS), Wireless Client)
* **Frekans bandı:** Cihazın çalıştığı frekans aralığı (MHz olarak)
* **Verici çıkış gücü:** Cihazın verici gücü (db olarak)
* **Alıcı hassasiyeti:** Cihazın alıcı hassasiyeti (db olarak)
* **Dış anten tipi:** Cihazın takılabilen anten tipi
* **Ağ desteği**: Cihazın kullanılabileceği ağlar (Server and Client)
* **Güvenlik:** Cihazın desteklediği güvenlik modları **(**64-bit, 128-bit 152-bit WEP şifreleme, WPA, 802.x vb.)
* **Çalışma menzili:** Cihazın iletişim kurabildiği menzili **(**Kapalı alanda, açık

Alanda)

2.1.1.1.2.7.3.2 PCMCI Adaptor

Bir başka kablosuz bilgisayar ağı parçası, son kullanıcıların bilgisayarlarına takılabilen WLAN ara yüzü ve dahili alıcı verici anteni bulunan PCMCI kartıdır. Gerektiği durumlarda güçlü antenlerin de takılabilmesi için üzerinde yuvası bulunan bu kart, köprü cihazlarının kablosuz ağ bağdaştırıcısı olarak kullanılabildiği gibi ISA veya PCI adaptörleri aracılığı ile günümüz kişisel bilgisayarlarına da takılabilmektedir.

Piyasada kullanılan PCI adaptörlerine bir örnek Şekil 2.1.1.1.2.7.3.2’ de ve PCI adaptörü alırken dikkat edilecek özellikleri ile ilgili bilgiler aşağıda verilmiştir. Kuracağınız kablosuz LAN’ın yapısına uygun PCI adaptörü almanız ağınızın sağlıklı çalışması için hayati önem taşır. Dikkatlice inceleyiniz. [27]

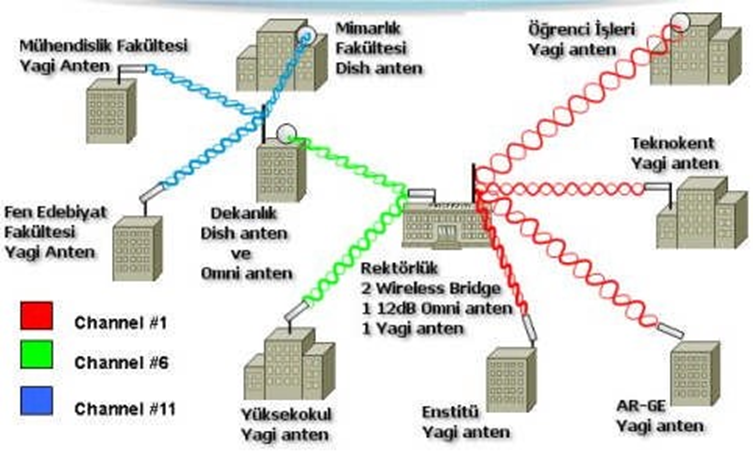


Şekil 2.1.1.1.2.7.3.2: Bit PCI slot

* **Standartlar:** Aygıtın desteklediği wireless LAN standartları
* **Modülasyon:** Aygıtın desteklediği modülasyon yöntemleri (OFDM)
* **Veri transfer değerleri:** Veri transferi yapabildiği hız değerleri
* **Ağ bağlantısı tipi:** Desteklediği ağ bağlantı tipi (Infrastructure ve Ad-hoc)
* **Frekans bandı:** Aygıtın çalıştığı frekans aralığı (MHz olarak)
* **Verici çıkış gücü:** Aygıtın verici gücü (db olarak)
* **Alıcı hassasiyeti:** Aygıtın alıcı hassasiyeti (db olarak)
* **Dış anten tipi:** Aygıtın takılabilen anten tipi
* **Güvenlik:** Aygıtın desteklediği güvenlik modları **(**64-bit, 128-bit 152-bit WEP şifreleme, WPA, 802.x vb.)
* **Çalışma menzili:** Aygıtın iletişim kurabildiği menzili (kapalı alanda, açık alanda)
* **Uyumluluk:** Çalışabildiği wireless LAN standartlı aygıtlar
* İşletim sistemi desteği: Windows 98SE/ME/2000/XP

2.1.1.1.2.7.3.3 ANTENNA

802.11 standardındaki cihazlar temel olarak iki tür anten kullanmaktadır. Noktadan çok noktaya iletim için “omnidirectional” ve noktadan noktaya iletişim için yönlendirilmiş “omnidiretional” anten için tipik olarak erişim mesafesi 45 m civarındadır. Yerel düzenlemelerin elverdiği durumlarda yüksek kazançlı antenler ve güçlendiricilerle mesafe 40 km ve üstüne çıkabilir. Noktadan noktaya iletim için kullanılan antenler LAN’ lar arası köprüleme için tercih edilmekte olup görüş hizasının sağlanmasını gerektirir. “Omnidirectional” uygulamalarda erişim cihazının yerleşimi çok önemlidir. Radyo frekans girişimlerine dikkat edilmelidir. Şekil 2.1.1.1.2.7.3.3’de bir üniversite kampüsünde kurulan kablosuz LAN görülmektedir. [27]



Şekil 2.1.1.1.2.7.3.3: Bir üniversite kampüsünde uygulanan wireless LAN’da kullanılan antenler

2.1.1.1.2.7.4 Wireless LAN System’lerinin Mimari Yapısı

Bilgisayarların birbirleri ile iletişiminin hangi hiyerarşik düzende olduğu mimari yapı (Topoloji) olarak ifade edilmektedir. Wireless LAN sistemlerinde peer-to-peer (Ad/Hoc) ve alt infrastructure (Client/Server) olmak üzere 2 çeşit mimari yapı kullanılmaktadır.

WLAN sistemlerinde kullanılan mimari yapılar ve temel özellikleri aşağıda verilmiştir. [1][2][3] [27]

2.1.1.1.2.7.4.1 Ad Hoc Modeli

Ad Hoc modeli iki ya da daha çok wireless iletişim özelliğine sahip bilgisayarın, bir sunucu kavramı olmadan birbirine bağlandığı ağ yapılarıdır. Bu tür ağlarda bulunan bilgisayarların sahip oldukları program, veri ve dosya gibi tüm kaynaklar ağdaki diğer bilgisayarlar tarafından kullanılabilir. Bu model prensip olarak daha hızlı kurulabilen ve kablo veya AP gibi herhangi bir altyapı ihtiyacı olmayan en basit ağ kurulum yöntemidir. İstemci veya sunucu olmasına bakılmaksızın ağda yer alan tüm bilgisayarlarda sadece kablosuz çalışma özelliğinin olması yeterlidir.

Ad Hoc modelinde wired network bağlantısı bulunmaz. Dolayısıyla internet veya intranet bağlantısı söz konusu değildir. Ad Hoc modelinde ağ içindeki bütün bilgisayarlar eşit düzeydedir. Yani istemci sunucu ayrımı olmayıp tüm bilgisayarlar aynı önceliğe sahiptir. Ağdaki her kullanıcı diğer kullanıcının kaynaklarına kolaylıkla erişebilir ve kullanabilir. Bu mimari yapı çok yaygın kullanılmamakla birlikte geçici ve hızlı bir ağ ihtiyacı duyulan grup çalışmalarında ve toplantılarda kullanılmaktadır. Ad Hoc modeli Şekil 2.1.1.1.2.7.4.1’ de görülmektedir. [1][3] [30] [27]



Şekil 2.1.1.1.2.7.4.1: Ad Hoc modeli

2.1.1.1.2.7.4.2 Infrastructure, Client/Server Modeli

WLAN sistemlerinin temel ve en yaygın kullanım şekli olan infrastructure, client/server modeli; wired network’e bağlı bir AP ve istenilen sayıda kablosuz erişim özelliğine sahip cihazdan oluşur. Wired network’de ihtiyaca göre genellikle bir geniş bant internet erişimi ve sunucu bilgisayar bulunabilir. Bu durumda ağda bulunan tüm bilgisayarlar AP aracılığıyla kablosuz olarak mevcut wired network’e ve internete bağlanabilir. Ev ve küçük iş yeri uygulamaları için temel altyapı çalışma modeli yeterli ve uygundur. Bu tür çalışma modelinde paylaşılan bütün kaynaklar sunucuda yer alır ve işlemler sunucu aracılığıyla yürütülür.

Sunucu işlemleri hızlı bir şekilde yaparak sonuçları istemciye yollar. Böylece işlem hızı ve kapasitesi artırılmış olur. Aksi durumda ise her bir bilgisayarın kendi programları ile verileri işlemesi gerekecektir. Bu durumda ise işlem hızı iş istasyonunun performansına bağlı olacaktır. Infrastructure, client/server modelinde geniş bant internet erişimi genellikle wired sistemler ile sağlanmakla birlikte kablosuz olarak da sağlanması mümkündür. Wired access olarak ADSL, Fiberoptik, Kablo TV şebekesi; wireless access olarak ise FWA kullanılmaktadır. Temel infrastructure, client/server çalışma modeli Şekil 2.1.1.1.2.7.4.2’de gösterilmiştir. [1][3] [27] [30]



Şekil 2.1.1.1.2.7.4.2: Infrastructure, Client/Server Çalışma Modeli

WLAN altyapı çalışma modelinde kullanıcı sayısının veya iletişim mesafesinin artırılması gereken durumlarda sisteme yeni AP’ler ilave edilebilir. Örneğin, bir toplantı salonundaki yoğun kullanımı karşılamak üzere ikinci veya üçüncü AP sisteme ilave edilebilir.

Kullanım alanını genişletilmesi ise hücre sistemine göre değişik noktalara AP’lerin kurulması ile gerçekleştirilir. AP’lerin sayısının ve montaj yerlerinin tespiti istenilen veri iletişim hızı, kullanıcı sayısı, iletişim alanının boyutu ve benzeri ölçütlere bağlı olarak belirlenir. [1][3] [27] [30]

2.1.1.1.2.7.5 Point-to-Point Wireless Connectivity

Point to point wireless connectivity ağ uygulamasında ve veri haberleşmesinde birçok alanda kullanılmaktadır. Her ne kadar wireless LAN uygulamalarında sistemler birbirini doğrudan point to point görebilse de point to point bağlantı sözcüğü daha çok Şekil 2.1.1.1.2.7.5’de görüldüğü gibi iki nokta arasındaki ana hattın (trunk) wireless connection’ı şeklinde değerlendirilir. Bu şekildeki bağlantılarda uç sistemlerin antenleri doğrudan birbirini görmesi gerkirken uydu sistemleri aracılığıyla da bağlantı sağlanabilir. Uydu sistemleri, kablosuz haberleşme teknolojileri arasında en çok bilinen ve yaygın olan türlerden biridir. Uydu hizmetleri coğrafi olarak elverişsiz noktalarla haberleşmeyi mümkün kılmaktadır. Ancak işletimi ve hizmetleri pahalıdır.



Şekil 2.1.1.1.2.7.5: Point-to-Point Wireless Connectivity

Şekil 2.1.1.1.2.7.5’de görüldüğü gibi, point-to-point wireless connectivity, wireless LAN standartlarına göre daha basittir denilebilir. Çünkü en azından antenler birbirlerine yönlendirilmiş durumdadır ve yalnızca bir çift uç sistem vardır. Bu tür wireless bağlantı, bağlanacak uç düğümlere ait ATM, ethernet gibi teknolojilerin fiziksel katmanının wireless olmasıyla gerçekleştirilir.

Point-to-point bağlantı ihtiyacı, wireless LAN standardı olan 802.11x ailesi tarafından desteklenmektedir. Bu durumda, ortada access point cihazı olmadan sistemler ad hoc modunda birbirleriyle veri alışverişinde bulunabilir. Bu tür bağlantı daha küçük uygulamalarda ve taşınabilir bir sistemin bulunduğu ortamda izin verilen bir sisteme bağlanmasında tercih edilmektedir. [1][2][3] [27] [32]

2.1.1.1.2.7.6 Wireless LAN Uygulaması

Wireless LAN kurulmasında ve kurulduktan sonra sağlıklı ve verimli çalışmasını sağlamak için bilinmesi ve dikkat edilmesi gereken noktalar vardır. Aşağıda bu noktalar kısaca açıklanmış ve Windows XP işletim sisteminde wireless LAN oluşturulması ile ilgili bir uygulama yapılmıştır. [1][3] [27]

2.1.1.1.2.7.6.1 Wıreless Local Network Oluşturmada İzlenecek Temel Adımlar

Wireless local network oluşturmanın tek bir yolu yoktur. Wireles network teknolojilerini ağ yapınıza tümleştirme şeklini ve zamanını ihtiyaçlarınız ve bütçeniz belirler. Bu sebeple, kendi wireless local network’ünüzü oluşturmaya daha çok adım adım işleyen bir süreç denebilir ve aşağıdakileri içerir:

**Almak istediğiniz donanımı belirleme**: İstek listenizde kablosuz dizüstü bilgisayarlar, erişim noktaları, kablosuz yerel ağ bağdaştırıcıları ve kablosuz kartlar gibi kablosuz özelliği etkinleştirilmiş cihazlar bulunmalıdır. Alacağınız donanım miktarı kullanıcı sayısına bağlıdır.

**Ağa erişmesi gereken kullanıcı sayısını belirleme**

**Wired local network’a bağlantıyı planlama:** Access point’ları kuracağınız yerleri belirlemeniz gerekir. Access point’u, etrafında wireless cihazların local network’e erişebileceği sınırlı bir wireless bölge bulunduğundan büyük ihtimalle merkezî bir konuma kurmak istersiniz. Ayrıca access point ile kullanım noktaları arasında çok az engel bulunmasını sağlamak için access point’u olabildiğince açık bir ortama kurduğunuzdan da emin olmak istersiniz. Bu, access point’un kablosuz kapsama alanını en üst düzeye çıkarır.

**Wireless cihazlarınızı ağınızla birlikte çalışacak şekilde yapılandırma:** Access point’u kurmak için yerel ağa bağlı bir ethernet kablosu takınız ve ağ adı ve şifre kodu atamak üzere erişim noktasıyla birlikte gelen yazılımı kullanınız.

**Hayata geçirmeden önce kurulumu sınama:** Tüm donanımınızı aldıktan ve yapılandırdıktan sonra yeni kablosuz kurulumunuzu sınamanız gerekir. Kablosuz yerel ağda birkaç kullanıcı ve cihaz kullanarak veri alışverişi yapmak üzere gerçekçi bir senaryo üzerinden uygulama yapınız. [1][2][3]

** Wireless local network yönetimi yordamı oluşturma**

1.1.1.2.7.6.2 Wıreless LAN’ larda Karşılaşılan Sorunlar

**Performans**

Radyo dalgaları gerçekte bütün yönlerde aynı mesafeye erişemezler. Duvarlar, kapılar, insanlar, asansör boşlukları ve diğer engeller, radyo frekansı yayılmasının bozulmasına ve düzensiz olmasına sebep olur. [25] [26] Performansı etkileyen temel ölçütler:

* Wireless cihazlar arasındaki mesafe, access point ile wireless ethernet kartı arasınki mesafe
* Transmisyon güç seviyesi
* Bina ve evdeki elemanlar
* Radio frekanslarının birbirine karışması
* Sinyal yayılımı
* Anten tipi ve yerleşimi

Wireless LAN uygulamalarından iyi bir performans alabilmek şu noktalar göz önünde bulundurulmalıdır.

* Wireless uygulama alanında, AP ile kullanıcılar arasındaki mesafe performansı doğrudan etkiler. Mesafe arttıkça aktarım hızı düşer.
* Wireless cihazların yerleşimi ve doğrultusu da önemli bir etkendir.
* Uygulamanın yapıldığı binanın yapısı, bina malzemesi, konstrüksiyon tipi sinyal kalitesini ve sinyal hızını etkiler.

AP ile kullanıcı arasındaki duvarın yapısına göre zayıflama değerleri Tablo 1.1.1.2.7.6.2 ‘de verilmiştir.

|  |  |
| --- | --- |
| **Engel Tipi** | **Zayıflama** |
| Alçı Duvar | 3dB |
| Tuğla Duvar | 4dB |
| Metal Çerçeveli Cam Duvar | 6dB |
| Cam Çerçeve | 3dB |
| Metal Kapı | 6dB |

Tablo 1.1.1.2.7.6.2: Duvarın yapısına göre sinyallerin zayıflama değerleri

\*Her 3 dB zayıflama sinyal gücünün yarıya düşmesine sebep olur.

Fiber duvarlar, alüminyum yüzeyler, boru ve elektrik kablolaması, mikrodalga fırınlar ve kablosuz telefonlar ise, kablosuz sistemin etkin olabileceği mesafeleri ve kaplama alanını olumsuz etkiler.

**Electromagnetic Interaction**

2.4Ghz radyo frekans spektrumunda çalışan diğer kablosuz cihazlar, 802.11b kablosuz cihazlarla aynı ortamda kullanıldığında elektromanyetik etkileşime sebep olabilir.

2.4GHz kablosuz telefonlar, mikrodalga, fırınlar, yakın mesafedeki florasan aydınlatma sistemleri ve yakın mesafedeki başka bir 802.11b kablosuz ağ bunlara örnek olarak verilebilir.

**Security**

Wireless sistemlerde dikkat edilmesi gereken en önemli özellik güvenliktir. Standart güvenlik sağlayan ürünler yerine kendi gelişmiş güvenlik algoritmalarını kullanan ürünler tercih edilmelidir. Ancak paketlerin yüksek seviyede (128bit, 256bit) kodlanması ve alıcıda tekrar kodların çözülmesi, iletişimde gecikmeye ve dolayısıyla ağ performansında azalmaya sebep olur. [40] [16] [5]

## 2.2 WIRED NETWORKS

Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan çalışma biçimine Computer Network denir. Bir bilgisayar ağında çok sayıda bilgisayar yer alır. Bu bilgisayarlar yan yana duran iki bilgisayar olabileceği gibi tüm dünyaya yayılmış binlerce bilgisayar olabilir. Ağ içindeki bilgisayarlar belli bir biçimde dizilirler. Bilgisayarlar arasında genellikle kablo ile bağlantı sağlanır. Kablo bağlantısının mümkün olmadığı durumlarda mikro dalgalar ve uydular aracılığıyla da ağ içindeki iletişim kurulur. Bilgisayar ağlarının ilk uygulamaları 1960’lı yılların sonlarında başlamıştır. Ancak yerel bilgisayar ağlarının yaygınlaşması 1980’li yıllarda başlamış ve gelişmiştir. 1980’li yıllarda, kişisel bilgisayarların çoğalması, bilgisayar teknolojisindeki ve iletişim teknolojilerindeki gelişmeler bilgisayar ağlarının daha yararlı olmasını sağlamıştır.

Bilgisayar ağı, birbirine bağlı birçok bağımsız bilgisayar anlamına gelir. İki bilgisayarın birbirinin kaynaklarını (diskini ya da diskinde yer alan bilgilerini) paylaşabilmesi ve konuşabilmesi onların birbirine bağlı olduğunu gösterir.

İşletmecilik açısından ağlar, yönetime ve denetime yardımcı olurlar. Bir bankanın ya da üniversitenin çok sayıda bilgisayarı birbirine bağlı olarak kullanılması, onları bağımsız olarak kullanmasından daha anlamlı ve verimli olur. Böylece birimler arası iletişim daha kolay sağlanmakta ve bütünleşik uygulamalar daha kolay gerçekleştirilmektedir. Ortak kaynak kullanımı ile donanım maliyetleri düşer, ortak çalışma imkânını arttırarak takım çalışmalarını hızlandırır, çalışanların verimini ve performansını arttırır. İletişim hızını arttırarak zaman kazancı sağlar, ayrıca önemli bilgilerin yedeklenmesi daha kolay hale gelir.

Bilgisayar ağına bağlı olan bir bilgisayar diğer bilgisayarlarla bağlantı içindedir. Diğer bilgisayarlarla iletişim kurar, onların sabit diskinde yer alan verilere erişir, onların programlarından yararlanır. En basit biçimi ile ağ, genellikle modemlerle birbirine seri bağlantılı olan iki makinedir. Daha karışık ağ yapılarında ise, TCP/IP (Transmissions Control Protocol / Internet Protocol), protokolü kullanılmaktadır. Bu, yüz binlerce bilgisayarın birbirine bağlı olduğu Internet üzerinde diğer bilgisayarlar ile bağlantı kurmamızı sağlayan protokol ailesidir [49] [50].



Şekil 2.2: Bilgisayar Wired Network Yapısı Örnek

Bilgisayar ağları tüm işleme modelleriyle (merkezi, dağıtık ve birlikte) birlikte bilgisayarları ve işletim sistemlerini içerir. Tipik bir ağ, sunucu, istemci, iş istasyonları, yazıcı ve diğer bilgisayar çeşitleri ile ağ cihazlarını içerebilmektedir.

Firmaların kullandıkları ağ teknolojileri ve ölçekleri, firmanın yaptığı işle ve firmanın ölçeğiyle paraleldir. Bilgisayar ağları genellikle boyutuna, kapsadığı alana veya yapısına göre sınıflandırılır. Aşağıdaki sınıflandırma ağın kapsadığı alanlara göre yapılmıştır [49] [50] [31] [32].

### 2.2.1 Yapılarına Göre Wired Computer Networks

Bilgisayar ağları, kaynaklara erişim, kapsadığı alan ve söz sahibi olma şekline göre üç gruba ayrılır.

#### 2.2.1.1 LAN (Local Area Network)

Local area network, göreceli olarak küçük olan sistemlerden ve iletişim ortamından oluşur. Yüksek hızlı, küçük alanları (bir bina, bir firma, bir bölüm, bir oda) kapsayan bir veri ağıdır. Yerel ağ içinde bilgisayarlar, sunucular, iş istasyonları, yazıcılar, çiziciler ve diğer çevre birimleri yer alabilir. Normalde tek tür iletişim kuralına eğilim gösterir.

Ancak farklı iletişim kurallarının (ağ protokolleri) kullanıldığı ağlar da mevcuttur. Yerel bilgisayar ağları, genellikle tek bir organizasyon tarafından sahiplenilir ve yönetilirler.

### 2.2.1.1.1 Ethernet Kavramı ve Standartları

Ethernet Xerox’un Palo Alto Research Center (PARC)’da 1976’da geliştirilmiştir.

Ethernet, 1980’de ilk olarak yayınlanan IEEE (Institute of Electrical and Electronics Engineers) 802.3 standardına teknolojik olarak temel sağlamıştır. Bundan kısa bir süre sonra, Digital Equipment Corporation, Intel Corporation ve Xerox Corporation beraberce IEEE 802.3 ile uyumlu bir Ethernet (sürüm 2.0) standardını geliştirdiler ve duyurdular. Ethernet ve IEEE 802.3, birlikte, şu anda yerel ağ protokolleri pazarında en büyük pazar payına sahiptir. Bugün Ethernet terimi genel olarak IEEE 802.3’ün de dahil olduğu Ethernet standartlarına uyan tüm taşıyıcı sinyalin algılanması, CSMA/CD (Carrier Sense Multiple Access/Collision Detection) ağları için kullanılır. [57]

İlk geliştirildiğinde Ethernet, uzun mesafeli düşük hızlı ağlar ve özel, yüksek hızlı veri taşıyan ancak mesafe kısıtlaması olan bilgisayar odası ağları arasındaki boşluğu doldurmak için tasarlanmıştı. Ethernet, yerel haberleşme ortamının dağınık bazen yüksek oranda ağır trafik taşıması gereken uygulamalar için uygundur. [58] [57]

Ethernet veriyi elektrik sinyaliyle kodlar. 10 Mbps (Megabit per second-Saniyede Saniyede Bir Milyon Bit) sistemlerde kodlama biçimine Manchester kodlaması denir. Bu sistem voltajda değişiklik yaparak ikilik sayıları sıfır ve bir olarak gösterir. Bir zaman diliminde voltajdaki artış ya da düşüşe bit periyodu denir, bitin ikili sayı değerini gösterir. [58] [57]

Ethernet’ler, kullanılan kablo ve iletişim hızlarına göre ayrıca sınıflandırılırlar. 10 Mbps hızıyla haberleşenler genel olarak Ethernet, 100 Mbps hızıyla haberleşenler Fast Ethernet, 1000 Mbps hızıyla haberleşenler Gigabit Ethernet olarak isimlendirilirler. [58] [60]

##### 2.2.1.1.2 Ethernet Ağ Elemanları

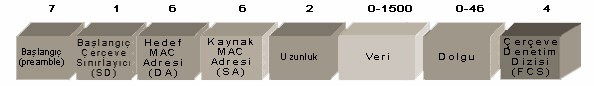
Ethernet LAN, network nodes ve fiziksel bağlantı medyalarını içerir. DTE (Data Terminal Equipment) ve DCE (Data Communication Equipment) olarak başlıca iki gruba ayrılırlar. Aygıtlar veri çerçevelerinin hedefi ya da kaynağı olabilir. DTE aygıtları kişisel bilgisayarlar, iş istasyonları ve dosya sunucuları olabilir. DCE aygıtları gelen veri çerçevelerini ağa ileten cihazlardır. Network switch, Repeater ve modemler DCE aygıtlarıdır [59] [60].

##### 2.2.1.1.3 CSMA/CD- Carrier Sense Multiple Access/Collision Detection

Ethernet’te veri iletim yoluna erişmek için kullanılan tekniktir. Ethernet, bir broadcast network teknolojisidir. Bu teknik veri iletim yoluna bağlı tüm birimlerin ağ ortamına erişmesini sağlar. Sadece bir düğüm belli bir zamanda ağı kullanmaya elverişlidir. Bu kavramda bir istasyon ağa bir çerçeve iletmek istediğinde ağın başka bir istasyon tarafından kullanılmadığından emin olmalıdır. Veri iletim yolu, bağlı olan tüm birimlerin veri aktarımına açık olduğu için aynı anda farklı birimler tarafından veri aktarılmaya çalışılması collision’a neden olur. Çatışma durumunda tüm veriler bozulur ve yeniden aktarılması gerekir. Bu nedenle veri gönderen bir düğümün aktarım sonrası hattı dinlemesi ve olası çatışmaların farkına varması gerekir. Collision denetimi, veri aktarmak isteyen her iki istasyonun benzerliğini fark eder ve eş zamanlı olarak ağın boş olduğunu tespit edebilir. Her iki istasyonda ağa çerçeve gönderdiğinde milisaniyeler sonra her iki çerçeve çarpışır. Çarpışmalar Ethernet’te normal olaylardır. Böyle bir çarpışma olduğunda iki istasyonda taşımayı durdurur rastgele bir gecikmeden sonra çerçeveyi yeniden gönderir. Gecikmenin rastgele olması önemlidir, aksi takdirde aynı çarpışma çok kez ortaya çıkacaktır. Her iki bilgisayar da çatışmayı sezince, veri aktarımına bir süre ara verip ikili üssel geri çekilme (binary exponential backoff) algoritmasını kullanılarak tekrarlarlar. Ethernet'te kullanılan CSMA/CD, veri çerçevelerini alır ve taşır, veri çerçevelerini OSI üst katmanına geçirmeden önce çözer, adreslerin geçerliğine bakar ve ağda ya da veri çerçevesinde oluşan hataları tesit eder. [57] [58] [59] [60]

##### 2.2.1.1.4 MAC (Media Access Control) Adres Kavramı

Ethernet ağ cihazlarına, 48 bitlik, onaltılık sayı düzeninde ve bir eşi daha olmayan seri numarası verilir. LAN içerisindeki yerel erişimler bu adresler kullanılarak gerçekleşir. Bu numaralar, üretici firmalar tarafından fabrikada verilmektedir. Örnek olarak 12:34:56: 78:90: AB bir MAC adresidir. Her üretici firmanın kendi ürünleri için kullanabileceği belli bir MAC adresi alanı vardır [15]. Ethernet çerçeve yapısı Şekil 2.2.1.1.4’de gösterilmiştir. [59] [61]



Şekil 2.2.1.1.4: Computer Networks

##### 2.2.1.1.5 Ethernet Standartları

Tablo 2.2.1.1.5’de Ethernet standartları, kablo tür ve mesafeleri verilmiştir. [58] [60]

Tablo 2.2.1.1.5: Ethernet standartları

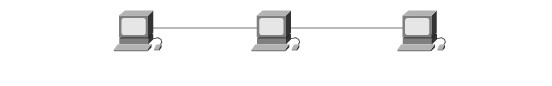
|  |  |  |  |
| --- | --- | --- | --- |
| Standart | Bant  Genişliği | Azami Mesafe | Kullanılan Kablo |
| 10Base-2 | 10 Mbps | 185 metre | 50 ohm sonlandırıcı ile sonlandırılmış ince koaksiyel (eşeksenel) kablo. |
| 10Base-5 | 10 Mbps | 500 metre | 50 ohm sonlandırıcı ile sonlandırılmış kalın koaksiyel kablo. |
| 10Base-T | 10 Mbps | 100 metre | Kategori 3, Kategori 4, Kategori 5 UTP (Kılıfsız Büklümlü Tel Çifti) kablo. |
| 10Base-F | 10 Mbps | 2Km (Kilometre) | Fiber Optik (Optik Lif Kablo) |
| 100Base-TX | 100 Mbps | 100 metre | Kategori 5 UTP |
| 100Base-T2 | 100 Mbps | 100 metre | Kategori 3, Kategori 4, Kategori 5 UTP |
| 100Base-FX | 100 Mbps | 400 metre-2000 metre | Fiber Optik |
| 1000Base-LX | 1000 Mbps | 440 metre-3 Km | Tek Mod veya Çoklu Mod Fiber Optik kablo. |
| 1000Base-SX | 1000 Mbps | 220 –550 metre | Çoklu Mod Fiber Optik kablo. |
| 1000Base-CX | 1000 Mbps | 25 metre | Bakır kablo. |
| 1000Base-T | 1000 Mbps | 100 metre | Kategori 5 UTP |

##### 2.2.1.1.6 Network Topologys

Topoloji, bilgisayarların birbirine bağlanma şekillerini tanımlayan genel bir terimdir. Yaygın olarak kullanılan topoloji türleri şunlardır;

###### 2.2.1.1.6.1 Bus Topology

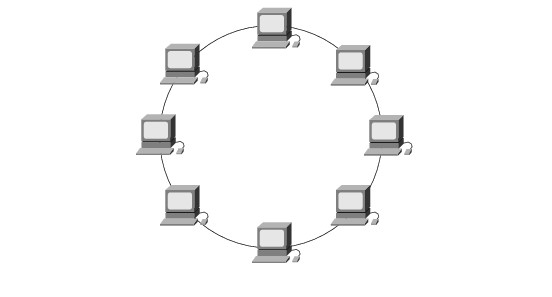
Tüm bilgisayarların aynı kabloya bağlı oldukları sistemdir. Tüm bilgisayarlar ortamı dinleyerek kendilerine gelen veriden haberdar olurlar.



Şekil 2.2.1.1.6.1: Veriyolu Topoloji

###### 2.2.1.1.6.2 Ring Topology

Ağ bir düğümden diğerine geçerek uzar. Düğümler arasındaki bağlantıların mutlaka bir halka oluşturması gerekir. Elektrik sinyali tek yönlüdür. Her noktada sinyal kuvvetlendirilir.



Şekil 2.2.1.1.6.2 : Ring Topology

###### 2.2.1.1.6.3 Star Topology

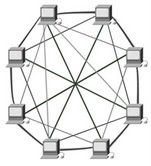
Yıldızağlarda tüm düğümler merkezdeki bir düğüme bağlanırlar ve düğümler arasındaki haberleşme merkez düğüm üzerinden gerçeklenir.



Şekil 2.2.1.1.6.3: Star Topology

###### 2.2.1.1.6.4 Mesh Topology

Düğümler arasında bağlantılar oluşturarak, tüm düğümlerden diğerlerine birkaç yol üzerinden erişimi sağlayan topolojilere mesh topoloji oluşturur [62].



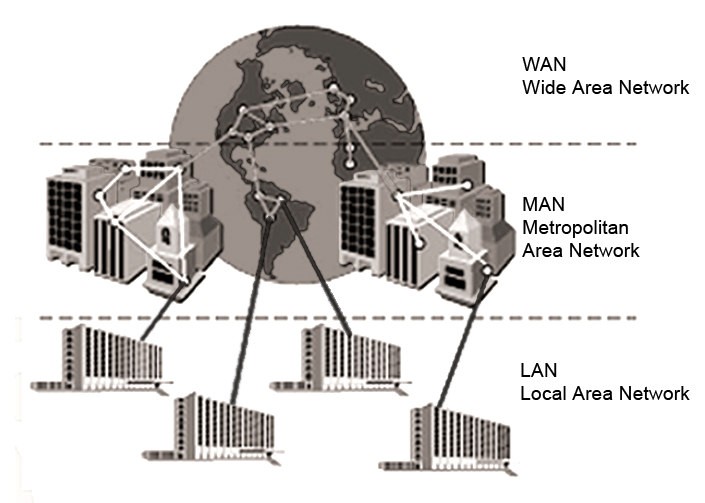
Şekil 2.2.1.1.6.4: Mesh Topology

#### 2.2.1.2 MAN-Metropolitan Area Network

Local network’lardan daha geniş, genellikle birkaç mevcut yerel bilgisayar ağının birleştirilmesi sonucu kurulan ağlardır. Genelde şehir içi uzak bağlantılar söz konusu olduğundan ve şehrin bir kısmını kapsadığından kentsel ağlar denmiştir. Mesafenin etkin olarak kapsanması gerektiği ve ağa bağlı her bölge arasında tam erişim gerekmediğinden değişik donanım ve aktarım ortamları kullanılır.

#### 2.2.1.3 WAN-Wide Area Network

Local veya metropolitan ağların birleşmesi ile oluşturulurlar. Şehir, ülke, kıta, hatta dünya çapındaki bilgisayarların birbirleriyle ilişkilendirilmesi sonucunda oluşmuş veya kurulmuş olan bilgisayar ağlarıdır. Geniş alan ağı, coğrafi olarak uzak mesafelerdeki kentsel ağdan geniş her tür ağı birbirine bağlamak için kullanılır. Ülkenin ya da dünyanın çeşitli bölgelerindeki yerel alan ağları birbirine bağlayan yapıdır [49] [50] [51] [31]



Şekil 2.2.1.3: Computer Networks

### 2.2.2 OSI (Open Systems Interconnection)

Bilgisayarlar arası iletişimin başladığı günden itibaren farklı bilgisayar sistemlerinin birbirleri arasındaki iletişim daima en büyük problemlerden birisi olmuş ve bu sorunun üstesinden gelebilmek için uzun yıllar boyunca çeşitli çalışmalar yapılmıştır. 1980'li yılların başında ISO (International Standarts Organization) bilgisayar sistemlerinin birbirleri ile olan iletişiminde ortak bir yapıya ulaşmak yönünde çabaları sonuca bağlamak için bir çalışma başlatmıştır. Bu çalışmalar sonucunda 1984 yılında OSI (Open Systems Interconnection) referans modeli ortaya çıkarılmıştır. Bu model sayesinde değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir. OSI referans modelinde, iki bilgisayar sistemi arasında yapılacak olan iletişim problemini çözmek için 7 katmanlı bir ağ sistemi önerilmiştir. Bir başka deyişle bu temel problem 7 adet küçük probleme bölünmüş ve her bir problem için ayrı bir çözüm yaratılmaya çalışılmıştır. OSI modeli, bir bilgisayarda çalışan uygulama programının, iletişim ortamı üzerinden başka bir bilgisayarda çalışan diğer bir uygulama programı ile olan iletişiminin tüm adımlarını tanımlar. En üst katmanda görüntü ya da yazı seklinde yola çıkan bilgi, alt katmanlara indikçe makine diline dönüşür ve sonuç olarak 1 ve 0’lardan ibaret elektrik sinyalleri halini alır.

OSI başvuru modelinin katmanları, uygun katmanlara arayüz oluşturmakta tasarlanmıştı. Örneğin sunum katmanı, Uygulama ve Oturum katmanları arasında arayüz oluşturmak için tasarlanmıştı. Her katman, diğer katmanlardan bağımsız belirgin işlevleri tanımlamaktadır. Bu da iletişim sisteminin bölünmesine izin verir. Böylece ağ mimarisi tasarım işlerliği her katmanda değişik problemlerin tutulmasına izin verir. Burada, tüm işletim sisteminin karmaşıklığı bölünüp basit süreçlere adreslenir. Katmanlı ağ mimarisi bu tarzda işlerliğin çoklu fiziksel aygıtlar arasında ağ tasarımının doğal bölünmesini sağlar. OSI’nin gelişi her türden bilgisayarın birbiri ile iletişimi sorununa çözüm olmuştur. OSI modelinin yedi katmanı vardır. [52] [53] [54]

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Uygulama**  1  2  3  4  5  6  7 | | **Sunum**  7  1  2  3  4  5  6 | | **Oturum**  6  7  1  2  3  4  5 | | **Ta**ş**ıma**  5  6  7  1  2  3  4 | | **A**ğ  4  5  6  7  1  2  3 | | **Veri Ba**ğ**ı**  3  4  5  6  7  1  2 | | **Fiziksel**  2  3  4  5  6  7  1 | | |  | | --- | | Kullanıcıya en yakın katmandır.  Kullanıcının elinin altındaki uygulamaları burada yer alır. | |
| |  | | --- | | Bu katmanda gelen bilginin karakter takımı dönüşümleri, şifreleme gibi işlemleri ile uğraşılır. | |
| |  | | --- | | İki bilgisayar üzerindeki uygulamaların birbirini fark ettiği katmandır. | |
| |  | | --- | | Burada, gelen bilginin doğruluğu araştırılıp, hatalıysa düzeltilmesine çalışılır. |  |  | | --- | | Bağlantıyı sağlayan yönlendirme protokolleri bu katmanda çalışır. | |
| |  | | --- | | Fiziksel adresleme, ağ yerleşim biçimi, akış denetimi gibi işler bu katmanın görevidir. |  |  | | --- | | Bu katman, modülasyon teknikleri, çalışma voltajı ve sıklık (frekansı) gibi elektriksel ve mekanik özellikleri belirleyen katmandır. | |

Tablo 2.2.2: OSI Katmanları

#### 2.2.2.1 Application Layer

Kullanıcıya en yakın katmandır. Kullanıcı uygulamalarına dosya aktarım, elektronik mektuplaşma, uzaktan dosya erişimi, ağ yönetimi, terminal protokolleri gibi standartlar geliştirilmiştir. Ayrıca uygulamaların birbirleriyle iletişimini kontrol eder. Diğer bilgisayarlar ile haberleşen bir uygulama, OSI uygulama katmanı kavramlarını kullanıyor demektir. Uygulama katmanındaki uygulamaların haberleşme yetenekleri bulunmalıdır. Örneğin, haberleşme yetenekleri bulunmayan bir kelime işlemci programı, haberleşme ile ilgili kodlar içermeyecek ve OSI uygulama katmanı kullanmayacaktır. Ancak, kelime işlemci programına, dosyaların gönderilmesi gibi bir seçenek eklenirse, kelime işlemci programı OSI uygulama katmanı kullanmak zorunda kalacaktı [5, 6, 7].

OSI uygulama katmanının kullandığı bazı uygulamalar şunlardır;

Telnet, http (Hypertext Transfer Protocol), FTP (File Transfer Protocol), NFS (Network File System), SMTP (Simple Mail Transfer Protocol).

#### 2.2.2.2 Presentation Layer

Veriyi alıcı cihaz tarafından okunabilir hale getirmekten sorumlu olan katmandır. Gönderilen verinin alıcı cihaz tarafından nasıl okunacağını belirtir. Verinin biçimlendirilmesi, şifrelenmesi ve sıkıştırılması görevini üstlenir [7]. Bu katmanın temel amacı, ASCII (American National Standard Code for Information Interchange) metni, EBCDIC (Extended Binary Coded Decimal Interchange Code) metni, BCD (Binary-Coded Decimal) gibi veri formatlarını tanımlamaktır. Şifrelemede, örneğin, FTP kullanırken ikilik ya da ASCII modda iletim yapılması sağlanabilir. Eğer ikilik mod seçilmiş ise, gönderici ve alıcı, dosyanın içeriğini değiştirmez. Eğer ASCII mod seçilmiş ise, gönderilen metni standart ASCII kodlarına dönüştürür ve veriyi gönderir. Alıcı, standart ASCII kodlarını bilgisayarda kullanılan karakter kümesine bağlı olarak yeniden biçimlendirir. [55] [54]

#### 2.2.2.3 Session Layer

Uygulamalar arasındaki oturumları başlatır, sonlandırır ve yönetir. Oturum katmanı eşzamanlı olarak iletişimi sağlar. Oturum katmanı, oturum olarak adlandırılan konuşmaların nasıl başlayacağını, biteceğini ve kontrol edileceğini tanımlar. Bu, birden çok iki yönlü mesajın idare ve kontrol edilmesini de kapsar. Bu sayede uygulama, sadece belli mesaj dizisinin iletilmesi tamamlandığında gerekli işlemleri yapmaya başlar. Oturum katmanının, gelen verinin kesintisiz bir görüntüsünü elde edebilmesini de bu sağlar. Örneğin, otomatik para çekme makinelerinde siz parayı almadan, para hesabınızdan düşürülmez. Oturum katmanı, hangi işlemlerin aynı otururumun parçası olduğunu ve oturumun kapatılabilmesi için hangi işlemlerin tamamlanması gerektiğini belirleyebilir. [55]

#### 2.2.2.4 Transport Layer

Birincil görevi gönderici ve alıcı arasındaki veri akışının kontrolü ve verinin alıcıya ulaştığından emin olmaktır. Alıcı cihazın veriyi almaya hazır olup olmadığı ve veri gönderildikten sonra alıp almadığı gibi kontrollerin yapıldığı katmandır. Burada, gelen bilginin doğruluğu araştırılıp, hatalıysa düzeltilmesine çalışılır. Bu katman güvenilir bir dağıtımdan sorumludur. Bu da dağıtım sunumudur. Daha çok paket dağıtım sunumunu garantilemeye çalışan taşıma katmanı veri dağıtmayı garantiler. Eğer veri “paketi" olarak anılan paket dağıtılmayabilir ise istekte bulunan sunucuya gecikmenin olacağını bildiren bir ileti gönderilir. Dağıtımı garantilemek için kullanılan yöntemler arasında, bilgilendirme iletileri, akış denetimi ve veri paketlerine atanan paket sıra numaraları yer alır. Bu katman iletinin doğru olarak dağıtıldığını garanti etmez. Sadece dağıtıldığını garanti eder. Düzeltmeye gereksinimi olan bir ileti varsa onu yeniden belirlemek ve yeniden göndermek sunum ve oturum katmanının sorumluluğudur [5]. Hata giderme imkânı sunan ya da sunmayan protokollerin seçimine imkân sağlar. Gelen veriyi, aynı makine üzerindeki farklı uygulamalara (örneğin TCP soketlerine) göndermek için çoğullama da bu katmanda yapılır. Sırayı bozan bir paket alındığında, paketin yeniden istenmesi de yine bu katmanda gerçekleştirilir. [55] [54]

#### 2.2.2.5 Network Layer

Bu katman, paketlerin uçtan uca gönderimini tanımlar. Ağ katmanı bilgiyi ağa yerleştirmekten sorumludur. Ağ katmanı bunu yapabilmek için, uç noktaların belirlenmesinde kullanılmak üzere mantıksal adresleme yapar. Bu katman sunucu adres alanından kaynaklanan iletileri düzeltir ve daha ileri geçirir. Eğer sınanan sunucu uzak bir sunucu değilse paket, uzak sunucunun yolunu içeren farklı bir ağ dilimine geçirilir (forward). İleti ileri geçirme işlemi yönlendirme ile ilintilidir. Yönlendirme işlemi, iletinin uzaklara erişmesi için en kısa ve en iyi yolun bulunmasıdır. Bilginin aktarılacağı yolun bulunması bir hesaplamaya dayanmaktadır. Sınanan ileti bir sunucu için ise daha ilerde işlenmek üzere taşınma katmanında tutulur. Farklı ortamlarda, iletilebilecek maksimum veri miktarının farklı olmasından dolayı yaşanan sıkıntıları gidermek amacıyla, bir paketi daha küçük paketlere bölme işlemi de bu katmanda tanımlanır. [55] [54]

#### 2.2.2.6 Data Link Layer

Gönderilecek verinin elektronik sinyallere dönüştürülüp kabloya iletilmesine ve kablodan gelen elektronik sinyallerin veriye dönüştürülmesini sağlayan katmandır. Bu dönüştürme işlemi kullanılan ağ teknolojisine göre değişkenlik gösterebilir. Elektronik sinyallerin kablo üzerinde sorunsuz bir şekilde ilerleyip ilerleyemediğinin kontrolü bu katmanda yapılır. Ayrıca bu katmanda fiziksel adresleme yapılır [7]. Fiziksel katmandan gelen bir dizi 0’lar ve 1’ler çerçeve ve paketlere dönüştürülür. Çerçeveler ve paketler, iletilerin kaynak ve varış adresleri, gerçek ileti daha sonraki katmanlarda istenen herhangi bir denetim bilgisini içerir. Veri Bağı katmanı veriyi fiziksel katmana göndermeden önce özel denetim bilgilerini ekler ve bu bilgileri veriyi ağ katmanına göndermeden önce bilgiden soyar alır. Veri bağı katmanında bazı hata düzeltme işleri yapılır. CRC (Cyclic Redundancy Check), ECC (Error Correction Codes) ile bit hatası yakalanır, düzeltilir. [55] [54]

#### 2.2.2.7 Physical Layer

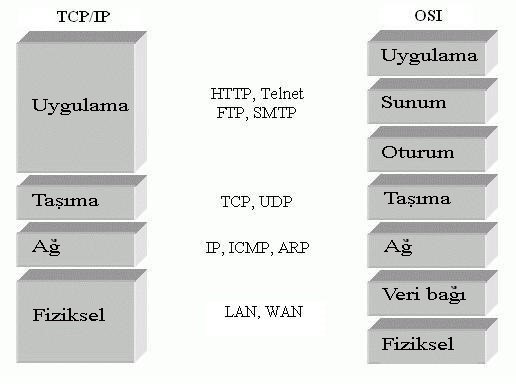
Veri bağı katmanı tarafından elektronik sinyallere dönüştürülen verinin taşınmasından sorumludur. Basit olarak ağ kablosudur. Gerçek kablolama ile bilginin konulması ve alınmasının yapıldığı katmandır. Mekaniksel, kablolama ve elektriksel sinyallerin ayrıntıları burada tutulur. Bunlar kullanılan konnektör bağlayıcı tipi, kullanılan ortamın tipi (eş eksenli, bükülmüş tel çifti veya fiber optik gibi) ve bant genişliğidir. Bu katman duvarlar boyunca koşan kablolar, her bilgisayarın arkasında yer alan bağlayıcılar ve elektriksel sinyallerin özellikleri ile ilgilidir. [55] [54]

### 2.2.3 TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)

TCP/IP birçok küçük protokolden oluşur. Adını en çok bilinen ikisinden (TCP ve IP) alır [6]. TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Birçoğu, IP paketlerinin alt katman protokollerine nasıl taşınacağını gösterir. Setteki anahtar protokoller TCP, IP ve UDP (User Datagram Protocol)’dür. TCP/IP ilk günden beri yerel alan ağları, yerel ve geniş alan ağları bağlantısı, bilgisayar ağı yönetimi ve bilgi servisi sağlanması gibi yeni ortaya çıkan konulara hitap etmektedir. Protokol kümesi akla gelebilecek her tip bilgisayara destek vermektedir. TCP/IP’nin kaynak kodu genel ortamda bulunup, kullanımı teşvik edilmektedir.

TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan verilerin tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek veri bir kerede gönderilemeyecek kadar büyük ise TCP onu uygun boydaki segmentlere böler ve bu bölütlerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni birtakım uygulamalar da daha kolay geliştirilebilmektedir. Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP’de IP katmanını çağırmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler. Belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine katmanlaşma adı verilir. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır [17]. Uygulama katmanı altında sırasıyla taşıma, yönlendirme ve fiziksel katman yer alır. Taşıma katmanında TCP ve UDP protokolleri, yönlendirme katmanında IP, ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) tanımlıdır. Fiziksel katman için varolan tanımlar (Ethernet) geçerlidir. [63]

Şekil 2.2.3’de TCP/IP mimarisi açıklanmış ve OSI katmanları karşılaştırması gösterilmiştir.



Şekil 2.2.3: TCP/IP ve OSI karşılaştırması

#### 2.2.3.1 Uygulama Katmanı Protokolleri

Uygulama katmanı, SMTP, HTTP, FTP, Telnet gibi protokoller üstünde bulunan programlara hizmet verirler [44].

**SMTP**: Temel elektronik posta olanağını sağlar. SMTP birbirinden ayrı bilgisayarlar arasında bir mesaj aktarımı mekanizmasını üretir. SMTP postalama listesi, kabulleri geri döndürme ve ileriye geçirmeyi (forwarding) içine alan özellikleri taşır. SMTP protokolü mesajların yaratılma yöntemini belirlemez. Mesaj yaratıldıktan sonra, SMTP mesajı alır ve TCP yi kullanarak diğer bilgisayardaki SMTP modülüne gönderir. Hedef SMTP modülü yerel elektronik posta paketini kullanıcının posta kutusuna gelen mesaj olarak koyar. [64]

**HTTP:** Web sayfalarının alışverişini sağlar. [44]

**FTP:** Kullanıcıların komutlarına bağlı olarak dosyaları bir sistemden diğerine göndermede kullanılır. Hem ikili hem de metin dosyalarına yer verilir. Protokol kullanıcı erişimini denetlemek için olanaklar üretir. Kullanıcı dosya aktarımını istediği zaman, FTP denetim mesajlarının değişimi için hedef sisteme TCP bağlantısını hazırlar. Bu durum kullanıcının ID ve anahtar sözcüğünü aktarması kullanıcıya dosyayı belirlemesi ve dosya eyleminin başlatılmasına izin vermek demektir. Bir kez aktarım geliştirildiğinde ikinci bir TCP bağlantısı veri aktarımını hazırlar. Dosya aktarımı veri bağlantısı üzerinden yapılır ve uygulama düzeyinde herhangi bir başlık ve denetim bilgisi yükü getirmez. Aktarım tamamlandığı zaman, bağ denetimi tamamlamayı sinyal eder ve yeni bir dosya aktarım komutu kabul edilir. [64]

**TELNET:** Terminalde ve kişisel bilgisayardaki kullanıcının, uzak bilgisayar ve fonksiyonlarını sanki doğrudan bilgisayara bağlıymış gibi çalışmasına izin verir. Bu protokol basit scroll-mode terminallerde çalışmak üzere tasarlanmıştır. TELNET gerçekte iki modülde çalışır. Kullanıcı TELNET, terminalin I/O modülü ile etkileşim için yerel terminal ile iletişir. Böylece gerçek terminal karakteristiklerini bilgisayar ağı standartlarına dönüştürür ya da bunun tersi bilgisayar ağı standartları gerçek terminal karekteristiklerine dönüşür. Sunucu TELNET, uygulama ile etkileşir ve uzak terminalin uygulamaya yerelmiş gibi davranmasını sağlar. Kullanıcı TELNET ve sunucu TELNET arasındaki trafik TCP bağlantısı üzerinden sağlanır. [64]

#### 2.2.3.2 Taşıma Katmanı Protokolleri

TCP/IP’de ulaşım katmanı için TCP ve UDP olarak adlandırılan iki protokol tanımlıdır. TCP bağlantılı düzene dayalı protokoldür. Bağlantılı düzende, gönderici ve alıcı iletişim başlamadan önce birbirleriyle anlaşırlar. İki taraf iletişim yapma konusunda istek ve onaylarını birbirlerine gönderirler. UDP ise bağlantısız düzenli basit bir protokoldür. Bu protokolde iletişim başlamadan önce gönderici ve alıcının bir anlaşmaya varmalarına gerek yoktur. [44] [64]

**TCP (Transmission Control Protocol):** TCP, şu fonksiyonları gerçekleştirmektedir:

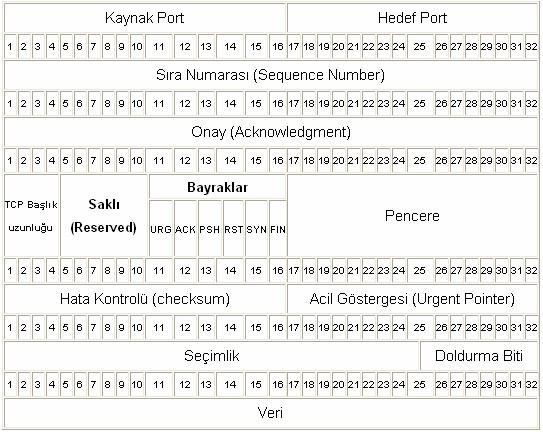
Multiplexing

Troubleshooting (Reliability)

Windowing kullanarak akış kontrolü

Bağlantı kurulması ve bağlantının sonlandırılması

Data transfer



Tablo 2.2.3.2: TCP paket formatı

Multiplexing: Gelen verinin hangi uygulamaya verileceğine karar verilme sürecidir. Uygulama katmanı ile taşıma katmanı protokolleri arasında port olarak adlandırılan bir geçit tanımlıdır. Her portun 16 bitlik bir numarası vardır ve her uçta 216 adet port tanımlıdır.16 bitlik port no, bir iletim kontrol protokolü ve 32 bitlik IP adresi soketi oluşturur. [44] Port numaraları 1 ile 65536 arasında yer alır. TCP ve UDP her biri 65,536 portu kullanmıştır [18]. Cihazlar, port numaralarını 1024’ten başlayarak dinamik olarak tahsis ederler. Yaygın olarak bilinen port numaraları (1–1024) sunucular tarafından kullanılır. FTP, Telnet sunucular gibi, bir hizmet sağlayan uygulamalar, yaygın olarak bilinen bir portu kullanarak bir soket açarlar ve bağlantı isteklerini dinlerler. İstemcilerin yaptığı bu bağlantı istekleri hem kaynak hem de hedef port numaralarını içermek zorundadır ve sunucular tarafından kullanılan port numaraları yaygın olarak bilinen portlar olmak zorundadır [6]. 0 ve 255 arası port numaraları, standart uygulama katmanı hizmetlerine erişim için ayrılmıştır. [44] Port numaraları birden fazla uç-nokta bağlantısı için kullanılabildiğinden, kullanıcılar bir port kaynağını eşzamanlı olarak paylaşabilir. [65]

Troubleshooting: TCP güvenli veri aktarımı sağlar. Bu amaçla TCP başlığı içindeki sıra ve onay numaralarını kullanarak veri baytlarını numaralandırır. Her iki doğrultuda da güvenlik sağlar. Bunu bir doğrultuda sıra numarası (squence number) alanını ve diğer doğrultuda acknowledgement field kullanarak sağlar. [55]

Windowing kullanarak akış kontrolü: TCP akış kontrolünü TCP başlığındaki sıra ve onay numaralarının yanında pencere (window) alanını kullanarak gerçekleştirir. Pencere alanı, TCP penceresinde ne kadar alan olduğunu gösterir. Alış denetimi için kullanılır. 16 bitliktir [19]. Herhangi bir anda izin verilen onaylanmamış en fazla bayt sayısını belirtir. Pencere küçük olarak başlar ve hatalar oluşana kadar büyür. Ağ performansına bağlı olarak yukarı veya aşağıya doğru kayar. Pencere dolu olduğunda, gönderici veri göndermez. Böylelikle veri akışı kontrol edilir. Pencere alanı alıcı tarafından, göndericiye bir sonraki onayı almak için durup beklemeden önce ne kadar veri gönderebileceğini söylemek için kullanılır. Diğer TCP özelliklerinde olduğu gibi, pencere kaydırma simetriktir. Her iki tarafta alır ve gönderir. Pencere kaydırma tüm durumlarda göndericinin iletim yapmayı durdurmasını gerektirmez. Pencere dolmadan önce bir onay alınırsa, yeni bir pencere başlar ve gönderici o pencere dolana kadar veri göndermeye devam eder. [55]

Bağlantı kurulması ve bağlantının sonlandırılması: TCP bağlantısı, diğer özellileri çalışmaya başlamadan önce kurulur. Bağlantı kurulması, sıra ve onay alanlarına ilk değerlerin atanması ile kullanılacak port numaraları üzerinde anlaşma sürecidir. [55]

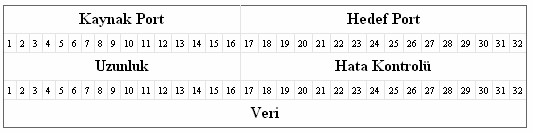
Veri aktarımı: TCP, kaybolan segmentleri yeniden gönderir ve sıralı olarak iletilmemiş segmentleri sırasına koyar. Böylelikle yeniden iletim yapılmasına gerek kalma. [55]

##### 2.2.3.2.1 UDP (User Datagram Protocol)

UDP, TCP / IP protokol grubunun iki taşıma katmanı protokolünden birisidir. Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokolü yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir yordam içerir. Bu protokol hareket yönlendirmelidir. Paketin teslim garantisini isteyen uygulamalar TCP protokolünü kullanır. WAN ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır. UDP bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir. UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır. UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur. UDP protokolünü kullanan programlara örnek olarak 161 no' lu portu kullanan SNMP servisini verebiliriz.

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere tasarlanmıştır. TCP’de olduğu gibi UDP’de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir, bu kez numarası alanına UDP’ ye ait değer yazılır. Fakat UDP, TCP’nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP’ nin tek sağladığı port numarasıdır. Böylece pek çok program UDP’ yi kullanabilir. Daha az bilgi içerdiğinden UDP başlığı TCP başlığına göre daha kısadır. [23]

Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren tüm bilgidir [67].



Tablo 2.2.3.2.1: UDP paket formatı

##### 2.2.3.2.2 UDP ile TCP 'nin Farkları

UDP, gönderilen paketin yerine ulaştığını kontrol etmediğinden güvenilir bir protokol değildir. User Datagram Protocol’ün TCP' den farkı sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılması için olmasıdır; veri küçük boyutlu olduğu için parçalanmaya gerek duyulmaz. UDP protokolü ağ üzerinde fazla bant genişliği kaplamaz. UDP başlığı TCP başlığına göre daha kısadır.

Aktarım katmanında UDP’nin oluşturduğu veri bütününe “datagram”, TCP’nin oluşturduğu veri bütününe “segment” adı verilir. İkisi arasındaki temel fark, segmenti oluşturan veri grubunun başında sıra numarası bulunmasıdır. Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve herbir IP paketi birbirinden bağımsız olarak hedef cihaza gönderilir. Tablo 2.2.3.2.2’de TCP ile UDP farkları karşılaştırılmıştır.

Tablo 2.2.3.2.2: TCP ile UDP farkları

|  |  |  |
| --- | --- | --- |
| Servis | TCP | UDP |
| Bağlantı kurulumu | Zaman alır ancak TCP bunu güvenli şekilde yapar. | Bağlantıya gerek yoktur. |
| Teslim garantisi | Gönderildiğini onaylar. | UDP onay mesajı göndermeden, alıcı paketin alındığına dair sinyal göndermez. Kaybolan paketler tekrar iletilmez. |
| Paket ardışıklığı (paketlerin doğru sırası hakkında bilgi) | Ardışık numaralanmış paketler | UDP ardışıklık numarası vermez. Paketlerin sürekli ulaştığı veya kaybolduğu düşünülür. |
| Akış kontrolü | Alıcı göndericiye yavaşlaması için sinyal gönderebilir. | Paket akış kontrolü için  TCP' de kullanılan onay UDP' de geri dönmez. |
| Tıkanıklık kontrolü | Ağ cihazları TCP onayları sayesinde göndericilerin tavrını kontrol edebilir. | Onay olmadan ağ tıkanıklık sinyali gönderemez. |

UDP kullanmanın en önemli nedeni az protokol yüküdür. Video sunucu gibi gerçek zamanlı veri akışı gerektiren bir uygulama için TCP fazla yük getirir ve görüntü gerçek zamanlı oynamaz. Bu nedenle çoğa gönderim(multicast) uygulamalarında datagram soketler kullanılır. Ayrıca video ve ses görüntülerinde genelde az bir veri kaybı sesi veya görüntüyü bozmaz. Bu nedenle sıkı paket kontrolüne gerek yoktur. Eğer iyi bir fiziksel bağlantınız varsa hata oranı düşük olacaktır ve bu nedenle TCP'nin yaptığı hatalı paket kontrol işlemleri fazladan yük olacaktır [67].

#### 2.2.3.3 Network Layer Protocols

Yönlendirme katmanında tanımlı protokolleri bir üst katmandan gelen segmentleri alıcıya, uygun yoldan ve hatasız ulaştırmakla yükümlüdür [44].

##### 2.2.3.3.1 ARP (Address Resulotion Protocol)

ARP, her tür yayın ağında kullanılabilen OSI birinci katman adresleri ikinci katman adreslere çözümleyen, ikinci katmana ait genel bir protokoldür. Terminaller, yerel alan ağına dahil olduklarında ağ içindeki diğer terminallerle veri alışverişinde bulunabilmek için ARP paketleri yayınlarlar. Bu paketler, ağa dahil olan tüm terminallere ulaşır ancak hedef IP adrese sahip olan terminal bu pakete cevap verir. [69] Yerel ağlarda bir IP paketi gönderebilmek için veri bağı katmanı başlığı ve kuyruğu yaratılmalıdır. Bu yeni başlıktaki kaynak MAC adresi bilinmekte ancak, hedef MAC adresi bilinmemektedir. ARP, IP’nin hedef MAC adresini bulmak için kullandığı metottur [55].

##### 2.2.3.3.2 ICMP (Internet Control Message Protocol)

ICMP, TCP/IP' nin işlemesine yardımcı olan bilgilendirme protokolüdür. Her düğümde ICMP protokolü çalışır. Hata durumunda düğüm tarafından geri bilgilendirmeyi sağlar. Şu amaçlarla kullanılır;

TTL- Time to Live süresi dolduğu zaman paketin sahibine bildirim yapmak

Herhangi bir durumda yok edilen paket hakkında geri bildirim sağlamak

Parçalanmasın komutu verilmiş paket parçalandığında geri bildirim sağlamak

Hata oluşumlarında geri bildirim sağlamak

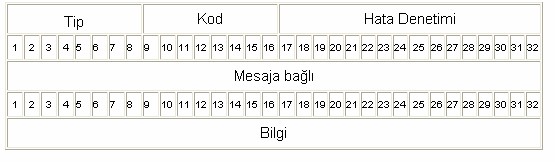
Paket başka bir yoldan gideceği zaman geri bildirim sağlamak

Güvenilir bir veri dağıtım protokolü değildir. Ortama geri besleme sağlar, IP' yi güvenilir bir protokol haline sokar. IP paketinin veri bölümünde taşınır. [68] ICMP mesaj tipleri Tablo 2.2.3.3.2’de gösterilmiştir [55, 68].

Tablo 2.2.3.3.2: ICMP mesaj tipleri

**Mesaj Amaç**

|  |  |
| --- | --- |
| Destination Unreachable  Time Exceed | Kaynak makineye paketi iletmek ile ilgili bir problem olduğunu bildirir.  Paketi iletmek için harcanan zaman uzamış ve paket düşürülmüştür. Yaşam süresi içerisinde hedefe ulaşmamış paketler son router üzerinde yok edilir. Time exceed paketi ile paket sahibi bilgilendirilir. |
| Source Quench | Akış kontrol işlevini yerine getirir, kaynak, iletilebilen veriden daha hızlı veri gönderdiğinde yavaşlaması için bu mesaj kullanılır. |
| Redirect | Yönlendirme ile ağ üzerindeki cihaza seçilebilecek en iyi yol bilgisi verilir. |
| Echo | Ping komutu ile test işlevini yerine getirir, bağlanırlılığı kontrol etmek için kullanılır. |
| Parameter Problem | Parametre sorunu paket başlık parametrelerinde oluşan hataları “parameter problem” mesajı ile geri bildirir. |
| Timestamp | Zaman damgası, alıcı kendisine gelen paketin alım için geçen süresini hesaplayıp Time Stamp Reply paketi ile süreyi kaynak düğüme bildirir. |
| Address Mask Request/Reply | Kullanılacak subnet mask öğrenmek ve hakkında bilgi edinmek için kullanılır. “Address Mask Reply” paketi ile geri gönderilir. |



Tablo 2.2.3.3.2.a: ICMP formatı

Tip 8 bittir, mesaj tipini belirler. Kod, 8 bit kullanır ve mesaj tipi alt gruplarına detaylı tanımlama sağlar. Hata denetimi 16 bit, ICMP mesajının hata denetiminin yapılabilmesi amacıyla kullanılır. Mesaj bağımlı, rezerve edilmiştir. Bilgi alanında IP başlığı kaynak ve hedef adresleri bilgileri yer alır [68, 70].

##### 2.2.3.3.3 IP (Internet Protocol)

Temel olarak datagram paketleri için bir iletim yolu belirleme işlevini yerine getirir.

IP’nin sağladığı fonksiyonlar şunlardır:

Global adresleme yapısı

Servis isteklerini tiplendirme

Paketleri iletim için uygun parçalara ayırma

Hedef alıcıda paketleri tekrar birleştirme

TCP, hedef bilgisi bulunan segmenti IP’ye verir. IP bu segmenti alır herhangi bir diğer datagram veya segmentten önce veya sonra hedef düğüme iletim için bir yol belirler. Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve her bir IP paketi birbirinden bağımsız olarak hedef düğüme gönderilir. Paketler üzerinde çok sınırlı hata kontrolü vardır. IP 16 bitlik checksum sağlar. Bu IP paketini alan düğümün IP başlığında bir bozulma oluşup oluşmadığını kontrol etmesini sağlar. Acknowledge mekanizması kullanmaz. Verinin internet katmanına bozuk ulaştığını değerlendirip yeniden gönderimi sağlayabilecek fonksiyona sahip değildir. Bu görev bir üst katmandaki TCP’de yapılır, TCP’nin kullanılmadığı durumlarda daha üst katman protokollerince yerine getirilir.

Akış kontrol ve paket sıralama mekanizmalarına sahip değildir. IP bağlantısız paket dağıtım servisi sunar [70].

##### 2.2.3.3.4 IP Adresleme

TCP/IP kullanılan ağlarda, adresleme IP adreslere dayanılarak gerçekleştirilir. Ağda bulunan iletişim kuracak her cihaza bir IP adresi atanır, diğer cihazlar bağlantı kurmak için bu adresi kullanır. IP adresleri şu anda yaygın kullanımda olan IP sürüm 4 (IPv4) için 32 bit boyunda olup, noktalarla ayrılmış 4 adet 8 bitlik sayıyla gösterilirler. Ağ katmanında paketler bir noktadan diğer noktaya iletilirken mantıksal adresler kullanırlar. Mantıksal adresler paketin kaynak ve gideceği en son yerin ağ adresini içerir. Adres alanı içinde varış noktasının ağ adresi ile düğüm adresi bileşimi bulunur. Adres uzunluğu 32 bittir. 232 adet IP adresi içerir, bu durumda 4.294.967.296 bilgisayar internete bağlanabilir. IP adresleri, bilgisayar ağlarını bölümlemek ve farklı büyüklüklerde bilgisayar ağları oluşmak üzere sınıflandırılmıştır. IP, 5 farklı adres formatını destekler, bunlar; A, B, C, D ve E sınıfı adreslerdir. Her adres sınıfı o adresi tanımlayan ilk baytın en anlamlı bitlerine yerleşen bir bit dizisi ile tanımlanır. Bu bit dizisini A, B, C sınıfı adreslerde ağ adresi ve sonrasında düğüm adresi takip eder. [44, 70].

A sınıfı adreslerde ilk bayt ağı tanımlamak için kullanılır. İlk bit 0’dır. Ondan sonraki 7 bit ağ adresini oluşturur. Geri kalan 24 bit ağdaki host sayısını belirler. 224-2 ile herbiri 16.777.214 adet bilgisayar içeren 126 adet altağ (subnet) kullanılabilir. Host bitlerinin tamamı 1 olan adresler yayın (broadcast) ve 0 olanlar ise ağ adresi olarak kullanılır.27-2 ile 126 olan altağ sayısı hesaplanır. 0.0.0.0 adresi varsayılan yönlendirme 127.0.0.0 adresi ise yerel çevrim için kullanılır [44]. İlk sekizli aralığı 1–126, geçerli ağ numaraları 1.0.0.0 – 126.0.0.0’dır [55].

B sınıfı adreslerde ilk iki bayt, ağı tanımlar. İlk iki bit adres sınıfını belirler, 1 ve 0 şeklindedir. Diğer 14 bit ağ adresini oluşturur, sonraki 16 bit ağdaki host sayısını belirler. Her biri 65.534 olmak üzere 16.384 adet altağa izin verir. 128.0.0.0 ve 191.254.0.0 adres aralığını kullanılır [66].

C sınıfı adreslerde ilk üç bayt ağı tanımlar. İlk üç bit(110) adres sınıfını belirler ve diğer 21 bit ağ adresini oluşturur. Kalan 8 bit ağdaki host sayısını belirler. 254 adet bilgisayar içeren 2.097.152 altağa izin verilir. 192.0.1.0 ve 223.255.254.0 aralığı kullanılır [55, 44].

D sınıfı adresler multicast adresleme için kullanılır. İlk dört biti 1110 şeklindedir.

224.0.0.0 – 239.255.255.255 adresleri kullanılır.

E sınıfı adresleme yedek olarak saklı tutulmaktadır. İlk dört biti 1111 şeklindedir.

Yerel ağlarda kullanılmak üzere 10.0.0.0, 172.0.0.0 ve 192.168.0.0 ağ adresleri saklı tutulmuştur [44].

IP adreslemesi IPv4 standartlarına göre yapılmakta, IP adresleri 32 bitten oluşmaktadır fakat bu IP adreslerinin tamamı tükenmek üzere olduğunda IP adresleri IPv6 standartlarına göre verilmeye başlanacaktır. Bu adresleme tekniğinde IP adresleri 32 değil 128 bitten oluşmaktadır [70].

#### 2.2.3.4 Data Link Layer

Gönderilecek verinin ağ ortamında nasil iletileceğini, fiziksel adreslemeyi ve ağ topolojisini tanımlar. Fiziksel kabloda çarpışma olmadan veri iletimini sağlamak (CSMA/CD) ya da verilerin bu medyaya nasıl konulacağı belirlemek ve yine verinin hatalara karşı kontrolünü yapmak, ağ üzerindeki diğer pc’lerin kimlik doğrulamalarını yapmak, anlık iletişimin kimin tarafından yapıldığını tespit etmek bu katmanın görevidir.

3. katmanda (Network Layer) paketlere dönüştürülen data, bu katmanda artık fiziksel ortama aktarılmadan önce son kez işlem görerek frame yapılara dönüştürülür. Çerçeveler verileri belli bir kontrol içinde göndermeyi sağlayan yapılardır. Veri bağlantı katmanı üzerinden iletimi yapılan her paket, source ve destination adreslerini içerir, yani her paket başlangıcı ve bitişi belli olacak şekilde özel bitlerle işaretlenir. Bu katmanda kullanılan protokollerden bazıları şunlardır:[161]

Seri hatlar üzerinde HDLC (High-Level Data Link Control)

• IEEE 802.3/802.2

• FDDI

• PPP

• X.25

• Frame Relay,

• ATM

• IEEE 802.5/802.2

Katmanın görevleri genel itibari ile şöyle özetlenebilir:

• Veri bağlantı katmanı, fiziksel katmana erişimi ve ağ birimlerini kullanarak gönderilecek verinin hedefinin belirlenmesini sağlar.

• MAC (Media Access Control) adresleri kullanılarak fiziksel bağlantılar arasında güvenli data iletimine imkân sağlar.

• MAC adresinin kullanımı sayesinde bilgisayarların aynı fiziksel bağlantıyı kullanmalarına ve birbirlerinde farklı şekilde tanımlanmalarına yardımcı olur. Her MAC adresi birbirlerinden farklı adreslere sahiptir. Ethernet kartlarına atanan donanım adresleri üretimleri sırasında atanır.

• Hata denetimin yapılmasını sağlar. Katman üzerinden gönderilen her bir paket için akış kontrolü sağlar, CRC hata kontrolü bu katman üzerinde yapılır. Eğer paketlerin iletimi sırasında hata meydana gelmişse, oluşan hata üst katmana iletilir.

1.Katman olan physical layer, ağ ortamını, gönderilecek verinin bitlere dönüşümünü ve ağ üzerinde taşınmasını denetler ve yönetir. Bu görevini yerine getirirken de üst katmanlarla olan iletişimi ve gönderilen verinin nereye gitmesi gerektiğini belirleyemez. Bunlar Data-Link Layer tarafından gerçekleştirilir. Bu katman gönderilecek bitleri organize eder ve gruplandırarak paket yapıya dönüştürür.

The Institute of Electrical and Electronic Engineers (IEEE), ağ standartlarını tanımlayan profesyonel bir kuruluştur. IEEE Project 802 adlı LAN standarda sahiptir. Yerel ağlarda yaygın olarak kullanılan IEEE 802.3 ve IEEE 802.5 standartları bu kuruluş tarafından tanımlanmıştır Bu standarda göre Data Link Katmanında oluşan iki alt katmanla yönlendirme gerçekleştirilir. Bunlar:

• Logical Link Control (LCC)

• Media Access Control (MAC)

**Logical Link Control (LLC):** Logical Link Control alt katmanı mantıksal bir arabirimi noktası kullanarak üst katmanlarla olan iletişimi sağlar. Bu standartlar 802.2 ile tanımlanır. Bozulmuş olarak giden paketlerin tekrar gönderilmesini sağlamak temel görevlerindendir. Flow Control yani alıcının işleyebileğinden fazla veri paketi gönderilerek boğulmasının engellenmesinden de LLC sorumludur. İlgili Protokole özel mantıksal portlar oluşturur (Service AccessPoints, SAP). Verinin kapsüllenmesi sırasında ağ katmanlarından gelen veriye Destination Service Access Point (DSAP) ve Source Service Access Point (SSAP) ekler ve tekrar paketlediği veriyi bir alt katman olan Media Access Control(MAC) katmanına aktarır. Böylece kaynak makinada ve hedef makinada aynı protokoller iletişime geçebilir (örneğin TCP/IP <==> TCP/IP şeklinde).[161]

**Media Access Control(MAC):** MAC alt katmanı, kullanılan teknolojiye bağımlı olarak Fiziksel Katmanla olan iletişimi kurmaktadır. Bu katman veriyi hata kontrol kodu (CRC-Cyclic Redundancy Code), hedef ve kaynak bilgisayarın MAC adresleri ile beraber çerçeve yapıya dönüştürür ve fiziksel katmana gönderir. Alıcıda da bu işlemleri tersine çevirip veriyi Data-Link içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.

Ayrıca bilgisayarların ağ ortamına erişim sistemini de organize eder. 2 çeşit ortama erişim kontrol protokolü vardır. Bunlar;

•**Deterministic**

•**Non-deterministic**

**Deterministic MAC Protocol:**

Sırayla ortama veri aktarımının yapılmasını sağlayan protokollerdir. Örneğin; Token-Ring protokolü bu çeşit bir protokoldür.

**Non-Deterministic MAC Protocol:**

Bu tür protokoller ilk gelen ilk servisi alır mantığıyla çalışır. Bundan dolayı ağda çarpışmaların olması muhtemeldir. Örneğin; Ethernet, Carrier Sense Multiple Access with Collision Detection-CSMA/CD protokolü bu çeşit protokoldür.

**Data Link Katmanındaki Switch ve Bridge'ler;**

Bridge ve switche’ler bu katmanda çalışır. Frame iletimi yapmaktadırlar. Switch ve Bridge aygıtları Data Link Layerda çalışarak MAC adresine göre ağı filtrelemeyi sağlarlar.

Ağda Hub aygıtlarının yerine Switch kullanmanın başlıca nedeni collision domain adı verilen trafikteki çakışmanın önlenmesidir. Hub aygıtları çok fazla çatışmaya neden olurlar.

2.2.3.4.1 PAKETLERİN FRAME YAPIYA DÖNÜŞTÜRÜLMESİ

Dijital sinyallere dönüştürülen ve tek başına anlaşılamayan veri için bu sinyalleri anlaşılabilir hale dönüştürme işlemine framing denir. Bu dönüştürme işlemi data link katmanı tarafından yapılmaktadır. Frame yapıdan anlaşılabilecek bilgilerin bazıları:[161]

•Hangi bilgisayarların birbirleriyle iletişim kuracağı,

•Bilgisayarların ne zaman iletişim kuracağı ve sona erdireceği,

•İletişim sırasında gönderilen datada hata oluşup oluşmadığı,

•İletişim kurulduktan sonra hangi bilgisayarın data göndereceği şeklindedir.

2. katmanda verinin çerçeve yapıya dönüştürülmesi datanın hem anlamlandırılmasını hem de korunmasını sağlamaktadır.

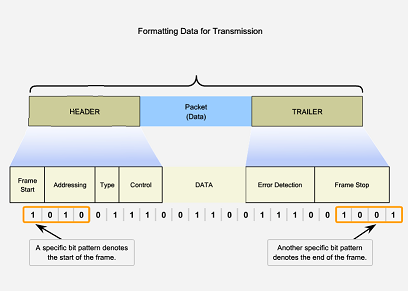
Frame yapılarının temel olarak içeriği:

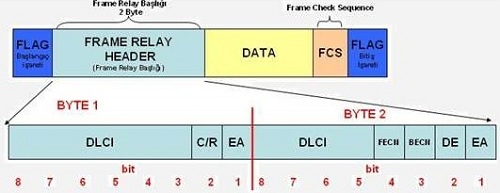
• Data- Ağ Katmanından gelen paket

• Header- Adresleme gibi kontrol bilgilerini içeren ve PDU (Protokol Data Unit) başında yer alan bölüm

• Trailer- PDU sonuna eklenmiş kontrol bilgisi içeren bölüm

##### 2.2.3.4.1 FRAME YAPISI





Şekil 2.2.3.4.1: Frame Yapısı/Frame formatı genel olarak şu alanlardan oluşmaktadır.

**Frame başlangıç alanı:** Yeni bir frame yapının gelmekte olduğunu belirten alandır.

**Adres alanı:** Kaynak ve Hedef bilgisayarların MAC adreslerinin bulunduğu alandır.

**Frame tipi ve uzunluğu alanı:** 3. katmanda kullanılan protokolün belirtildiği ve toplam frame uzunluğunun belirtildiği alandır.

**Data Alanı:** 3. katmandan gelen paketin bulunduğu alandır.

**FCS Alanı**: Belirli bir algoritma kullanılarak hesaplanan ve frame yapının sağlam olarak ulaşıp ulaşmadığını tespit etmede kullanılan alandır.

**Frame bitiş alanı:** Frame yapının bittiğini belirten alandır.[161]

#### 2.2.3.5 Physical Layer

Fiziksel katman, veri bağı ve fiziksel ortamı içermektedir. OSI referans modelindeki birinci ve ikinci katmanların görevlerini yerine getirir. Fiziksel katman için bir protokol tanımlanmamıştır. Ethernet bağlantısı, modem üzerinden çevrimiçi bağlantı ve varolan fiziksel bağlantı türlerini kullanmaktadır. Uç sistemde TCP/IP modülünün çalışması yeterlidir [44].

## 2.3 WIRED ve WIRELESS NETWORK’LERDE FİZİKSEL GÜVENLİK

Bilginin ve kaynakların paylaşılması gereksinimi sonucunda kurumlar, bilgisayarlarını çeşitli yollardan birbirine bağlayarak kendi bilgisayar ağlarını kurmuşlar ve sonra dış dünyayla iletişim kurabilmek için bilgisayar ağlarını İnternet’e uyarlamışlardır. Eskiden kilitli odalarla sağlanan güvenlik kavramı, bilgisayar ağları ve İnternet gibi ortamların gündeme gelmesiyle boyut değiştirmiştir. İnternet yasalarla denetlenemeyen bir sanal dünyadır. Bu sanal dünyada saldırganlar bilgiye ulaşmada ağların zayıf noktalarını kullanarak yasadışı yollar denemektedirler. Sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların bilinçsizce yaptıkları hatalar nedeniyle birçok bilgi başka kişilerin eline geçmekte veya içeriği değiştirilmektedir. Kurumlarda oluşan kayıplar maddi olabileceği gibi güven yitirme gibi manevi zararlar da olabilmektedir. Bu tür durumlarla başa çıkabilmek için bazı kuralların belirlenmesi gerekmektedir.

Kurumların kendi kurmuş oldukları ve İnternet’e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur. Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır. Ağ güvenlik politikaları mümkünse sistem kurulmadan ve herhangi bir güvenlik sorunuyla karşılaşmadan önce oluşturulmalıdır.  Bu aynı zamanda, kurulu olan bir sistemin güvenlik politikasını oluşturmaktan daha kolaydır. Güvenlik politikası olmadan güvenli bir bilgisayar ağı gerçekleştirilemez. Bu kadar öneme sahip olmasına rağmen Amerika’da güvenlik politikalarının gerçekleştirilme oranı sadece %60’larda kalmakta, Türkiye için bu oran daha da düşmektedir.

Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Bilgi ve ağ güvenlik politikalarından söz edildiğinde birçok alt politikadan söz etmek mümkündür. Bunun nedeni, politikaların konuya veya teknolojiye özgü olmasıdır. Fakat biz çalışmanın bu bölümde, sadece wired ve wireless network’lerde fiziksel güvenliğin sağlanması için gerekli olan temel fiziksel güvenlik kavramı ve fiziksel güvenlik politikasını ele alacağız. [66]

### 2.3.1 Fiziksel Güvenlik

Bir saldırgan ana cihaza, wired ve wireless network’lere fiziksel olarak erişebiliyorsa, cihazın kontrolünü rahatlıkla ele alabilir. Hatta trafik gönderebilir ya da hattı dinleyebilir. Bu hususa özellikle dikkat edilmeli ve gerekli önlemler alınmalıdır. Bazı fiziksel güvenlik yöntemleri şunlardır; [66]

* Cihazlar sadece yöneticinin açma yetkisi bulunan odalarda ya da kilitli **dolaplarda(kabinet)** tutulmalıdır.
* Cihaza fiziksel olarak erişenlerin isimlerini erişim zamanlarını da gösteren bir listede tutmak akıllıca bir davranıştır.
* Kablolar etiketlenmeli ve ne iş yaptıkları belirlenmelidir. Kullanılmayan kablolar ağdan çıkarılmalıdır.
* Cihazalara erişim bilgileri açık yerde tutulmamalıdır.
* Güç kaynaklarının yerleri belirlenmeli ve bu kaynaklar gözden uzakta kilitli tutulmalıdır. Böylece saldırganın gücü kesmesi engellenmelidir.

Günümüzde artık çok kritik bir öneme sahip olan güvenlik konusunda, wired ve wireless network’lerde fiziksel güvenlik kavramı, bizim için temel ve hayati kavramlardan biri haline gelmiştir. Fiziksel güvenlik kavramı ve bilgi güvenliğinin fiziksel anlamda en üst düzeye çıkarılması için, sağlanması gerekli önlemler, yer ve durumlarına göre aşağıda incelenmiştir. [71] [66]

#### 2.3.1.1 Binalar

* Alanlar belirlenmelidir. Örneğin:

1. Alan: Kamuya açık alanlar

2. Alan: Sadece şirket çalışanlarına açık alanlar

3. Alan: Korunan alanlar. Sadece kimlikle girilebilen alanlar, erişim katı bir şekilde kontrol edilir. İçeriden eşlik edilmeyen dış erişimlere izin verilmez.

* Binalar ofis saatleri dışında mutlaka kilitlenmelidir. Ofis saatlerinde de erişim resepsiyon üzerinden yapılmalıdır.
* Kamuya açık alanlarda ateş duvarı olmadan iç bilgiye erişen bilgisayarlar olmamalıdır.
* 3. Seviye sunucu odaları kilitlenmeli ve mümkünse elektronik kart ile erişim sağlanmalıdır.
* 3. Seviye sunucuları uzaktan monitör izlenmesi, modem izlenmesi, radyasyon ölçümü ile monitör görüntüsü yaratılması (Van Eck Radyasyon yöntemi ile gözetleme(snooping)) yöntemlerine karşı korumak gerekir.
* Sistemler elektromanyetik akımlara karşı korumak gerekir.
* 4. Seviye sunucu odaları kilitlenmelidir, erişim kartı kullanılmalı ve çok az insanda bu kart olmalıdır.
* 4. Seviye sunucu odaları 24 Saat/7 Gün güvenlik personeli tarafından gözlem altında tutulmalıdır.
* 3. Seviye için bir felaket, yangın, çalınma, patlama, vb. olaylarda kullanılmak üzere felaket planları, senaryoları yapılmalıdır. [71]

#### 2.3.1.2 Verinin Taşınması

Verinin ne şekilde (aleni, gizli, şirket içi...), hangi tip ürünlerle (disk, CD, disket, kaset, kâğıt, bilgisayar...) taşınacağı hakkında şirket içinde bir politika olması gerekmektedir.

Ve her seviye güvenlik için bu politika gerekiyorsa değişmelidir. [71]

#### 2.3.1.3 Veri Yedeklemeleri

3. Seviye verilerin yedekleme üniteleri kilitli dolaplarda veya kilitli odalarda tutulmalıdır. Ayrıca bu veriler için alınan bazı düzenli yedeklemeler (örneğin ayda bir alınan) alandan başka bir yerde saklanmalıdır. (Başka bir bina, departman, vb.) Yedeklemeler sadece güvenli yöntemlerle taşınmalıdır. (Para transferinde olduğu gibi) [71]

#### 2.3.1.4 Diskler

Disketler ve taşınabilir diskler sıklıkla virüs ve yasal olmayan yazılımlar için kaynak olmaktadır (e-postada bu durumdadır). Ayrıca bunlar gizli bilgilerin yasal olmayan bir şekilde kopyalanmasında kullanılabilir. Disketlerden veri silindiği zaman bu veriler bir daha geri getirilemeyecek şekilde silinmelidir. Kullanıcılar güvenilir ağ, ağ yazıcıları, dosya sunucuları ve e-postaya sahiplerse disket sürücülere gerek yoktur. [71]

* Taşınabilir diskler ve disketler (bu kelimeyle sadece disketler değil tüm taşıma ürünleri kastedilmektedir.) sadece gerekli olduklarında kullanılmalıdırlar.
* 3. Seviye verilerin disketlere kopyalanmaması gerekir.
* 4. Seviye veriler şifrelenmelidir. Eğer iç ağın yeterince güvenilir olmadığı düşünülüyorsa dosyalar yerel olarak şifrelenip daha sonra ağ sunucusuna kaydedilebilir.
* 3. Seviye veri güvenliği için gizli disklerin onarılması engellenmelidir, yok edilmelidir.
* Veri diskleri sınıflandırılmalı ve seviyeleri üzerlerine yazılmalıdır.
* Saklama ürünlerini etkileyecek elektromanyetik akımlara karşı korumak gerekir.

#### 2.3.1.5 Dizüstü Bilgisayarlar

3. Seviye veri içeren dizüstü bilgisayarların sabit diskleri şifrelenmelidir ve korunmalıdır. Ve bir bilgisayarı korumakta kullanılan mekanizmalarla güvenlik güçlendirilmelidir. (Ateş duvarları, antivirüs yazılımları, vb.) [71] [66]

#### 2.3.1.6 Yazıcılar

Gizli bilgileri yazdırmada sadece yöneticilerin odalarındaki ya da erişimin kısıtlandığı odalardaki yazıcılar kullanılmalıdır. [71]

#### 2.3.1.7 Bilgisayarlar

EPROM şifreleri kullanılmalıdır. Açmak için de güvenli işletim sistemleri ve şifre ile erişim kullanılmalıdır. Şifreyle durdurulan ve 15 dakikada devreye giren ekran koruyucuları kullanılmalıdır. Bilgisayarlar mümkünse kilit altında tutulmalıdır. Güvenlik mekanizmaları mutlaka her bilgisayarda bulunmalıdır. [71] [66]

#### 2.3.1.8 Wired Network Hatları

Wired network hatlarına ait kabloların, güvenli hatlardan geçirildiğinden emin olunmalıdır. Saldırganın kolayca kablolara erişim yapamayacağı güzergâh ya da toprak altındaysa yeterli derinlikte olmalıdır. Fiziksel anlamda kritik öneme sahip hat kablolarının güvenliği hayat önem arz etmektedir. Yoksa bilinmelidir ki, ağ kablolarına kolay erişimin sağlanabildiği bir sistemde güvenlik kavramından söz edilemez. [71] [72]

#### 2.3.1.9 Bağlantı ve İletişim Elemenları

**Ethernet: (Network Interface Card- NIC):** Yerel ağların oluşturulmasında veri alışverişini yöneten ve gerçekleştiren elemanlardır. Teknolojileri 100 Megabit veri transferi yapabilecek kapasiteye kadar çıkmıştır. PCI veya ISA yuvalara takılan bu kartların kablo bağlantıları BNC ya da RJ45 konnektörleri ile yapılabilmekte; yani iki tip kablo ile kullanılabilmektedirler. Ethernet elemanları görevi dolaysıyla fiziksel olarak korunması en kritik öneme sahip ağ elamanlarından biridir. Dolaysıyla Ethernet elemanları kilitli yerlerde tutulmalı ve sadece yetkili kişi erişimine açılmış olmalıdır. [72] [71]

**Cables:**Yaygın olarak TwsistedPair (UTP) ya da Koaksiyel (BNC) kablo kullanılmaktadır. Fiziksel boyutlarda kablo güvenliği için 3.1.8. başlıktaki önlemler alınabilir. [72] [71]

**Hub:**TwsistedPair kablo ve RJ45 konnektörlerle oluşturulan ağ sistemlerinde, ağın temel dağıtım elemanlarıdır. Kapalı alanlarda muhafaza edilmeli ve erişimi sınırlı tutulmalıdır. [72] [71]

**Switch:**Hub gibi dağıtım elemanı olup, veri anahtarlama ve iletinin güçlendirilmesini sağlar. Yine diğer ağ elemanları gibi kapalı ortamlarda muhafaza edilip sınırlı kişileri erişiminde olmalıdır. [72] [71]

**Gateway:**Haberleşme kontrolünü üstlenen ağ geçididir. Ağa giren ve çıkan tüm veriler bu aygıttan geçerler. Bu özelliği dolaysıyla fiziksel açıdan korunması kritik ağ elemanlarının başında gelmektedir. Kötü niyetli kişilerin erişemeyeceği yerlerde muhafaza edilip sınırlı kişiler tarafından erişilebilmelidir. [72] [71]

**Repeaters:**Bir repeater kablodaki sinyali yükseltir ve erişim mesafesini uzatır. Data transferi için ek bir yazılıma ihtiyaç duymaz. Hiç beklemeye gerek kalmadan, giriş sinyalini yükseltilmiş olarak çıkışa verir. Ayrıca bazı repeaterler gürültüler için filtrasyon görevi de yaparlar. Repeaters da fiziksel olarak korumalı bir bölgede tutulmalıdır. Çünkü kablodaki sinyali alan ve sadece sinyal yükseltme işi yapan bu ağ elemanına yapılacak art niyetli bir müdahale ile bilgilere kötü niyetle erişilebilir. [72] [71]

**Bridges:**Bridge’ler repeaterlere göre daha akıllı cihazlardır. Aynı ya da farklı topolojiler kullanan iki network’ü, data-link seviyesinde birbirine bağlar. Basit olarak, bir server’a iki ayrı sınıftan network kartı takmak suretiyle bir bridge yapılabilir. Örneğin, bir server’a aynı anda hem ethernet hem de token-ring kartla kurulan network kullanıcıları, her iki topolojideki bilgisayarlarla iletişim kurabilirler. Ayrıca bir server’a aynı tip iki ethernet kart takılarak da geniş bir LAN’ı iki parçaya ayırarak, daha basit bir yapı elde edilebilir. Bu yolla da bir bridge yapılmış olur. [72] [71]

Bir Bridge, Data-Link seviyesindeki Media Access Control alt seviyesini (MAC) kullanır. Bu seviye, hedef worstation adresini içerir. Gerçekte doğru Workstation adresini tespit eden bu seviye, kendine bağlı olan tüm Workstationları tanımakla yükümlüdür. Bridge’ler gelen verilerin (veri çerçevelerinin) hangi hedefe gönderildiğine bakarak iletim yapıyor olmasından ötürü ulaşılabildiği takdirde bilgilere art niyetle ulaşılabilir veya adresleri değiştirilebilir. Bu yüzden de bridge’ler fiziksel olarak kapalı ve korunaklı yerlerde saklanmalı sadece yetkili kişilere erişim izni tanınmalıdır. [72] [71]

**Routers:**Routerlar repeaterlerden bir üst seviyede işlem yapar. Bu seviye IPX’inde çalıştığı network seviyesidir. IPX’ler, routerler ile ilgili emir ve talimatlarıda içerirler. Bir Novel Netware Server, iki ya da daha fazla network interface kartını otomatik olarak kullanabilir. Bir routerin Bridge’den farkı, paket içindeki LAN adreslerini ve Workstation adreslerinin her ikisini de okur ve kullanır. Bridge’ler sadece kendilerine bağlı Workstationların adresleri hakkında bilgi sahibi iken Routerler hem Workstation hem de diğer LAN adresleri hakkında bilgi sahibi olmalıdırlar. Aksi halde, en doğru route bilgisini tespit etmeleri mümkün olamazdı. Bu nedenle kritik önem arz eden bu ağ elemanı da diğer elemanlar gibi korunaklı şekilde muhafaza edilmelidir. Sadece belirli ve yetkili kişilere erişim izni verilmelidir. [72] [71]

**Modem:** Uzak ağ sistemlerine erişimi çevirmeli ağ, (Dialup Networking) erişimini sağlayan aygıttır. Modem (MOdulation DEModulation) temel olarak Analog veriyi Digital’e, Digital veriyi Analog’a çevirerek, telefon hatları ile iletilmesini sağlar. Modemler de bu özelliklerinden dolayı 3. kişilerin erişim sağlayabileceği şekilde muhafaza edilmemelidir. Modeme erişildiği takdirde bilgi hırsızlığı çok kolay olacağından ötürü fiziksel olarak sadece istenilen kişilerin erişebileceği alanlarda saklanmalıdır. [72] [71]

# BÖLÜM 3: WIRED ve WIRELESS NETWORK’LERDE GÜVENLİK İLKELERİ ve KAVRAMLARI

Wired ve wireless network’lerde güvenlik ilkeleri ve kavramları denince ilk olarak akla bilişim güvenliği gelmektedir. Bilişim güvenliğinin ilke ve kavramları bize wired ve wireless network’lerde güvenliğin ilke ve kavramlarını verir.

Özellikle 1990’lı yıllardan başlayarak yaşanan hızlı teknolojik gelişmeler ve internetin yaygınlaşmasının bir sonucu olarak bilişim güvenliği son yıllarda giderek önem kazanan bir konu haline gelmiştir. Konunun önümüzdeki dönemde kurumların öncelik listesinde giderek artan bir öneme sahip olacağı ve kurumların bilişim güvenliği alanına gereken önemi vermeye başladıkları, ilgili önlemleri alma çabası içine girdikleri bilinmektedir. Ancak, bilişim güvenliğinin sadece teknolojik önlemlerle sağlanabileceği gibi genel bir yanılsamanın olduğu da gözlenmektedir.

Bu dokümanda bilişim güvenliğinin temel kavramları, en önemli bileşenleri ele alınmaktadır. Konunun esas olarak çok boyutlu ve karmaşık bir süreç olmasından hareketle, bilişim güvenliğinin bütünsel yaklaşımlarla ele alınmamasının tehlikeleri açıklanmaktadır.

Dokümanın ikinci bölümünde bilişim güvenliğinin temel kavramları ve bileşenleri, üçüncü bölümde ise bilişim güvenliğinin nasıl sağlanabileceği ele alınmaktadır. Dördüncü bölümde kurum yönetiminin alması gereken önlemler, beşinci bölümde geliştirilmiş güvenlik teknolojileri uygulamalarının başlıcaları, altıncı bölümde de güvenlik eğitimi konusunda yapılması gerekenler işlenmektedir. Yedinci bölümde bilişim güvenliğine ilişkin uluslararası standartlar ele alınmakta, sekizinci bölümde ise Oracle veritabanı yönetim sisteminin güvenlik özellikleri açıklanmaktadır. [74] [75]

## 3.1.“Bilişim Güvenliği”nden Ne Anlamalıyız?

### 3.1.1 Bilişim Güvenliği Nedir?

1990’lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri *“olmazsa olmaz”* bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir.

Bilişim sistemlerine ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır.

Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da o denli artacaktır. Bu duyarlılık arttıkça da bilgisayar sistemlerine ve ağlarına yönelik olarak gerçekleştirilecek olan saldırıların sonucunda; para, zaman, prestij ve değerli bilgi kaybı da artacaktır. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda ise kaybedilen insan hayatı bile olabilir.

Bilgisayar Güvenliği Enstitüsü (Computer Security Institute- CSI) ve Federal Araştırma Bürosu (FBI) tarafından geleneksel olarak gerçekleştirilen “Bilgisayar Suçları ve Güvenlik Araştırması”nın 2001 yılı raporuna göre bilişim suçları 1997- 2001 yılları arasında her yıl neredeyse ikiye katlanacak biçimde artmıştır. Aynı araştırma, gizli bilgilerin çalınması ve finansal kayıtlarda yapılan yasadışı değişikliklerin, en çok maddi zarara neden olan iki saldırı biçimi olduğunu göstermektedir.

Bilişim güvenliği konusunun, önümüzdeki dönemde de bilişim sektöründe giderek artan bir öneme sahip olacağı bilinmektedir.

İzleyen paragraflarda son yıllarda yaşanmış bilgisayar güvenliği ihlallerine ilişkin bazı örnekler verilmektedir. [74] [75]

**Melissa virüsü,** 26 Mart 1999 tarihinde ilk kez ortaya çıkmış, anti virüs programlarını atlatarak Windows 9x, NT işletim sistemleri altında Word 97 ve Word 2000 programlarını kullanarak bilgisayarlara zarar vermiştir. Melissa virüsü internete gönderilmiş ve milyonlarca dolar zarar yol açmış “kötü amaçlı” (malicious) bir programdır ve e-posta yolu ile yayılmıştır. Virüsün 34 yaşındaki yaratıcısı David L. Smith, evdeki bilgisayarı yardımı ile virüsü internete göndermiştir. Virüs her bulaştığı bilgisayardan 50 yeni bilgisayara bulaşma özelliğine sahiptir. Bu nedenle çok hızlı ve durdurulamaz bir şekilde yayılmıştır. Smith virüsü ilk olarak biri çalıntı diğeri kendine ait olan iki America Online hesabını kullanarak bir e-posta mesajı ile beraber bir haber grubuna (news group) göndermiştir. Söz konusu e-posta mesajında “e-postanın eklentisinin yetişkin (adult) içeriğe sahip web sayfalarına giriş parolalarını bulmayı sağlayan bir program olduğundan bahsedilmiştir. Bu e-posta mesajı açılır açılmaz kurbanın bilgisayarına virüs bulaşmaktadır. Daha sonra virüs, Microsoft Outlook programı yardımı ile kendisini, kurbanın adres defterindeki ilk 50 kullanıcıya postalamaktadır. Olay hakkında delil toplama sürecinde America Online yetkilileri de görev almışlardır. 1 Nisan 1999’da Smith, FBI ve New Jersey Yüksek Teknoloji Suçları Birimi görevlileri tarafından kardeşinin evinde yakalanmış ve gözaltına alınmıştır. Smith, 2 Mayıs 2002 tarihinde 20 ay hapis cezasına çarptırılmış ve 3 yıl göz hapsi ile 100 saat kamu hizmetinde çalışma cezasını almıştır. Melisa virüsü saldırısının 80 Milyon dolar zarara yol açtığı tespit edilmiştir. [74] [75]

Bir zaman bombasınıngeri döndürülemez zararlar vermesine bir örnek 1996 yılında yaşanmıştır. Timothy Allen Lloyd (39), yüksek teknoloji ürünü ölçme ve kontrol cihazları üreten Omega Mühendislik şirketinde çalışan “şef bilgisayar ağı program tasarımcısı” idi. Lloyd, Omega’da 11 yıl çalıştıktan sonra 10 Haziran 1996’da şirket ile ilişkisi kesildi. Bunun üzerine Lloyd hazırladığı “zaman bombası” yardımı ile Omega’nın tüm karmaşık üretim yazılımlarını geri döndürülemez bir şekilde sildi. Bu sabotaj sonucunda şirket, satışları ve ileri tarihli anlaşmaları da göz önünde bulundurulduğunda 10 Milyon dolarlık bir kayba uğramıştır. Bu olay olduğu sırada, Amerikan Gizli Servisi tarihinde, benzer olaylar arasında yol açtığı zarar en yüksek olan sabotajlardan biri olarak kayda geçmiştir. Olay ortaya çıkarıldığında, Lloyd 41 ay hapis ile cezalandırılmıştır. [74] [75]

1999 yılında Kanada’da yaşanan olay ise, elektronik sahtecilikkonusunda verilebilecek en iyi örneklerdendir. Bu olay, Kosta Rika, ABD ve Kanada makamlarının ortak çalışmaları sonucunda ortaya çıkarılmış bir dolandırıcılıktır. *“Www.triwestinvest.com”* adlı sitede, daha önceden sadece çok zengin yatırımcılara sunulan, yıllık %120’lik bir kâr marjı olan ve para kaybı riski olmayan bir yatırımdan söz edilmekteydi. Yatırımcılardan, 1000 dolarlık paketler halinde paralarını yatırmaları istenmekteydi. Bu siteye paralarını ilk yatıranlara, kâr payı ödemesi altında birtakım ödemeler de yapılarak siteyle daha fazla müşterinin ilgilenmesi sağlanmıştır. 1999- 2001 yılları arasında bu site aracılığı ile yatırım yapan 15.000 kurbanın paraları ile Alyn Richard Waage; Mexico ve Kosta Rika’da milyon dolarlık gayrimenkuller, yatlar ve helikopterler satın almıştır. Bunun yanında, dolandırdığı paraların bir kısmını gizlemek için de Kosta Rika’da paravan şirketler kurmuş ve paraların bir kısmını da bu şirketlerden kazanmış gibi göstermiştir. Waage, internet üzerinden dolandırıcılık yapmak ve bu yolla yatırımcıları kandırarak 60 Milyon $ toplamaktan suçlu bulundu, paranın çoğu sahiplerine iade edildi.

Bu örnekler, bilişim güvenliğinin gerek tehditler ve riskler gerekse de alınması gereken önlemler açısından ne denli önemli olduğunu göstermektedir. [74] [75]

### 3.1.2 Güvenlik Prensipleri

Bilişim Güvenliğinin birçok boyutu olmasına karşın, temel olarak üç prensipten söz edilebilir: Gizlilik, Veri Bütünlüğü ve Süreklilik. [74] [75]

#### 3.1.2.1 Confidentiality

Bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Confidentiality, hem kalıcı ortamlarda (disk, tape, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla erişebilirler: Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının, ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir. [74] [75]

Confidentiality

Integrity

Continuity

Şekil 3.1.2.1: Temel Güvenlik Prensipleri

#### 3.1.2.2 Data Integrity

Bu hizmetin amacı, veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır. Bu hizmeti, geri dönüşümü olan ve olmayan şekilde verebiliriz. Şöyle ki; alıcıda iki tür bütünlük sınaması yapılabilir: Bozulma Sınaması ya da Düzeltme Sınaması. Bozulma Sınaması ile verinin göndericiden alıcıya ulaştırılması sırasında değiştirilip değiştirilmediğinin sezilmesi hedeflenmiştir. Düzeltme sınaması’nda ise, Bozulma Sınaması’na ek olarak eğer veride değişiklik sezildiyse bunu göndericiden çıktığı haline döndürmek hedeflenmektedir. [74] [75]

#### 3.1.2.3 Availability

Bilişim sistemleri, kendilerinden beklenen işleri gerçekleştirirken, hedeflenen bir başarım (performance) vardır. Bu başarım sayesinde müşteri memnuniyeti artar, elektronik işe geçiş süreci hızlanır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler. Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dahilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler.

Sistem sürekliliği, yalnızca kötü amaçlı bir “hacker”ın, sistem başarımını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir.

Aşağıda, yukarıdaki üç temel prensibe ek olarak ikinci planda değerlendirilebilecek izlenebilirlik, kimlik sınaması, güvenilirlik ve inkâr edememe prensiplerinden bahsedilmiştir. [74] [75]

#### 3.1.2.4 Accountability

Bu hizmetin hedefi sistemde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Burada olay dendiğinde, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlayabiliriz. Bir sistemde olabilecek olaylara, kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak göndermek ya da icq ile mesaj yollamak gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin örüntülerine rastlanırsa ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse alarm mesajları üretilerek sistem yöneticileri uyarılır. [74] [75]

#### 3.1.2.5 Authentication

Ağ güvenliği açısından authentication; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri yaygın olarak kullanmaya başlanmıştır. [74] [75]

#### 3.1.2.6 Reliability- Consistency

Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir. [74] [75]

#### 3.1.2.7 Non-Repudiation

Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. [74] [75]

Bu hizmetler, zaman içinde bilgisayar sistemlerine karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir hizmet, belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir, denilebilir. [74] [75]

### 3.1.3 Threats

*Tehdit*, bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden, olarak tanımlanabilir. Her tehdidin bir kaynağı (threat agent) ve bu kaynağın yararlandığı sistemdeki bir “güvenlik boşluğu” vardır. *“Sistemi neye karşı korumalıyım?”* sorusuna verilecek cevap bir sisteme yönelik olan tehditleri belirlemekte yardımcı olacaktır.

Tehditler, tehdit kaynağı açısından bakıldığında iki gruba ayrılarak incelenebilir:

1. **İnsan Kaynaklı Tehditler:** Bu tür tehditleri de kendi içinde iki alt gruba ayırabiliriz:
   1. Kötü niyet olmayan davranışlar sonucu oluşanlar: Bir kullanıcının, sistemi bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu sistemde ortaya çıkma olasılığı olan aksaklıklardır.
   2. Kötü niyetli davranışlar sonucu oluşanlar: Sisteme zarar verme amacıyla, sisteme yönelik olarak yapılacak tüm kötü niyetli davranışlardır. Bu tür tehditlerde, tehdit kaynağı, sistemde bulunan güvenlik boşluklarından yararlanır.
2. **Doğa Kaynaklı Tehditler:** Bu tür tehditler genellikle önceden tespit edilemezler ve büyük bir olasılıkla olmaları engellenemez. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi bu tür tehditlere örnek olarak verilebilir.

Tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre *iç tehditler*, kurum içinden kuruma yönelik yapılabilecek saldırılar, *dış tehditler* ise kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanır. [74] [75]

### 3.1.4 Vulnerability

Vulnerability, sistem üzerindeki yazılım ve donanımdan kaynaklanan ya da sistemi işletim kuralları ve/veya yönergelerindeki açık noktalar ve zayıf kalmış yönlerdir. Bir güvenlik boşluğu sayesinde bir saldırgan, sistemdeki bilgisayarlara ya da bilgisayar ağı üzerindeki kaynaklara yetkisiz olarak erişebilir. Bir sunucu bilgisayar üzerinde çalışan bir hizmet (örneğin web sunucu ya da e-posta alma/gönderme hizmeti), modem üzerinden içeri doğru sınırlandırılmamış arama hizmeti, bir güvenlik duvarı üzerinde açık unutulmuş bir erişim noktası (port), sunucu bilgisayarların bulunduğu odaya giriş çıkışlarda fiziksel erişim denetimi eksikliği, sunucular üzerinde belli bir politikaya dayandırılmadan belirlenen parolalar güvenlik boşluklarına örnek olarak verilebilirler.

Yazılım ya da donanımdan kaynaklanan güvenlik boşlukları, program üreticisi ya da başka bir kaynak tarafından geliştirilen bir “yama program” yardımıyla kapatılmalı ve eldeki yazılım ve donanımların üreticilerinin yayınladığı yama listeleri sürekli olarak takip edilmelidir ve çıkan yamalar vakit geçirilmeden sisteme uygulanmalıdır.

Tehditler, bilgisayar sistemlerindeki güvenlik boşluklarına yönelik olarak tanımlanırlar. Yani bir güvenlik boşluğu ortadan kaldırılırsa ya da “yama program” yardımıyla düzeltilirse, söz konusu tehdit ortadan kaldırılır. Aşağıdaki tablodan da anlaşılacağı üzere, bir tehdidin oluşması için bir güvenlik boşluğuna ve bu güvenlik boşluğundan yararlanabilecek bir tehdit kaynağına ihtiyaç vardır. [74] [75]

### 3.1.5 Network Security Monitoring Süreçleri

Network Security Monitoring (NSM) kavramı, intrusion saptanması ve ona göre önlemler alınması için aşağıdaki süreçleri tanımlar [73]:

* Gerekli verilerin toplaması,
* Belirti ve uyarıların artışının analizidir.

NSM, ağ farkındalığı yaratmak için aşağıdakilere gereksinim duyar [73]:

* Alert verisi,
* Session verisi,
* Full content verisi,
* İstatistiksel veri

NSM ile hedeflenen; bir nüfuzun kapsamının ve etkisinin değerlendirilmesi için gerekli kanıtların toplanması, etkin ve etkili önlem iyileştirme aşamalarının gerçekleştirilmesidir [73]

NSM bir kavramdır ve özellikle ağ farkındalığı için akış (flow) takibi önemlidir.

Kullanılabilecek yöntemler, programlar ve uygulama örneği aşağıda verilmiştir.

Bütün ağ paketlerini biriktirmek mümkün değildir. Bunun yerine, aşağıdakiler gerçekleştirilebilir:

Kısmi zamanlı, sampling veya belirli IDS uyarıları durumunda,

* Sunuculara gelen istek paketlerinin takibi,
* Kritik sunucularına hem gelen hem de giden trafiğin bütünün takibi. Kritik sunucular ile söz edilenler şunlardır:
  + Kurum için önemli bilgiler barındıran sunucular,
  + Tarafımızdan yönetilmeyen ve muhtemel güvenlik sorunları olduğundan şüphelenilen sunucular,
  + Honeypot olarak kullanılan sunucular.
* Sunuculara gelen/giden trafiğin IP paket başlığının tümü ve payload kısmının belirli bir kısmı tutulabilir.

Kullanılabilecek programlara örnekler:

* Network ve flow dinleme programları:
* Tcpdump
* Argus
* Paket analiz programları:
* Argus flow analiz programları (ra, racluster, ragraph, ragrep, racount, rahosts …)
* Tcpslice
* Tcpdstat
* Tcptrace
* Honeysnap
* Sguil
* Paket tekrar oluşturma:

○ Tcpreplay

* Grafiğe dökme programları:

○ Xplot

○ Flowscan

○ Afterglow

Argus, özellikle netflow gibi Cisco L3 cihaza bağımlı olmaması ile dikkati çekiyor. Ağ üzerindeki herhangi bir segmentte, herhangi bir makine üzerinde çalıştırabilirsiniz. Bunun yanı sıra analiz içinde birçok yazılımla beraber geliyor. Bunun yanı sıra, Afterglow ile süreci grafiğe dökmek de mümkün olmaktadır. [73]

### 3.1.6 Risk

Bir tehdit kaynağının, bir sistemdeki güvenlik boşluğundan yararlanarak sisteme yetkisiz erişimde bulunması olasılığı, bu tehdidin *riski* olarak ifade edilir. Tehdit kaynaklarının ya da güvenlik boşluklarının azaltılması, tehdide ait riskleri de aynı oranlarda azaltacaktır. [74] [75]

Tablo 3.1.6’da tehdit kaynağı- güvenlik boşluğu – risk ilişkisine örnekler verilmiştir.

Tablo 3.1.6: Tehdit Kaynağı- Güvenlik Boşluğu- Risk İlişkisine örnekler

|  |  |  |
| --- | --- | --- |
| **Tehdit** **Kaynağı** | **Etkileyebileceği**  **Güvenlik Boşluğu** | **Oluşan Risk** |
| Virüs | Antivirüs yazılımının eksikliği | Virüs bulaşması |
| Hacker | Sunucu bilgisayar üzerinde çalışan güçlü hizmet programları | Gizli bilgilere yetkisiz erişim hakkının elde edilmesi |
| Kullanıcılar | İşletim sisteminde yanlış ayarlanmış bir parametre | Sistemin çalışamaz duruma gelmesi |
| Yangın | Yangın söndürme cihazının eksikliği | Bina ve bilgisayar sistemlerinin zarar  görmesi ve can kaybı olasılığı |
| Çalışanlar | Erişim denetim mekanizmalarının yetersizliği | Görev-kritik bilgilerin zarar görmesi |
| İş ortağı olan bir firmanın yetkilisi | Erişim denetim mekanizmalarının yetersizliği | Ticari sırların çalınması |
| Saldırgan | Kötü yazılmış bilgisayar programları | “tampon taşması” hatasının alınması |
| Kötü niyetli ziyaretçi | Güvenlik Görevlisinin olmayışı | Kıymetli cihaz ve / veya bilgilerin fiziksel olarak çalınması |
| Çalışan | Tutulan kayıtlardaki yetersizlik | Veri işleme programına verilen  giriş verileri ve çıkış olarak elde edilen veriler üzerinde değişiklikler yapılması |
| Saldırgan | Güvenlik Duvarı’nın ayarlarının iyi yapılmamış olması | Bir “hizmet durdurma” saldırısının gerçekleşmesi |

Potansiyel riskler, tedbirler yardımı ile azaltılabilirler. Bir tedbir, bir güvenlik boşluğunu ortadan kaldırır ya da bir tehdit kaynağının bir güvenlik boşluğunu kullanması riskini azaltır. Tedbirler, yazılım, donanım ya da geliştirilen bir kullanım yönergesi şeklinde karşımıza çıkabilirler. Tedbirlere, sağlam bir parola yönetim politikası, bir güvenlik görevlisi, bir işletim sistemi üzerinde akıllı kartlara dayalı bir erişim denetim mekanizması, güvenlik konusunda kullanıcıların eğitimi gibi örnekler verilebilir. Şekil 3.1.6’da yukarıda bahsedilen kavramların birbirleri ile etkileşimleri gösterilmektedir. [74] [75]

Tehdit

Artt

ı

r

ı

r

Güvenlik

Bo

ş

lu

ğ

u

Risk

Tehdit

Kayna

ğ

ı

Sahip olunan

de

ğ

erler

Aç

ı

ğ

a ç

ı

kma

Kar

ş

ı

Tedbirler

Do

ğ

rudan etkiler

Aç

ı

ğ

a ç

ı

kar

ı

r

Yol aça

r

Zarar verebilir

Nede

n

olu

r

korunabili

r

Şekil 3.1.6.a : Temel Güvenlik Kavramlarının Birbirleri İle Olan İlişkileri

*(Shon Harris, CISSP All-in-One Exam Guide)*

# BÖLÜM 4: WIRED ve WIRELESS NETWORK’LERDE BİLİŞİM GÜVENLİĞİ

## 4.1 Bilişim Güvenliğinin Sağlanması

Bilişim sistemlerinin güvenli hale getirilmesi konusu, kapsamlı ve bütünleşik bir yaklaşımla ele alınmadığı takdirde, başarı kazanmak büyük olasılıkla mümkün olmayacaktır. Bilişim güvenliğinin sağlanması üç temel açıdan ele alınabilir. Bu üç süreç alanı şunlardır: [95]

1. Yönetsel Önlemler
2. Teknoloji Uygulamaları
3. Eğitim ve Farkındalık Yaratma

**YÖNETSEL**

**ÖNLEMLER**

**EĞİTİM VE**

**FARKINDALIK**

**YARATMA**

**TEKNOLOJİ**

**UYGULAMALARI**

Şekil 4.1: Bilgi Güvenliğinin Sağlanmasında Bütünleşik Yaklaşım

### 4.1.1 Bilişim Güvenliği Süreç Alanları

Güçlü bir güvenlik altyapısı kurabilmek için bu üç parçayı birbiri ile bütünleştirmek ve hepsini birlikte bütünsel bir yaklaşımla ele almak gerekir. Bu bahsedilen süreç alanlarının içinde, bilgisayar ve bilişim güvenliği teknolojilerinin dışında kalan farklı alanlar da bulunmaktadır. Diğer bir deyişle, bir kurumun, kurumsal bilişim güvenliğini sağlamak amacıyla, sadece bilişim teknolojilerini devreye sokarak başarıya ulaşma şansı oldukça azdır.

Bütün bunlara ek olarak, bu üç süreç alanından her biri, başarıya ulaşmak için diğer iki süreç alanının tam ve eksiksiz çalışıyor olmasına ihtiyaç duyar. Bu üç alan birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Birlikte çalışmalarından oluşacak sinerji, kuruma bilişim güvenliği yönünden tehdit oluşturacak tüm etkenlere karşı güçlü bir kalkan görevini üstlenecektir.

Yönetsel Önlemler, güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi, bilişim güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından, belirlenenlerin yazıya dökülmesi, yani prosedür, yönerge ve talimatlar gibi dokümanların oluşturulması gelmelidir.

Günümüzde basında ve haber bültenlerinde çok yüksek maddi kayıplara yol açan virüsleri, bilgisayar ağlarına yönelik saldırılardan zarar gören şirketleri konu alan haberler sıkça yer almaktadır. Bununla birlikte, bir sistem yöneticisinin ve güvenlik uzmanının uğraştığı işlerin, her zaman gazete haberlerinde çıkanlarla sınırlı olduğu düşünülmemelidir. Bunlar dışında, günlük ya da periyodik olarak gerçekleştirilecek birtakım işler vardır ki işte yönetsel önlemler, bu tür işleri kapsayan ve tanımlayan bir süreç alanıdır. Bu süreç alanını oluşturan temel süreçler şunlardır: [95]

1. Risk Yönetimi
2. Güvenlik Politikaları
3. Standartlar, Yönergeler ve Prosedürler
4. Güvenlik Denetimleri

Yönetsel önlemlerin uygulanması, teknoloji uygulamaları ve eğitim süreçlerinin yanında fiziksel güvenlik uygulamaları ile de desteklenmelidir.

**Fiziksel Önlemler**

**Teknolojik Önlemler**

**Yönetsel Önlemler**

Kurumsal gizlilik

ta

ş

ı

yan veri ve

kaynaklar

Şekil 4.1.1: Kurumun Sahip Olduğu Değerli Varlıkların Korunması

Yönetsel önlemlerle ortaya konulan kurumun güvenlik ihtiyaçlarının karşılanmasında, teknolojik uygulamalardan da faydalanılır. Günümüzde bir bilgisayar ağına ya da tek başına bir bilgisayara yapılacak bir saldırının sonuçlanması saniyelerle ifade edilen çok kısa bir süre içinde oluşur. Bu tür saldırılara, ancak teknolojik birtakım önlemler ile karşı koyulabilir. Bunun yanında kullanılan teknolojiler, güvenlik yöneticilerinin hayatının kolaylaştırılması ve kurumun, bilişim güvenliği açısından bütün resminin görülmesi gibi yararlar da getirirler. [95]

### 4.1.2 Bilişim Güvenliği Teknolojileri

Bilişim güvenliğinin sağlanmasında kullanılan teknolojilerden bazıları aşağıdaki listede verilmiştir. Unutulmamalıdır ki, güvenlik uygulamalarının bütünü bunlarla sınırlı değildir. Burada en yaygın kullanılan ve en popüler teknolojilerden bahsedilmiştir: [95]

1. Kriptografi
2. Sayısal İmza ve PKI
3. Ağ Bölümlemesi ve Güvenlik Duvarları
4. Yedekleme
5. Saldırı Tespiti ve İzleme
6. Erişim Denetimi
7. Güvenlik Derinliği
8. Anti-Virüs

### 4.1.3 Eğitim

Eğitim ve Farkındalık Yaratma süreci, bir kurumun bilişim güvenliği açısından karşı karşıya bulunduğu riskleri azaltmada kullanılması gereken ana yöntemlerden biridir. Günlük faaliyetlerini bilişim teknolojisini kullanarak gerçekleştiren kullanıcıların, güvenlik konusunda eğitimlerle bilinçlendirilmesi, onların bir güvenlik boşluğu ve kurum açısından risk oluşturacak bir etken olmaları olasılığını en aza indirecektir.

Örneğin bilişim güvenliği konusunda bilinçsiz kullanıcılardan oluşan bir kurum düşünelim. Bu kurumun coğrafi olarak farklı illere dağılmış kolları ve şubeleri olsun. Her kurumda olduğu gibi bu kurumda da şubeler ve merkez arasında; pazardaki durum, yapılan bir toplantıya ilişkin görüşler, yeni teknolojilerin kullanılması hakkında alınacak kararlar ve bunlara dayanarak stratejik yönetim planların hazırlanması, finansal durum, geleceğe yönelik tahminler ve bunlar gibi daha birçok konuda bilgi akışını gerçekleştirmek gerekir. Kurumun bu bilgi akışını, şu anda rahat ve hızlı bir teknoloji olan eposta yoluyla gerçekleştirdiğini varsayalım.

Kurumdaki kullanıcılar, e-posta güvenliği konusunda eğitilmemişlerse, gönderdikleri e-postaların başkalarının eline geçmesinin, günümüz teknolojisi ile çok basit olduğu hakkında bilgi sahibi değillerse, gönderdikleri bilgilerin karşı tarafa ulaştırılması sırasında, araya giren bir saldırgan tarafından verilerde değişiklik yapılabileceğini bilmiyorlarsa, bu kurumun bilişim güvenliği yönünden alacağı bütün teknolojik önlemler boşa çıkacaktır.

Kullanıcı bilinçlendirilmesi olmadan, bilişim güvenliğinden söz edilemez. Kullanıcıların eğitim ve farkındalık yaratma süreçleri ile bilinçlendirilmesi, sosyal faktörlerin bilişim güvenliği açısından oluşturdukları riskin de azaltılmasını sağlayacaktır. [95]

Eğitim ve Farkındalık yaratma süreç alanı da aşağıdaki süreçlerle ifade edilebilir:

1. **Bilinçlendirme Eğitimleri:** Bu tür bir eğitimde, konu hakkında temel bilgilendirme ve genel bir bilgi vermek amaçlanır. Bu tür eğitimlere teknik olmayan personel ile yönetici düzeyindeki personel katılabilir.
2. **Kullanıcı Eğitimleri:** Belli bir teknolojinin ya da uygulamanın teknik olmayan kullanıcılar düzeyinde kullanımı konusunda bilgi verme amaçlı eğitimlerdir. Bilinçlendirme eğitimlerine göre daha derinlemesine bir eğitim türüdür. Katılacak kullanıcılar teknik olmayan son kullanıcılardır.
3. **Teknik Eğitimler:** Belli bir teknolojinin yönetilmesi, gerektiğinde yeni düzenlemelerin ve ayarların yapılması konusunda verilen derinlemesine eğitimlerdir. Kurumun güvenlik yönetiminden sorumlu personeli katılabilir.

## 4.2.Yönetsel Önlemler

Bir kurumun elindeki bilgisayarlar ve bu bilgisayarlar üzerinde bulunan veriler, genellikle, kurumun kritik amaçları ve hedefleri ile doğrudan bağlantılıdır. Bu nedenle, kurumun üst yönetimi, bu kaynakların korunmasını kendine bir görev olarak almalı ve gerekli zaman, para ve insan kaynağının bu tür faaliyetlere tahsisi gerçekleştirmelidir.

Yönetsel önlemler, bilişim güvenliği açısından en yukarıdaki üst yöneticilerden en alttaki son kullanıcılara kadar, hiyerarşik bir sorumluluk yapısını ortaya koyar. Önce, nelerin hangi düzeyde bir güvenlik ihtiyacı olduğu belirlenmelidir. Yasal platformda, yürürlükte olan ve bilişim güvenliği konularını da kapsayan kanunların ve tanımlanan sorumlulukların anlaşılması ve kurumun bir bütün olarak bu sorumlulukları yerine getirmesinin sağlanması, yönetsel önlemler açısından değerlendirilmelidir.

Bu durumda, bir kurumun güvenlik yönetimi biriminin temel görevi, güvenlik yönetimine yönelik yönerge ve direktifler oluşturmak değil, öncelikle üst yönetimden güvenlik yönetimi ile ilgili gelen istekleri yerine getirmek olmalıdır. Üst yönetimin desteği olmadan, kurumsal tabanda bir işi gerçekleştirmek hayli zordur. Bu nedenle üst yönetim ile güvenlik yönetimi arasında açık bir iletişim kanalı kurulmalı ve her iki yönde de kusursuz bir bilgi akışı sağlanmalıdır. Bu sayede, yürütülen güvenlik yönetim programı üst yönetimden ihtiyacı olan desteği alır, üst yönetim de gerektiğinde devreye girerek gerekli stratejik kararları verir.

“Bilişim Güvenliği” açısından uzun soluklu bir stratejinin oluşturulması, kurumun bireylerden bağımsız olarak bir güvenlik altyapısı kurması için gerekli bir ön koşuldur. Bu amaçla geliştirilecek olan güvenlik politikalarında kullanılan dil, girilecek ayrıntı seviyesi, politikanın yazılış biçimi gibi faktörler dikkate alınmalıdır. Güvenlik politikasının yalnızca teoride ve lafta kalan bir doküman değil, bunun yerine uygulamaya dönük bir içeriğe sahip olması için gereken çaba gösterilmelidir.

Güvenlik yönetiminin yetersiz olması, kurum bazında güvenlik alanında gerçekleştirilen tüm çabaların boşa gitmesinin sebebi olabilir. Eğer üst yönetim, güvenlik gereksinimlerini tam olarak anlayamaz ise, yönetimin diğer hedeflerinin yanında pahalı, gereksiz, görünürde hiçbir yararı olmayan bir faaliyet olarak görebilir ve yeterli desteği sağlamayabilir. Böyle bir durumda, bilişim güvenliği alanındaki en güçlü teknolojiler satın alınsa bile, yönetim desteği olmadığı takdirde verimsiz ve âtıl birer yatırım olarak kalacaklardır. [95]

### 4.2.1 Risk Yönetimi

Risk, kuruma zarar verici bir olayın gerçekleşme olasılığı, olarak tanımlanabilir. Risk yönetimi ise, kurumun karşı karşıya bulunduğu risklerin tanımlanması, bu risklere değer biçilmesi, risklerin kabul edilebilir bir seviyenin altına indirilmesi ve sürekli bu seviyenin altında kalmalarını sağlayacak mekanizmaların devreye sokulmasıdır.

Yüzde yüz güvenli bir çalışma ortamı kurmak imkânsızdır. Her çalışma ortamında, bir takım güvenlik boşlukları ve bunlara bağlı riskler mevcuttur. Yapılması gereken, karşı karşıya olduğumuz riskleri, doğru bir şekilde yönetmektir.

Bilişim Güvenliği açısından karşımıza çıkabilecek riskler, aşağıdaki şekilde sınıflandırılabilir:

* Fiziksel zarar
* İnsan hatası
* Donanım hatası
* Gizli verilerin ifşası/değiştirilmesi
* Verilerin yok olması
* Yazılım uygulamalarının hatalı çalışması [95]

#### 4.2.1.1 Kurumsal Bilgi Kaynaklarına Değer Biçme

Kurumsal bilgi kaynaklarına değer biçilirken, farklı açılardan bakmak gerekebilir. Örneğin, bir sunucu bilgisayarın satın alma maliyeti 5 Milyar TL ise bu kaynağa 5 Milyar TL değer biçmek doğru değildir.

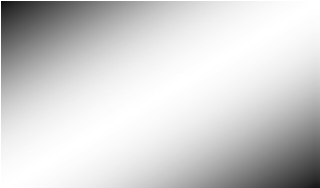
Değer biçme sırasında göz önünde bulundurulması gereken birtakım hususlar şunlardır (Burada belirtilen hususların tümü her bilgi kaynağı için uygun olmayabilir):

* Kaynağın yeniden satın alınması ya da geliştirilmesi maliyeti
* Kaynağın idamesi ve korunması maliyeti
* Kaynağın sahipleri ve kullanıcıları açısından maliyeti
* Kaynağın, kurumun rakipleri açısından maliyeti
* Fikir hakları açısından maliyeti
* Başka kurumların kaynağa sahip olma maliyeti
* Kaynağın yok olması durumunda üretimin etkilenmesi ve operasyonel açıdan yaratacağı etkiler sonucunda ortaya çıkacak olan maliyet
* Kaynağın açığa çıkması durumunda doğacak sorumluluğun maliyeti
* Kaynağın kullanışlılığı açısından maliyeti [95]

#### 4.2.1.2 Risk Analizi

Risk analizi, risklerin gerçekleşme olasılıklarının, gerçekleşmeleri durumunda yol açacakları kayıpların doğru bir şekilde belirlenmesi ve buna göre uygun tedbirlerin devreye sokulmasıdır. Risk analizinin üç temel amacı vardır:

* Risklerin belirlenmesi
* Tehditlerin potansiyel etkisinin belirlenmesi
* Riskin gerçekleşmesi durumunda getireceği zararla, bu riskten korunmak için seçilecek tedbir arasında ekonomik bir denge kurulması



Kurumsal Bilgi

Kaynaklar

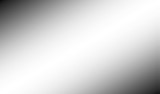
ı

na

De

ğ

er Biçme

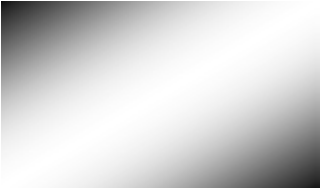


Risk Analizi ve

De

ğ

erlendirme



Kar

ş

ı

-

tedbirlerin

belirlenmesi ve

gerçeklenmesi

Şekil 4.2.1.2: Risk Yönetiminin Adımları

Doğrudan ve dolaylı maliyetler dikkate alınmadığında, bir kurum için, kâğıt üstünde “çok güvenli” bir güvenlik altyapısı kurmak kolaydır. Ancak kurumun hedefi, kendisi için “yeterli, etkin ve yönetilebilir” bir güvenlik altyapısını oluşturmak olmalıdır. Bu yeterlilik düzeyini belirlemekte risk analizi önemli bir role sahiptir. Risk analizi yardımıyla kurumlar, karşı karşıya bulundukları riskleri öncelik sırasına koyabilir ve her bir riske karşı alınacak önlemlerin ve tedbirlerin getireceği maliyetleri değerlendirebilirler.

Risk analizi sayesinde kurum çalışanları bir maliyet/yarar analizi yapabilirler. Kullanılacak tedbirlerin yıllık maliyetleri ile bir tehdidin gerçekleşmesi durumunda neden olacağı zarar karşılaştırılabilir. Örneğin gizli bir bilginin değeri 100 Milyar TL ise, bu veriyi korumak için 150 Milyar TL harcamanın bir anlamı yoktur.

Risk analizi yardımı ile kurumun bilişim güvenliği konusundaki amaçları ile diğer kurumsal amaçlar bütünleştirilebilir. Bu bütünleştirme derecesi, amaçlara ulaşmada doğrudan bir etkendir. [95]

#### 4.2.1.3 Tedbirlerin Seçimi

Tedbir, ya da başka bir deyişle “koruyucular”, maliyet-etkin ve kendisine harcanan paranın hakkını verecek şekilde seçilmelidir. Bir koruyucunun kullanımında karşılaşılabilecek maliyetler aşağıdaki tabloda gösterilmiştir:

* Çalışma ortamında yapılması beklenen değişiklikler
* Üretkenliğe Etkisi
* İdamesi için gereksinimler
* Diğer tedbirlerle uyumlu çalışabilme
* Test gereksinimleri
* Gerektiğinde onarım/yerine yenisini koyma ve güncelleme maliyetleri
* Tasarım/Planlama
* Operasyon ve Destek [95]

### 4.2.2 Güvenlik Politikaları

Güvenlik Politikası, kurumda güvenliğin oynadığı rolün genel bir anlatımıdır. Güvenlik Politikası üst yönetim, seçilmiş bir Kurul ya da bir Komite tarafından yazılabilir. Güvenlik Politikaları, bireylerden ve teknolojiden bağımsız hazırlanmalıdır. Kurumda uygulanacak güvenlik kontrolleri, ayrıntıya girilmeden kavramsal olarak tanımlanmalıdır.

Internet Week dergisinin 2000 yılı sonunda üst düzey yöneticiler arasında yaptığı bir araştırmaya göre, araştırmaya katılanların %70’i kurumlarında güvenlik teknolojisinin kullanılmakta olduğunu bildirmiş, ancak yalnızca %38’i yazılı bir güvenlik politikasına sahip olduklarını söylemişlerdir.

Güvenlik politikasının kuruma üç yararından bahsedilebilir:

1. Kurum çalışanlarını ve üçüncü tarafları yasal sorumluluktan kurtarmak,
2. Kuruma özel gizli bilgileri; hırsızlığa, suistimale, yetkisiz kişilerin eline geçmesine, ifşaya ve değiştirilmeye karşı korumak,
3. Kurumun bilgi-işlem yeteneğini oluşturan kaynakların israfını ve boşa kullanımını engellemek.

Bir kurum için hiyerarşik olarak farklı düzeylerde güvenlik politikalarından bahsedilebilir:

1. **Kurumsal Güvenlik Politikası:** Üst yönetim tarafından, kurumda bilişim güvenliği programının çerçeve çalışması ifade edilir. Bu tür bir politika, kurumun gelecekteki tüm güvenlik faaliyetlerini kapsaması ve yönlendirmesi açısından önem taşır. Politika içerisinde; programın amaçları, verilecek sorumluluklar, güvenliğin stratejik/taktik açıdan önemi ve uygulamada yapılacak işler, genel hatları ile kavramsal olarak tarif edilir. Kurumsal Güvenlik Politikası içerisinde, ilgili kanunlara, yasal düzenlemelere ve diğer yönerge ve prensiplere başvurular yapılabilir. Üst yönetimin, bilişim güvenliği açısından kabul edilebilir bulduğu risk düzeyi de bu tür bir politikada yer alabilir.
2. **Konuya Özel Güvenlik Politikası:** Üst yönetim, belli konularda çalışanlarını daha fazla bilgilendirmek, daha ayrıntılı bilgi vermek, bu konuyu kapsamlı bir şekilde ifade etmek istediğinde bu tür bir politika geliştirilebilir. Örneğin, e-posta gönderme alma konusunda, üst yönetimin kararlarını, haklarını, yapıp-yapamayacaklarını bu tür bir politika içerisinde ifade etmek uygun olacaktır. Üst yönetimin, gerekli görüldüğünde çalışanların e-postalarını okuyabileceği, epostalar yoluyla gizlilik dereceli bilgilerin gönderilip alınamayacağı gibi hususlar, e-posta özel politikası içerisinde ifade edilir.
3. **Sisteme Özel Güvenlik Politikası:** Üst yönetimin, bilgisayarlar, bilgisayar ağları ve uygulamalar ve kurumsal veriler hakkında aldığı ayrıntılı kararları içerir. Bu tür bir politika içerisinde, kullanılmasına izin verilen yazılımlar, veritabanlarının nasıl korunacağı, bilgisayarlara uygulanacak erişim denetim kriterleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular açıklanabilir.

Güvenlik politikalarını desteklemek üzere daha ayrıntılı birtakım dokümanlar oluşturulabilir. Kurumun stratejik ve taktik hedefleri arasındaki farklılık, politika ile standart, yönerge ve prosedürler arasındaki farklılıkta da kendini gösterir. Güvenlik Politikası, kurumun stratejik bir hedeflerini içerirken; standart, yönerge ve prosedürler taktik düzeyde olan hedefler içerir. Taktik hedefler, stratejik hedefleri gerçekleştirmek amacıyla ortaya konur. [95]

### 4.2.3 Standartlar, Yönergeler ve Prosedürler

Bir kurumun *güvenlik standartları*, o kurumdaki bilgisayar yazılım ve donanımlarının nasıl kullanılacağı hakkında bilgi verir. Kullanılan teknolojilerin ve uygulamaların, her bir kullanım sırasında tanımlanmış standartlara uygun olarak kullanılmasını garanti eder.

*Yönergeler*, kurumsal bir standardın belli bir uygulamada kullanılmasında güçlük çekildiğinde, yol gösterici birtakım öneriler içerecek şekilde hazırlanırlar. Standartlar, gerçek hayatta ve uygulamada karşılaşılabilecek bütün durumları ele alamayabilir. Bu durumda bir yönerge yardımı ile standartta yeterince açık olmayan “gri alanlar” açıklığa kavuşturulur.

*Prosedürler*, belli bir işi gerçekleştirmeye yardımcı olmak amacıyla hazırlanmış olan ve atılacak adımları ayrıntılı olarak içeren dokümanlardır. Örneğin bir yazılımın yüklenmesi, bir donanımın kurulması, yazılım ya da donanımın ayarlarının değiştirilmesi/düzeltilmesi, sistemde yeni bir kullanıcı hesabının tanımlanması, yok edilmesi gereken malzemenin nasıl imha edileceği gibi konularda prosedürler hazırlanabilir. Tanımlanmasında büyük yarar olan prosedürler şunlardır:

* Konfigürasyon Yönetim Prosedürü
* Yedekleme ve Yedekleme Ortamlarını Saklama Prosedürü
* Olay Müdahale Prosedürü
* İş Sürekliliği ve Felaket Kurtarma Prosedürü

Prosedür, yönerge ve standartlar, birbirleri ile bütünlük içinde ve birbirlerini destekleyecek şekilde hazırlanmalıdır. Örneğin bir yönergede, “kullanıcının bir sisteme girmesi için kimlik sınamasından geçmesi gerektiği” yazıyorsa, ilgili prosedürde de bu tür bir kimlik sınaması için yapılması gereken faaliyetler adım adım ve okuyanın anlayacağı bir şekilde belirtilmelidir.

Prosedür, yönerge ve standartları, tek bir büyük dokümanın içine sıkıştırmak yerine, modüler bir şekilde hazırlamak, kullanım kolaylığı ve esneklik açısından daha verimli bir çalışma sağlayacaktır.

Çünkü bu türlerden her birinin kullanım alanı ve kullanacak kişiler farklılık gösterir bu şekilde dokümanların kullanıcılarına dağıtılması ve gerektiğinde güncellenmeleri kolaylaşmış olur. [95]

### 4.2.4 Güvenlik Yaşam Döngüsü

Çeşitli teknik ve yönetsel yönlerini vurgulamış olduğumuz bilişim güvenliği kavramlarının etkinliğini sağlamak, konuyu sürekli canlılığını koruyacak bir yaşayan proje olarak ele almakla mümkün olacaktır. Tehditlerin sürekli olarak yenilenmesi ve çeşitlilik kazanması, kullanılan altyapıların sık aralıklarla güncelleme, iyileştirme, genişleme ve benzeri değişikliklere uğraması ve yazılım sistemlerindeki sürekli değişimler, herhangi bir anda güvenli kabul edilebilecek bir sistemin takip eden sürede güvenli kalmasını garanti edemez. Bu nedenle, güvenlik çalışmaları bir yaşam döngüsü ile modellenmektedir.

Genel kabul görmüş yaklaşımlardan biri olan CERT (Computer Emergency Response Team) tarafından önerilen yaşam döngüsü, aşağıdaki adımları içermektedir:

* Sistem Güçlendirme (Harden / Secure)
* Hazırlık (Prepare)
* Saldırı / Sorun Tespiti (Detect)
* Tespit edilen olaya özgü önlemlerin alınması / kurtarma (Respond)
* İyileştirme, tespit edilen olayın tekrarını önleyecek önlemler (Improve)

Bu adımların tekrarlı bir biçimde gerçekleştirilmesi sayesinde, sürekli olarak potansiyel sorunlar tespit edilebilir ve zamanında önlem alınarak sistem güvenliği azami seviyede korunmaya çalışılır.

### 4.2.5 Güvenlik Denetimleri

Güvenlik denetimi, bir kurumun güvenlik altyapısının, güvenlik politikasının, prosedürlerinin ve personelinin ayrıntılı bir biçimde ele alınması, zayıf yönlerin tespiti ve bu zayıflıkların giderilmesi için öneriler sunulmasıdır.

Başarılı bir denetim, tüm ilgili tarafların iş birliği ile gerçekleştirilebilir. Genelde güvenlikle ilgili bir denetim söz konusu olduğunda, birçok insan olumsuz bir önyargıya kapılır ve rahatsız olur. Bununla birlikte, güvenlik denetimi kurum içinde güvenlik politikasına uygun çalışılıp çalışılmadığının tespitinde kullanılabilecek tek yoldur.

Denetlenecek faaliyetler arasında; bilgisayarlara giriş/çıkışlar, dosya işlemleri ve sistem ve ağ erişim haklarının değiştirilmesi olarak sayılabilir. Bir denetim sırasında sorgulanabilecek konulardan bazıları şunlardır:

* Hangi veriler “salt okunur”, hangileri “yazılabilir”dir?
* Önemli verileri kim/ne değiştirebilir?
* Sistem erişimini ve kaynak kullanımını ne engelleyebilir?
* Sistem üzerindeki değişiklikler nasıl yapılmaktadır?
* Sisteme nasıl erişilebilir?
* Bilgisayarlar, bilgisayar ağları ve bunların bulundukları binalar fiziksel açıdan güvenli mi?
* Sistemde yapılan değişiklikler izleniyor mu?
* Sistemde aksaklık çıktığında, bunun nedenleri ortaya çıkarılabiliyor mu?
* Kullanıcı grupları tanımlanmış mı? Hangi kullanıcıların erişim yetkileri, diğerlerine nazaran daha fazla? Tüm kullanıcıların sahip olduğu haklar neler?

İki tip denetim vardır. Biri kurumun kendi personeli tarafından gerçekleştirilen “İç Denetim”, diğeri ise kurum dışı, bağımsız bir kuruluş tarafından gerçekleştirilen “Dış Denetim”dir.

Başarılı bir denetim için iki temel nokta göz önüne alınmalıdır:

1. Planlama: Bir denetim planında, kurumun hangi açılardan denetleneceği ve sonuçların nasıl değerlendirileceği ortaya konur.
2. Kullanılan Araçlar: Denetimin yapılmasına yardımcı olacak belge, yazılım, kamusal birtakım kriterler bu sınıfa girerler. [95]

## 4.3.Teknoloji Uygulamaları

Bu bölümde, güvenlik tedbirlerinde kullanılan teknolojilerden bahsedilmiştir. Tüm teknolojiler burada bahsedilenlerle sınırlı değildir. Bunun yanında burada adı geçen teknolojiler, bilişim güvenliği söz konusu olduğunda ilk akla gelenlerdir. Sırasıyla Bölüm 3.1’de Kriptografi, Bölüm 3.2’de Sayısal İmza ve PKI, Bölüm 3.3’de Ağ Bölümlemesi ve Güvenlik Duvarları, Bölüm 3.4’de Yedekleme, Bölüm 3.5’de Saldırı Tespiti ve İzleme, Bölüm 3.6’da Erişim Denetimi ve Bölüm 3.7’de Anti-virüs teknolojilerinden bahsedilmiştir.[95]

### 4.3.1 Kriptografi

Kriptografi, veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan bir teknolojidir. Kriptografi’de veri, matematiksel yöntemler kullanılarak kodlanır ve başkalarının okuyamayacağı hale getirilir. Bu matematiksel kodlamaya “*kripto algoritması*” adı verilir. İlk bilinen kripto algoritmaları 4000 yıl kadar önce ortaya çıkmıştır. Zaman geçtikçe, kullanılan teknikler ve cihazlar gelişmiş ve her geçen gün yeni teknikler kullanılır ve yeni algoritmalar üretilir olmuştur. Bu teknoloji şu anda bilişim güvenliğinin vazgeçilmez bir parçasıdır.



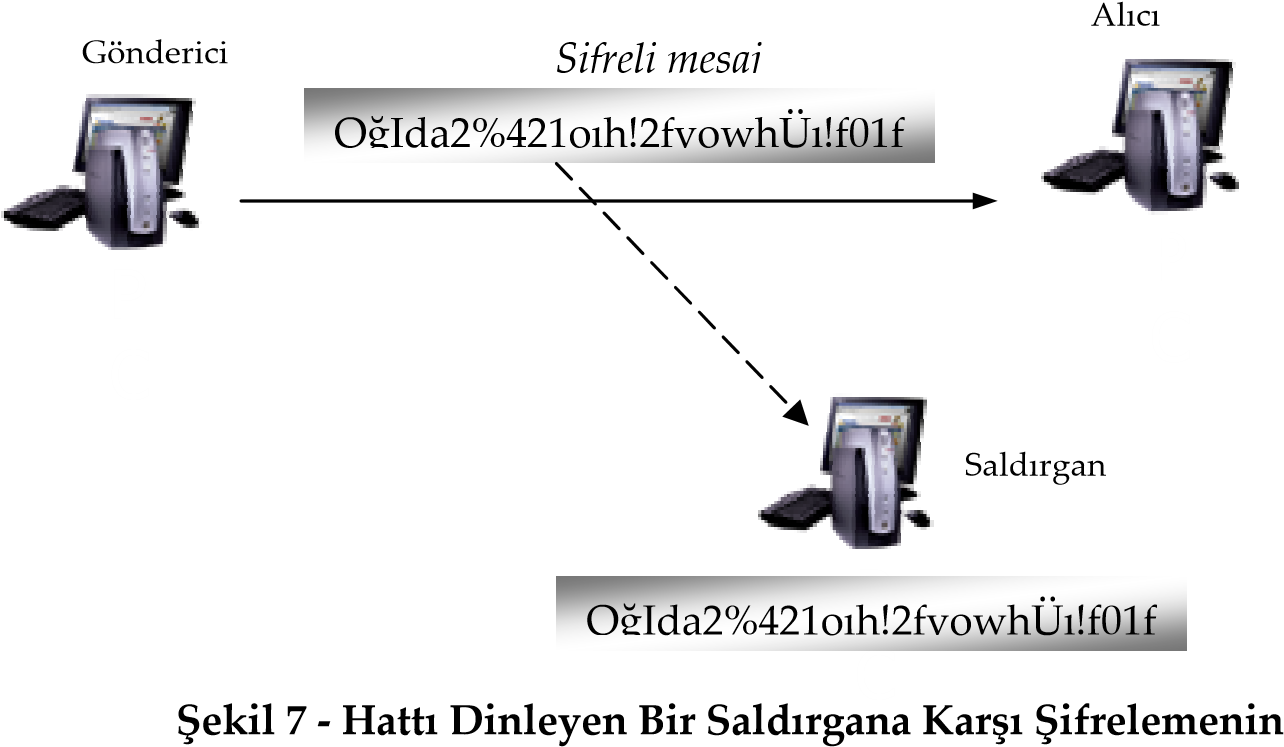
Şekil 4.3.1: Temel Kriptogtafi Mekanizması

Şifrelenmemiş bir bilgiye “açık metin” (clear text) denir. Açık metin, bir insanın okuyabileceği bir yazı ya da bir bilgisayarın anlayabileceği çalıştırılabilir (.exe, .com) bir program ya da bir veri dosyası (.txt) olabilir. Bir kripto algoritması kullanılarak, herkesin okuyamayacağı bir şekilde kodlanmış bilgiye ise “şifreli metin” (ciphered text) denir. Açık metinden şifreli metne geçme işlemi “şifreleme”, şifreli metinden açık metne geçme işlemi ise “şifre çözme” olarak adlandırılır. Şifreleme ve şifre çözme yapan bir sistem de “kriptosistem” olarak adlandırılır. Bir kriptosistemin, şifreleme ve şifre çözme yapan hem donanım hem de yazılım bileşenleri olabilir.

Algoritmalar, açık metin üzerinde yapılan karmaşık işlemlerden oluşan matematiksel formüllerdir. Bir algoritma, hem yazılımla hem de donanım bileşenleri ile gerçekleştirilebilir. Birçok algoritma, şifreleme ve şifre çözme işlemini gerçekleştirmek amacıyla, açık metinden başka, “anahtar” denen bir değer de kullanır. Anahtar “0” ve “1”lerden oluşan uzun bir bit dizisidir. Her algoritmanın kullandığı anahtar boyları farklıdır. Genellikle anahtar boyu arttıkça, olası anahtar sayısı arttığından, saldırganın bu şifreyi çözmesi güçleşir, ama aynı zamanda da şifreleme ve şifre çözme hızı yavaşlar. Bir algoritmanın olası tüm anahtarlar olasılıklarının oluşturduğu topluluğa “anahtar uzayı” denir.

Şekil 4.3.1.a’da bir saldırganın hattı dinleyerek mesajı ele geçirmesi gösterilmiştir. Ancak saldırgan mesaja sahip olsa bile, mesaj kriptolu olduğundan içeriği konusunda bilgi sahibi olamaz.

Kripto sistemleri, ilk bölümde bahsedilen Gizlilik, Veri Bütünlüğü, Kimlik Sınaması ve İnkâr Edememe hizmetlerinde kullanılır. [95]



Şekil 4.3.1.a: Kullanışı

Kripto algoritmaları temelde ikiye ayrılırlar: Simetrik Algoritmalar ve Asimetrik algoritmalar. Aşağıdaki bölümlerde bu iki algoritma türü sırasıyla tanıtılmıştır. Bölüm 3.1.3’de ise özetleme fonksiyonlarından bahsedilmiştir.

#### 4.3.1.1 Simetrik Algoritmalar

Simetrik algoritmalarda şifreleme ve şifre çözme için aynı anahtar kullanılır. Bu anahtara Secret Key denir. Bu gizli anahtar iki tarafça da (gönderici ve alıcı) bilinir.

Simetrik algoritmalar asimetrik algoritmalara nazaran daha hızlı çalışırlar. Bununla beraber, asimetrik algoritmalara nazaran saldırıya karşı daha az dirençlidirler. Simetrik algoritmalara örnek olarak AES, DES, 3DES, Blowfish, IDEA, RC4 ve SAFER algoritmaları verilebilir. [95] [96]

#### 4.3.1.2 Asimetrik Algoritmalar

Şifreleme ve şifre çözme için ayrı anahtarlar kullanılır. Bu anahtarlardan birine Public Key, diğerine Private Key denir. Kullanılacak bu iki anahtar birlikte üretilirler. Bununla birlikte bu anahtarlardan herhangi birine sahip olan bir şahıs, diğer anahtarı üretemez, bu matematiksel olarak imkânsız denebilecek derecede zordur.

Asimetrik algoritmalar, simetrik algoritmalara göre daha güvenli ve kırılması zor algoritmalardır. Bununla birlikte, başarımları (performans) simetrik algoritmalara göre oldukça düşüktür. Asimetrik algoritmalarda her şahsın bir anahtar çifti vardır. Bir şahsın özel anahtarı, yalnızca kendi kullanımı içindir ve başkalarının eline geçmemesi gerekir. Bu şahsın açık anahtarı ise, bu şahsa mesaj göndermek isteyen herhangi biri tarafından kullanılabilir. Gönderici mesajı, alıcının açık anahtarı ile şifreler. Alıcı, gelen mesajı kendi özel anahtarı ile açar.

Mesaj gönderebileceğimiz kullanıcıların sayısı arttıkça, elde etmemiz gereken açık anahtar sayısı da artacaktır. Sistemde 100 kullanıcı varsa, her bir kullanıcının ayrı bir açık anahtarı olacağından, tüm bu açık anahtarlar, erişilebilir olmalıdır. Bu problem de sayısal sertifikalar teknolojisi yardımı ile çözülebilmektedir. Bölüm 4.3.2’de bu teknoloji açıklanmaktadır.

Asimetrik algoritmalara örnek olarak RSA, ECC, Diffie-Hellman ve El Gamal algoritmaları verilebilir.

Görüldüğü gibi simetrik ve asimetrik algoritmaların birbirlerine göre birtakım üstünlükleri ve zayıf yönleri vardır. Her iki algoritma grubunun üstünlüklerinden faydalanarak zayıf yönlerini bir kenara bırakmak amacıyla “hibrid kripto sistemler” kullanılmaktadır. Bu tür sistemlerde hem simetrik hem de asimetrik algoritmalarla hem başarımı hem de güvenliği yüksek şifreleme yapılabilmektedir. [95] [96]

#### 4.3.1.3 Özetleme Fonksiyonları

Bir özetleme fonksiyonu, herhangi bir uzunluktaki metni, giriş değeri olarak alır ve sonuç olarak sabit uzunluklu bir değer üretir. Bu değere Message Digest adı verilir. Burada üretilen özet, fonksiyona giren metnin karakterini taşımaktadır denilebilir. Giriş metninde yapılacak tek bir karakter değişikliği bile üretilecek özette büyük değişikliklere yol açar. Ayrıca, özetleme fonksiyonu tek yönlü olduğundan, özetten asıl metne geri dönüş yoktur. Özetleme fonksiyonları, uzun metinlerin, asimetrik bir algoritma ile şifrelenmeleri sırasında, asimetrik algoritmanın başarım dezavantajını ortadan kaldırmak amacıyla kullanılırlar. Tüm mesaj metni değil de yalnızca mesajın özeti alınarak asimetrik algoritmayla şifrelenir. Özetleme algoritmalarına örnek olarak SHA-1, DSS, MD2, MD4, MD5 algoritmaları verilebilir. [95] [96]

### 4.3.2 Sayısal İmza ve PKI

Bir sayısal imza, şifrelenmiş bir özet (hash) değeridir. Sayısal imzalar yardımıyla, alıcı taraf göndericinin kimliğinin sınamasını yapar ve göndericinin kim olduğundan tam olarak emin olur. Bunun yanında, sayısal imza teknolojisi, gönderilen verilerin bütünlük sınamasında da kullanılabilir. Buna göre sayısal imza teknolojisi, ilk bölümde bahsedilen Kimlik Sınaması ve Veri Bütünlüğü prensiplerinin gerçekleştirilmesinde kullanılırlar.

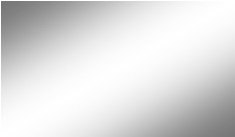
Sayısal imzalar, gerçek hayatta kullanılan ve elle atılan imzanın (ıslak imzanın) bilişim dünyasındaki karşılığı olarak görülebilir. Bir sayısal imza, imzaladığı içeriğin, imzalandığı andan itibaren değişmediğinin kanıtlanmasında kullanılabilir.

Sayısal imzalama, asimetrik kripto algoritmaları yardımı ile yapılır. Sayısal imzalama, mesaj bir mektup zarfına konulduğunda üzerinin mühürlenmesi gibi düşünülebilir. Sayısal imzalar, bilgisayar ağları yoluyla yapılan finansal işlemlerin güvenli bir şekilde yapılması ve veritabanı bütünlüğünün kontrolü gibi kullanım alanları bulmuşlardır.

Sayısal imzalar, Public Key Infrastructure (PKI) teknolojisinin de belkemiğini oluşturur. PKI, çok geniş bir coğrafi alana yayılmış kullanıcılar arasında, güvenli bir haberleşme altyapısı kurmayı hedefleyen bir teknolojidir. Public Key Infrastructure’ı oluşturan elemanlardan başlıcaları şunlardır:

1. **Sayısal sertifikalar:** Bir sayısal sertifika, gerçek hayatta kullanılan bir kimlik kartının, bilişim güvenliğindeki karşılığıdır. Bir sertifikanın içinde; sahibinin kimlik bilgileri, yetki derecesi, sertifikanın son kullanma tarihi, sahibinin kripto anahtarı bilgisi yer alır. Bir sayısal sertifika, bir kullanıcının bir sisteme girerken kimlik sınamasının yapılmasında ya da kriptolu e-posta mesajlarının

Dosya



Özetleme

fonksiyonu



**ÖZET**

ÖzelAnahtar

Say

ı

sal

İ

mza

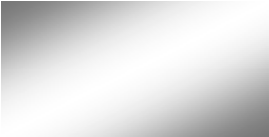


**Şİ**

**FRELENM**

**İŞ**

**ÖZET**



Say

ı

sal

İ

mza

Şekil 4.3.2: Bir Mesajın Sayısal İmzasıʹnın Oluşturulması gönderilmesinde kullanılabilir. Sayısal sertifikalar için ISO tarafından X.509 standardı yayınlanmıştır ve bu standart yaygın olarak kullanılmaktadır.

1. **Sertifikasyon Otoriteleri:** Bir PKI sistemine dahil olan kullanıcılar için sayısal sertifika üretim ve saklama merkezleridir. Bir kullanıcıya mesaj gönderilirken ya da gelen bir mesajdaki sayısal imzanın doğruluğunun sınanırken, o alıcının açık anahtarına ihtiyaç duyulur. Bu açık anahtarı elde etmek için, sertifikasyon otoritesinden, kullanıcının kimliği yardımı ile kullanıcının sayısal sertifikası elde edilir. Kullanıcının açık anahtarı, bu sertifika içerisinden alınarak kullanılır. [95]

### 4.3.3 Ağ Bölümlendirmesi ve Firewalls

Firewall, bir kurumun ağ güvenliği politikasının uygulanmasında kullanılan bir teknolojidir. Firewalls, bir bilgisayar ağından başka bir bilgisayar ağına geçişi sınırlarlar. Birçok kurum, kendi bilgisayarlarına, internet üzerinden gelebilecek saldırılara karşı güvenlik duvarlarını kullanır. Bunun yanında, kurum içi bir ağ bölümü ile yine kurum içi başka bir ağ bölümü arasındaki geçiş sınırlamasında da güvenlik duvarı kullanılabilir. Bir firewall, ağ üzerindeki bir boğum noktası olarak düşünülebilir. Çünkü iki ya da daha çok ağ arasındaki tüm trafik güvenlik duvarından geçmek zorundadır. Firewalls, yazılım olarak gerçekleştirilebildikleri gibi, yüksek trafik akışı olan noktalarda donanımla gerçeklenmiş güvenlik duvarları da kullanılmaktadır.

Birçok kurum firewall’ları, demilitarized zone kurulumu için kullanır. Bu düzenlemede güvenlik duvarının üç bacağı vardır: Birinci bacak dış ağ ile irtibatı ikinci bacak iç ağ ile irtibatı sağlar. Üçüncü bacak ise iç ve dış ağ arasında kalan “demilitarized zone” kurmayı sağlar. Bu üçüncü bacağın olduğu bölgeye, kurumun dışarı açık, web, e-posta ve DNS gibi birtakım hizmetlerinin sunulduğu bilgisayar kaynakları koyulabilir. Çünkü bu kaynaklar, saldırganlar tarafından ilk olarak saldırıya maruz kalması beklenen kaynaklardır. Günümüzde arınmış bölgelerin çoğunda kurulan bir Intrusion Detection System (IDS) yardımıyla saldırgan davranışları izlenerek gerekli tedbirler alınmaktadır.

Firewalls, Network Address Translation (NAT) hizmeti yardımı ile iç ağdaki bilgisayarların IP adreslerini, dışarıdaki saldırganlardan gizler.

Firewalls, iç ağdaki bilgisayarlara proxy hizmeti verebilirler. Bu şekilde, örneğin iç ağdaki bir kullanıcının bilgisayarı ile bu kullanıcının internet üzerinde bağlandığı web sayfası arasında doğrudan bir bağlantı kurulmaz. Bunun yerine kullanıcı ile vekil sunucu ve vekil sunucu ile internet sayfası arasında kurulan iki bağlantı söz konusudur. Vekil sunucunun görevi, kullanıcıya, kendi varlığını hissettirmeden, bağlantılar arasında verilerin taşınması ve bu sırada da tanımlanmış güvenlik politikasına göre de gelip geçen verilerin kontrol edilmesidir. [95]

Internet üzerinde belli ağ bölümlerine ya da hizmetlere erişilmesini engellemek ya da internet üzerinden kurumsal ağlardaki kaynaklara erişimi düzenlemek için de firewall’ların packet filtering hizmetinden faydalanılır. Bir packet filtering, kendisine gelen veri paketinin 5 özelliğine bakarak paketin, diğer ağ bölümüne geçişine izin verip vermeme kararını verir. Bu özellikler şunlardır:

1. Kaynak IP adresi
2. Kaynak hizmet noktası (port)
3. Hedef IP adresi
4. Hedef hizmet noktası
5. Bağlantı tipi (TCP, UDP, ICMP, vb.)

Paket eleyicilerin karar vermede kullandıkları politika tablosu da iki tür olabilir:

1. **Tanımlı olmayanlara izin verilmesi:** Paket eleyicinin politika tablosunda tanımlı olan kurallar dışındaki tüm trafiğin geçişine izin verilir. Örneğin kurum, kendi kullanıcılarının ICQ’ya ve IRC’ye bağlanmalarını istemiyorsa bu kurallar yazılır ve geri kalan tüm trafiğin geçişine izin verilir.
2. **Tanımlı olmayanlara izin verilmemesi:** Paket eleyicinin politika tablosunda tanımı olan kurallar dışındaki hiçbir trafiğin geçişine izin verilmez. Bu tür çalışmaya örnek olarak, kurum, kullanıcıların yalnızca web sayfalarına bağlanmasını istiyorsa, burada web sayfalarına erişimde kullanılan HTTP protokolünün hizmet numarası (port number) olan 80 tanımlanır. Bu şekilde herhangi bir sunucu üzerinde 80 numaralı porta erişimler hariç hiçbir trafiğe izin verilmez.

Bir kurumda birden fazla güvenlik duvarı art arda konularak çalışma verimi ve sağlanan güvenlik arttırılabilir. Daha yüksek güvenlik düzeyi gerektiren kurumsal bölümlerin ağ girişlerine de gerekirse ikinci bir güvenlik duvarı koyulabilir. [95]

### 4.3.4 Yedekleme

Bir sistemin yedeğini almak ve bunu düzenli olarak yapmak insanlara genellikle hep zor gelir; ta ki sistemlerinin devre dışı kaldığı, verileri kaybolduğu ya da bozulduğu güne kadar.

Sürekli ve tutarlı bir şekilde, çalıştığımız verilerin yedeğini almak, bir gün yaşayacağımız bir saldırı ya da doğal bir afetin sonuçlarının bizi en az şekilde etkilemesini sağlayabilir. Bir yedek alma sisteminin kurulmasının maliyeti, üretilmesi uzun zaman alan verimizi kaybettikten ya da veritabanımızdaki tüm kayıtlar silindikten sonra yeniden kazanma maliyetinden çok daha düşüktür.

Doğal olarak, sistemdeki her verinin yedeği alınmamalıdır. Bu tür bir çalışma yedekleme sistemimizin maliyetini oldukça arttıracaktır. Bu nedenle, hangi verinin bizim için kritik, önemli ve yedeği alınması gerekli veri olduğunun tespiti gerekir. Bu şekilde, farklı veri gruplarının yedekleme açısından öncelik sıraları belirlenir. Yedeği alınacak verilerin ve yedek alma sıklığının doğru tespiti ile yedekleme sürecini, sistemin günlük işleyişini en az şekilde etkileyecek şekilde düzenlemek gerekir.

Özellikle doğal afetlere karşı, yedeklerin farklı bir coğrafi bölgede saklanması gerekir. Bu tür bir yedeklemede veriler, çevrim-içi ve çevrim-dışı şekilde aktarılabilir. Çevrim içi aktarımda veriler, farklı bölgedeki merkeze, periyodik olarak bilgisayar ağı üzerinden aktarılır. Çevrim-dışı yolu ile yapılan yedeklemede ise, veriler, yüksek kapasiteli bir saklama ünitesi (teyp, flash bellek, taşınabilir hard disk, CDROM, DVD-rom gibi) üzerine yazılarak güvenli bir şekilde yedek alınan bölgeye ulaştırılır.

Veritabanı yedeklemesi, iş-sürekliliğinin sağlanmasında önemli bir faktördür. Kurumun veritabanlarını farklı bilgisayarlarda yedeklenmiş şekilde tutmak (replicated database), bir veritabanı sunucusunda meydana gelebilecek arıza ya da sistem güncelleme gibi durumlara karşı tüm sistemi toleranslı hale getirecektir.

Sistemlerin, elektrik kesilmelerine ve güç kaynağı arızalanmalarına karşı korunması da yedekleme konusunda ele alınabilir. Elektrik kesilmesi, hem kesinti boyunca çalışmamızın durmasına neden olur, hem de çalışan sunucumuz, “shutdown” gibi bir komut verilerek değil de sanki bir anda fişi çekilerek kapatıldığından, sunucuda geri dönülemez donanım ya da yazılım arızaları meydana gelebilir.

Bu tür durumlardan korunmak amacıyla, sistemler kesintisiz güç kaynakları ve yedek güç üniteleri ile desteklenmelidir. [95]

### 4.3.5. Saldırı Tespiti ve Saldırı Türleri

#### 4.3.5.1.Saldırı Türleri

##### 4.3.5.1.1 Sniffing

Sniffing temel olarak verinin yolunu kesmek olarak tabir edilebilir. Sniffing ile networkdeki paketler yakalanabilir içeriği okunabilir.

Kelime anlamı koklamak olan *sniffing*, bir ağ üzerindeki bilgisayarlar arasındaki veri trafiğinin dinlenmesi anlamına gelmektedir. Bunu yapmak için internette bol miktarda yazılım bulunmaktadır. Şebeke trafiğinin dinlenmesinde mantık, yönlendiricilere gelen her paketin kabul edilmesi dolayısıyla iki bilgisayar arasındaki tüm verilerin yakalanarak saklanmasıdır. Bu, korsanların kullandığı en önemli yöntemlerden birisidir. Bu yöntemden korunmak için bilgisayarlar arasındaki bağlantıların şifreli olması gerekmektedir. Kriptolu paketler de elbette dinlenip ele geçecektir ancak içeriğinden bir şey anlaşılamayacaktır. [76]

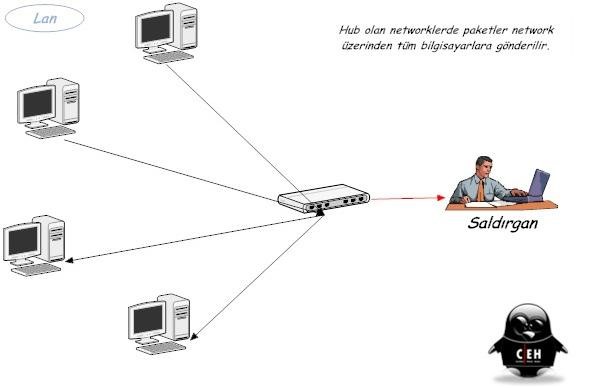
**Sniffingin Amacı**

Şifreleri (email, web, ftp, telnet, SQL), Email text’ini Transfer edilen dosyaları (e-mail, ftp) yakalamaktır. Sniffing metodu ikiye ayrılır; Pasif Sniffing ve Aktif Sniffing.

###### 4.3.5.1.1.1 Pasif Sniffing

Hub olan sistemler için geçerlidir, Hub olan networklerde paketler tüm bilgisayarlara iletilir.

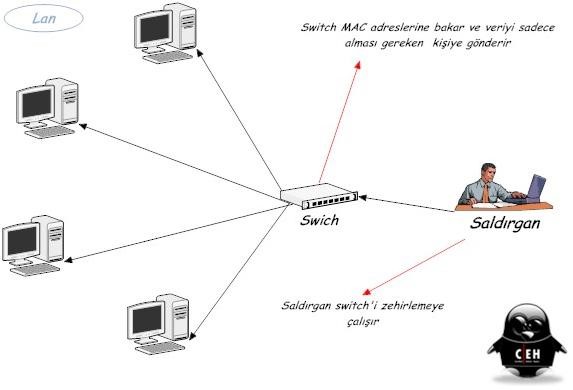
Networkteki veri lan üzerinden tüm bilgisayarlara gönderildiği için sniff etmek kolaydır.



Şekil 4.3.5.1.1.1: Pasif Sniffing

###### 4.3.5.1.1.2 Aktif Sniffing

Switch olan sistemler için geçerlidir. Switch MAC adreslerine bakar ve veriyi sadece alması gereken kişiye gönderir.



Şekil 4.3.5.1.1.2: Aktif Sniffing

Saldırgan switchi zehirlemeye çalışır, binlerce mac adresi gönderip switchin bir hub gibi davranmasına neden olur ve verinin tüm portlardan çıkmasını sağlar. [76]

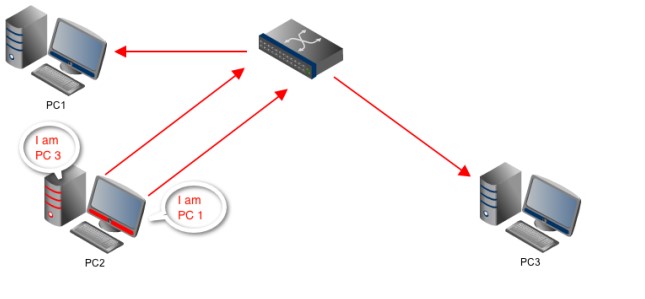
###### 4.3.5.1.1.3 ARP Poisoning

Arp veri göndermek için IP adresinin mac adresini çözümlemeye yarayan protokoldür. Arp paketleri taklit edilerek saldırgan kendi makinesine verileri yönlendirebilir. Saldırgan ARP poisoning yaparak iki bilgisayar arasındaki trafiğin ortasına geçebilir. Switche yapılacak flood ile verinin tüm portlara göndermesi sağlanarak sniff yapılabilir.

Adım 1: Saldırgan IP adresinin ve Mac Adresini gateway miş gibi broadcast yaparak duyurur.

Adım 2: Kurbanın internet trafiği saldırgan üzerinden geçmeye başlar ve saldırgan kurbanın tüm internet verilerini yakalar.

Adım 3: Saldırgan trafiği router a yollar.



Şekil 4.3.5.1.1.3: ARP Zehirlenmesi

**Korunma Yöntemleri**

Network kartlarına fiziksel ulaşımı engelleyerek sniffer kurulmasını engellenebilir.

Statik IP adresleri kullanın ve arp kayıtlarını statik olarak eklenebilir.

Netwrorkde sniffer olup olmadığını denetleyecek birden fazla araç vardır bunlardan bazıları;

* Arp Watch
* Promiscan
* Antisniff
* Prodetect
* Network swithlerinde Port güvenliğini sağlayacak özellikler aktif edilmelidir.
* Snifferlardan korunmanın en iyi yolu trafiği şifrelemektir. Bunun için Networkte SSH kullanan Ipsec kullanılır. Bu snifferın çalışmasını engellemeyecek fakat yakaladığı verilerin anlaşılmasını engelleyecek veya kırılması için gereken süreyi uzatacaktır.
* Büyük işletmelerde farklı vlan’lar tanımlanabilir. [76]

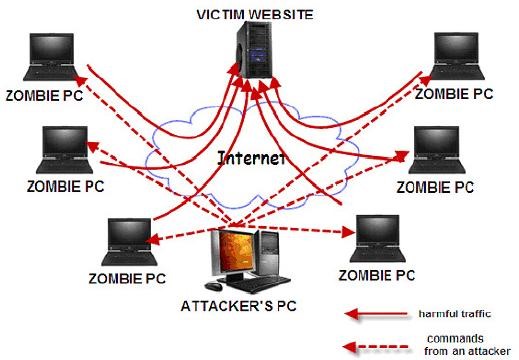
##### 4.3.5.1.2 Hizmet Dışı Bırakma (Denial Of Service)

DoS (Denial of Service), hizmeti aksatma veya hizmetin işlevini tamamen yok etme anlamına gelmektedir. İnternet kullanıcılarına ya hiç hizmet veremez ya da çok yavaş bir hizmet sunar.

DDos (Distrubuted Denial of Service) saldırısı ise, saldırganın saldırıya geçmeden önce oluşturduğu makine veya bilgisayar topluluğu ile hedefe saldırmasıdır ve DoS gibi hizmet aksatma veya hiç hizmet veremez hale getirme amaçlanır. Bununla birlikte saldırgan kolay bir şekilde kimliğini belli etmeden gizlenebilir ve saldırganın tespit edilmesi zorlaşır.

1999 yılında Minnesota Üniversitesi öğrencileri tarafından ilki gerçekleştirilen DDoS saldırıları, 2000 yılında Trinoo’nun, CNN, Yahoo, EBay, Datek gibi siteleri hedef alması, 2002 Kök DNS sunucularını hedef alan **DDoS atağı** gerçekleştirilmesi, 2007 yılında Estonya siber saldırıları, 2008 yılında gerçekleştirilen Gürcistan siber saldırısı, 2010 yılında Wikileaks gerçekleştirdiği, TİB, BTK, TÜBİTAK yönelik saldırılar ve 2011 yılında Anonymous’un Malezya, Türkiye, Paypal, Mastercard gibi ülkelere gerçekleştirilmiştir. Bu saldırılar daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara saldırı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesini amaçlayan saldırılardır.

DoS saldırı türünde amaç sınırlı sistem kaynaklarının sınırını aşarak, sistemin devre dışı kalmasını sağlamaktadır. [77]



Şekil 4.3.5.1.2: DDos Saldırısı

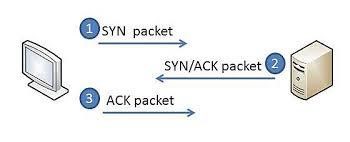
Saldırı DoS saldırısı olursa, yani tek bir IP üzerinden saldırı gerçekleşirse firewall’dan engellenebilir. Fakat DDoS saldırısında çok sayıda makine kullanıldığından, ip tespiti güçleşir ve firewall yakalayamayabilir. Log taşması sonucu firewall devre dışı kalabilmektedir. Bu nedenle DDoS, DoS saldırısına göre daha tehlikeli ve etkilidir. DoS saldırıları siber tehditler arasında 2. Sıraya girebilmektedir.

DRDoS, yani “Distrubuted Reflective Denial Of Service” DDoS’a benzerdir. Tek farkı, daha sık aralıklarla atak yapmak amacıyla ek ağlar kullanmaktadır. [77]

###### DoS Saldırı Çeşitleri

TCP three handshake tamamlanmadan yapılan bir yöntemdir. Yani istemci bir SYN, sunucuda buna yanıt olarak SYN+ACK paketlerini yollar ve ACK paketini beklemeye koyulur. Buraya kadar herşey güzel. ACK paketi gelmez ise bu bağlantı full-duplex değil "yarı-açık" bir bağlantı olurdu. Ve bu bağlantı çeşidi pek iç açıcı değildir.

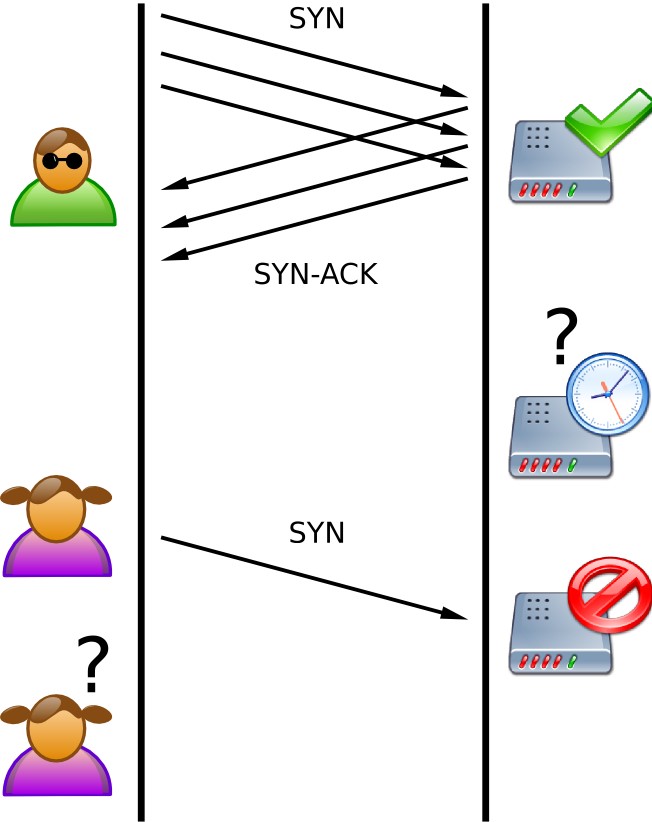
Sunucu SYN+ACK'yi yolladıktan sonra ACK için bekler. Fakat istemci ACK paketini yollamaz ise işler çıkmaza girer. Sunucu beklemeyi bırakmaz. Sürekli bekler. [77]



Şekil 4.3.5.1.2.a: TCP three handshake

Sunucu ACK için beklerken, karşıya ACK yerine bir bağlantı talebinde daha bulunduğumuzu varsayalım. Ve yine 3. adım'ı gerçekleştirmeyelim. Yani son ACK'yi yollamayalım. Hatta bunun tekrar tekrar yapılması ile sonuçta **"flood"** oluşur.

Hedef makine, saldırı yapılan makineden yanıt alamayacağından dolayı, SYN-ACK paketini 5 kez tekrar edecektir. Bunun tekrar süreleri, 3, 6, 12, 24 ve 48 saniyedir. Ayırdığı kaynağı boşa çıkartmadan evvel, 96 saniye sonra son bir kez SYN-ACK denemesi yapacaktır. Hepsini topladığınızda, görüldüğü gibi hedef makine ayırdığı kaynakları 3 dakika gibi bir süre tutacaktır. Bu sadece her bir SYN atağı için gerçekleşecek süredir. [77]



Şekil 4.3.5.1.2.b:TCP SYN Flood Saldırısı

Saldırgan bu tekniği tekrarlanan bir şekilde gerçekleştirdiği zaman, hedef makine ayırdığı kaynaklardan dolayı kaynak yetersizliğine kadar ulaşır ve artık yeni bir bağlantı karşılayamayacak duruma gelir. Ve bu durumda yetkili kullanıcılar bile makineye bağlanamaz. Yetkililer ne kadar bağlantı iptal ederlerse etsinler, yenileri eklenecektir.

TCP-SYN oturumu host ile client arasında kurulduktan sonra ACK veya PUSH ACK paketleri iletişim için kullanılır. Bu ACK paketleri kurban server'i n kaynaklarını tüketmeye başlarsa **ACK & PUSH ACK Flood** olarak adlandırılan atak gerçekleşmiş olur.

Eğer atak türü kurban nerwork'un bank genişliğini sömürürse, buna **ACK & PUSH ACK Flood** türü olan **Fragmented ACK** denir. Atak'da 1500 byte uzunluğunda paketler kullanılır.

TCP-SYN oturumunu sonlandırmak için **RST veya FIN** (açık olan TCP iletişim handshake oturumunu sonlandırma isteği) server değiştirir. **RST veya FIN** atak esnasında, kurban server **RST veya FIN** paketlerini yüksek oranda kaydeder ve sonuç olarak server'in kaynakları tükenmeye başlar (hafıza, CPU, RAM, vb.). Bu da RST **veya FIN Flood** olarak bilinir. Server bunu karşılayamazsa performansı azalır, isteklere cevap veremez veya kapanır. [77] [78]

###### 4.3.5.1.2.1 Land Flood

SYN Flood’a çok benzerdir. Bu atak çeşidinde hacker hedef sistemin IP adresini, source IP adresi olarak kullanarak networkü SYN paketleri ile istila ederler. Bu durumda host bilgisayar sanki paketleri kendi kendine göndermiş gibi görünür. Böylece, yukarıda söz ettiğimiz üç aşamalı bağlantı zincirinde (Three Way Handshake), hem dışarıdan paket almış, hem de kaynak kendisi olduğundan kendisine cevap vermiş olur. Böylece hedef sistem bir paket alması gereken birim zamanda iki paket alır ve saldırının boyutu da iki katına çıkar. Yani hedef sistem kendi kendine yanıt vermeye çalışırken sistem kullanılamaz duruma gelir. [77]

###### 4.3.5.1.2.2 UDP Flood

UDP, TCP’den en temel farkı belirttiğimiz gibi verinin ulaşıp ulaşmadığını garanti etmez. 3 yollu el sıkışma olmaması ve trafiğin karşı tarafa ulaşıp ulaşmadığını kontrol etmemesinden dolayı daha hızlı çalışır. UDP saldırısı uzaktaki bir bilgisayarın rastgele portlarına çok sayıda UDP paketi göndererek başlatılabilir. Bu durumda saldırıya uğrayan uzaktaki makine:

1. Portu dinleyen bir uygulama var mı diye kontrol eder;
2. Hiçbir uygulamanın o portu dinlemediğini görür;
3. ICMP "Hedefe Ulaşılamıyor" paketi ile cevap verir.

Böylece, çok sayıda UDP paketi gönderilmesi durumunda, mağdur sistem de yanıt olarak çok sayıda ICMP paketi göndermeye zorlanır ve bu da onun diğer istemciler tarafından erişilemez duruma gelmesine yol açabilir. **Saldırganın UDP paketlerinde sahte IP adresi olabilir, bu durum geri dönen ICMP paketlerinin ona ulaşmamasını** sağlar ve saldırganın bağlantı konumunu anonimleştirir.

Bu saldırı, istenmeyen ağ trafiğini filtrelemek üzere ağ içindeki kilit noktalara güvenlik duvarları kurularak yönetilebilir. Böylece, hedefteki makine UDP paketlerini asla almaz ve kötü niyetli UDP paketlerine asla cevap vermez. Çünkü güvenlik duvarı onları durdurur. [77] [78]

**UDP Fragmentation:** UDP flood türüdür. Büyük paketler kullanarak (1500 byte) bandgenişliğini sömürür. Bu paketler birbirleri ile ilişkisi yoktur ve paketler sunucuda birleştirilmeye çalışılır. Bu paketler birleştirilmeye çalışılırken CPU kaynağı harcanacaktır.

Bu sistemin yeniden başlamasını sağlar veya sistemin kapanmasına yol açar.

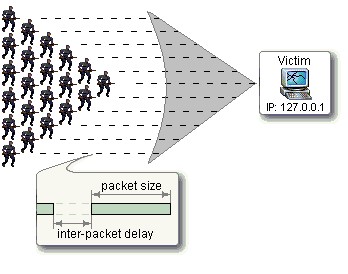
**VoIP Flood:** Özelleştirilmiş bir UDP Flood türüdür. Kurban VoIP server, yüksek sahte VoIP paketleri ve uzun IP dizilerini kaydeder. Network'u rasgele paket içeriğiyle ve iyileştirilmiş kaynak IP adresi ile istila eder.

**Non-Spoofed UDP Flood:** Bu atak yapılırken, kurban server sahte UDP paketi olmayan paketleri kaydeder ve gelen UDP paketlerin büyük miktarı istila eder. Atak network kaynaklarını tüketir ve sistem kapanır. Atak sırasında kullanılan IP sahte olmayan BOT'ların IP'sidir. [77] [78]

###### 4.3.5.1.2.3 ICMP Flood

Bu saldırı, ICMP (Internet Control Message Protocol) protokolünü hedef almaktadır. Bu sistemin özelliği, saldırının birden çok noktadan yapılması durumunda başarılı sonuç vermesidir. Aksi takdirde çok bir etkisi olmayacaktır. Bu saldırılar özellikle Linux üzerinden yapıldığında başarılı sonuçlar vermektedir ve saldırı için bazı özel komutlar kullanılmaktadır. Örnek olarak **“ping –s ip”** komutuyla 64 kb’lık paketler gönderilebilmektedir. Bu komutun, birçok farklı noktadan gönderilebileceği düşünülürse, oldukça etkili olduğu görülür.

ICMP, genel olarak sistemler arası iletişim ve hata ayıklama amacıyla kullanılan bir protokoldür. Hepimizin siyah ekran, cmd diye tabir ettiği komut satırı açarak yapabildiğimiz ping komutu bu protokol üzerinde çalışmaktadır. Bunun için CMD’ye **“ping –l 65510 ip”** yazmak işi görecektir. İstemci sistemin, hedef sisteme gönderdiği ICMP Echo Request (TYPE 8) paketine karşılık hedef sistem ICMP Echo Reply (TYPE 0) paketi gönderir. Böylece biz, hedef sistemin ulaşılabilir olduğundan emin oluruz. Burada hemen belirtelim, cevap gelmemiş olması sistemin ayakta olmadığını göstermez. [77]



Şekil 4.3.5.1.2.3: ICMP Flood Saldırısı

Bu yapıdan faydalanılarak, saldırgan makineler çok sayıda ICMP Echo Request (type 8) paketi gönderir. Kurban sistem, gelen tüm bu isteklere cevap vermek için çaba harcar ve sistem yorulmaya başlar. Sistem kaynakları bunlara cevap veremez hale gelir ve sistem erişilemez duruma düşer.

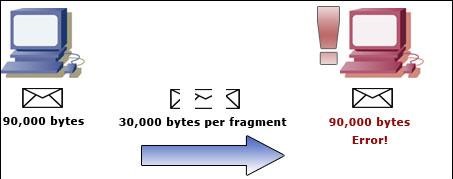
**ICMP Fragmentation:** Kurban server sahte, büyük ICMP paket parçaları (1500 byte) kaydeder ve bu baketler birleştirilemez. Büyük paket dizinleri ICMP atağın bant genişliğini artırır. Kullanışsız paketlerin birleştirilmesi girişiminde bulunduğunda CPU kaynakları devre dışı kalır. Ve fazla yükleme olduğunda yeniden başlayacaktır. [78] [77]

###### 4.3.5.1.2.4 Finger

Finger, belirli bir kullanıcı hakkında bilgi veren programdır, ayrıca kendi sisteminizde veya uzak sistemde giriş yapmış kullanıcıları listelemek için de kullanılır. Genelde kullanıcının tam adını, ne kadar zamandır işlem yapmadan beklediğini, hangi terminal hattından bağlandığını ve terminalin yerini gösterir. Bunlara ilaveten eğer mevcutsa kullanıcıya ait. Plan ve project dosyalarını görüntüler.

Farklı hostlar üzerinden saldırılacak sunucuya sürekli finger çekiliyorsa bu işlem sonucunda oldukça fazla bant genişliği gitmiş olur. Saldırı birçok farklı noktadan yapıldığından etkisi oldukça büyük olmaktadır. [77] [78]

###### 4.3.5.1.2.5 Ping of Death



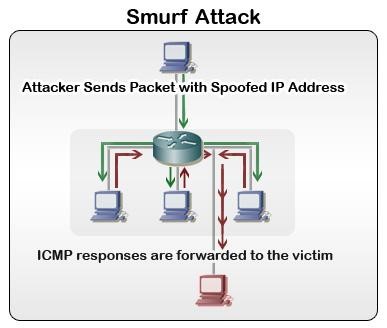
Şekil 4.3.5.1.2.5: Ölüm Pingi

Neredeyse bütün işletim sistemleri bu tür bir saldırıya karşı önlemini aldıysa da zamanında çok etkili bir yöntemdi. Bu yöntemin mantığı şöyle çalışır: ICMP protokolü ağda bilgisayarların hata mesajlarını birbirlerine göndermesini ya da 'Ping' gibi basit işlemlerin yapılmasını sağlar. ICMP spesifikasyonunda, ICMP Echo request'lerin data kısmı 216 ile 65,536 byte arasında olmak zorundadır. Eğer bu veri sınırlarının dışına taşmış bir paket kurban sisteme yollanırsa işletim sistemi böyle bir şey beklemediği için çalışamaz duruma gelecektir. [77] [78]

###### 4.3.5.1.2.6 Smurf

Smurf atakta, hacker kurbanı birçok “çöp” paketi ile tıkar, kurbanın band genişliği kullanılır. Bir smurf atakta, hackerlar sıkça kullanılan bir İnternet servisini sömürürler (*Internet Control Message Protoco*l). Ping, genelde belirli bir bilgisayar ya da serverin

İnternete bağlı çalışır olup olmadığını anlamak için kullanılır. Bir bilgisayar ya da server’a bir ping paketi gönderildiğinde, pingi yollayan kişiye bir cevap paketi yollar, "evet burdayım!" demiş olur (Bir networke yollanıldığında networkteki tüm bilgisayarlar cevap verir). Ping edilen network, saldırı hedefi değildir. Bir smurf atakta, hackerlar ping isteklerindeki geri dönüş adreslerini değiştirirler, böylece bu cevap paketleri kendilerine değil de hedeflenen adrese gider. Bunun iki nedeni vardır: hem hedefe saldırır hem de ping request üzerinde kendi adresi bulunmadığı için yakalanmaktan kendini korur. [77] [78]



Şekil 4.3.5.1.2.6: Smurf Saldırısı

Ping istekleri aralıksız bir şekilde network’ün “*directed broadcast*” adresine yollanır. Bu adres, geriye, networke bağlı her bilgisayara ping isteklerini yollar-ki bu da birkaç yüz belki de daha fazla bilgisayar eder. Yani bir ağdaki tüm bilgisayarlar işleme karışmış olur.

Bu birkaç yüzden fazla bilgisayarın herbiri ping isteğine cevap yollar. Bilgisayarlar, cevap paketlerini, ping isteğinin üzerinde adresi yazan hedefe yollar. Bunlar hackera gönderilmez çünkü o, önceden ping isteğindeki adresi değiştirmiştir.

Hedef yüzbinlerce ping cevap paketini saniyeler içinde alarak tıkanır-basit bir networkten saniye başı 5Mblik data’dan fazlası demektir. Ping paketleri hedefinin tüm bant genişliğini kapladığından, her saniye gelen bu kadar fazla data yüzünden hedef kullanıcıları data alışverişi yapamazlar. E-mail yollayıp alamaz, webde gezemez veya herhangi bir başka Internet servisi kullanamazlar.

Hedefin bu smurf ataklara karşı savunması zordur çünkü ping cevaplama paketleri hackerdan değil, yasal networkten gelir. Hedef, ping cevaplama paketlerinin nereden geldiğini ortaya çıkarmalı, sonra herbir networke bağlanmalı ve onlara ping cevaplama paketlerini kapamalarını söylemelidir. Bunu güçleştiren, hedef sistem kapandığında müşteriler ping isteği yollayıp, onun canlı ve Internete bağlı olup olmadığını öğrenmek ister. Bu nedenle de hedef sistem uygun ping paketlerini, smurf atak paketlerinden ayırabilmekte güçlük çeker. [77] [78]

ISP ler ve Internet routerlara yerleştirmek için smurf koruma özelliği olan yazılımlar kullanılmaktadır. Ancak sadece birkaç şirket bu yazılımı kullanmaktadır. [78]

###### 4.3.5.1.2.7 Fraggle

Fraggle da Smurf ile aynı mantığa sahiptir, sadece tek fark olarak UDP paketlerini 7 ile 19 (Unix sistemlerde) numaralı portlara iletir. [77] [78]

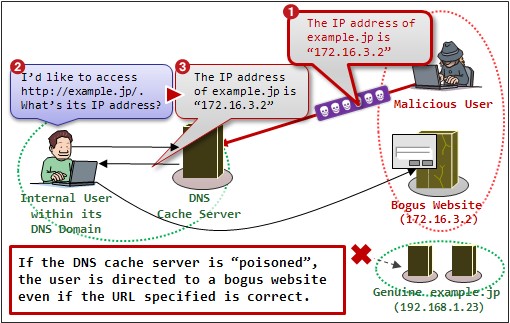
###### 4.3.5.1.2.8 DNS Poisoning

Alan Adı Sunucuları istemciler ve web sunucuları arasındaki haberleşmenin sağlanması amacıyla kullanılan IP adresinin sayısal değerini, insanın okuyabileceği gibi bir alan adına çeviren sunuculardır.

Bir DNS sunucusu, gerçek olmayan bir veriye sahip olduğunda ve bu veriyi performansı en uygun seviyeye getirebilmek için ön belleğe aldığında, DNS sunucusu bir zehirlenme olduğunu dikkate almaktadır.

Normal olarak ağ tabanlı bir bilgisayar bir ISP veya kullanıcının bilgisayarı tarafından sağlanmış bir DNS sunucusu kullanır. DNS sunucuları önceden elde edilen sorgu sonuçlarını önbellekleyerek cevap performansı duyarlılığını artırmak için genellikle bir organizasyonun ağında dağıtılır. Bir DNS sunucusundaki zehirleme atakları, eğer uygulanabilirse, direk gizliliği ihlal etmiş bir sunucudan veya dolaylı olarak onun aşağı sunucusu veya sunucularından sunularak kullanıcılara etki edebilir.

Bir önbellek zehirleme atağını yapabilmek için, saldırgan DNS yazılımındaki bir kusuru istismar eder. Eğer sunucu doğru bir şekilde güvenilir bir kaynaktan geldiğine emin olmak için doğrulama yapmazsa sunucu doğru olmayan girdileri yerel olarak önbelleklemeyi sonlandıracak ve onları diğer kullanıcılara aynı isteği yaparak sunacaktır. [77] [78]



Şekil 4.3.5.1.2.8: DNS Poisoning

Bu teknik kullanıcıları bir siteden saldırganın seçtiği başka bir siteye yönlendirmek için kullanılabilir. Örneğin, bir saldırgan verilen bir DNS sunucusundaki bir hedef websitesi için IP adresi DNS girdilerini onun kontrolündeki sunucunun IP adresiyle değiştirerek zehirler. Sonra hedef sunucusundaki isimlerle eşleşen onun kontrolündeki sunucuda dosyalar oluşturur. Bu dosyalar bilgisayar solucanı veya virüs gibi zararlı içerikler içerebilir. Zehirlenmiş DNS sunucusuna referans edilmiş bilgisayara sahip bir kullanıcı güvenilir olmayan bir sunucudan gelen içeriği kabul ederek kandırılmış olacak ve farkında olmadan zararlı içeriği indirmiş olacaktır. DNS sunucuya, yanlış DNS bilgileri tanıtılarak, istekler değiştirilmiş olan DNS sunucuya iletilir. [78]

###### 4.3.5.1.2.9 Buffer Overflows

Bilgisayarlarda bulunan bufferlar, belli bir kapasiteye sahiptir. Kapasitenin aşıldığı durumlarda kitlenme, reset atma gibi durumlar oluşabilmektedir. Hafıza taşması saldırı tipinde de çok fazla veri gönderilerek trafik yoğunlaşır ve iletişim engellenir. Bu sebeple, saldırganlar büyük boyutta ping göndermeyi tercih etmektedirler. [78]

###### 4.3.5.1.2.10 HTTP Fragmentation

Bu saldırıda, server ile BOT arasında geçerli bir HTTP bağlantısı kurulur. Sistem alarm vermeden açılan oturum süresi uzun tutulabilmektedir. Birçok server tasarlanan uygunsuz time-out mekanizması için, HTTP oturum zamanı, periyodik olarak uzatılabilir. Saldırgan, açılan periyodik uzatılmış oturumlar tarafından web serveri bir miktar Bot'lar ile durdurabilir. [78]

###### 4.3.5.1.2.11 Excessive VERB

Atak yapan BOT kurban web server'a geçerli HTTP isteğinde bulunur. Bu istekler web sayfa veya resim gibi büyük boyutlu yanıt GET veya POST istek türleridir. Her bir bot saniyede 10'dan fazla istek oluşturabilir. Burada server'in band genişliği fazla artmaz. Fakat kurban kaynakları tüketilerek yanıt veremez duruma gelmektedir. [77] [78]

**Recursive GET:** Bir VERB atak türüdür. Saldırgan birkaç sayfa veya resim toplar ve GET isteği üretir. Bunu belirlemesi zordur çünkü yasal bir istek oluşturulmuştur.

**Radom Recursive GET:** Bu atak Recursive GET'nin modifiye edilmiş halidir. Daha çok indeksli olan forum ve haber sitelerinde kullanılır. GET isteklerine rastgele geçerli olabilecek sayfa dizin numaraları eklenir. İstenilen her biri bir öncekinden farklıdır. [77] [78]

###### 4.3.5.1.2.12 Faulty Application

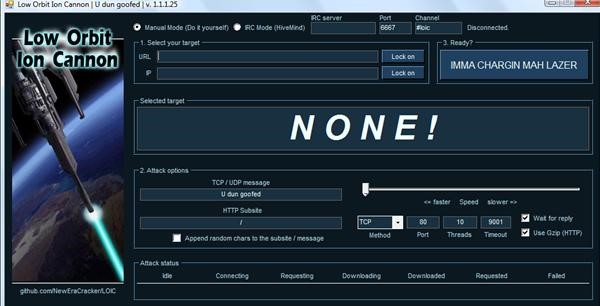
Saldırgan uygulamanın zayıf dizaynından veya database ile zayıf etkilişimden kaynaklanan kusuru kullanabilir. SQL injection gibi atak'lar üreterek server’in kaynaklarını sömürebilir (hafıza, CPU, vb.). [77] [78]

###### 4.3.5.1.2.13 Media Data Flood

VoIP ek olarak, UDP flood birkaç media paketi aldığında oluşur. Atak sırasında, kurban server media veri paket basınlarını yüksek bir veri ve çok uzun bir IP dizisiyle kaydeder. Sistem bunu karşılayamaz ve istila edilmiş olur. Network kaynakları sömürülür ve kapanır. VoIP gibi Media Data flood networku rastgele paketler ve iyileştirilmiş IP adresleri ile baskı uygular. Böylece network bant genişliği tüketilir. [77] **[**78]

DDos Savunma Yöntemleri

Anonymous tarafından daha önceleri çeşitli nedenlerden Scientology’e, Wikileaks sitesine gelen mali yardımların kesilmesini sağlayan PAYPAL ve Mastercard’a ve Türkiye’deki BTK, TİB gibi birçok kuruma karşı DDoS atağı gerçekleştirmiş ve Anonymous üyelerinin de bu saldırılarda rol alabilmesi için **LOIC** adlı yazılımı geliştirmişlerdi. Bu yazılıım ağ stres testi aracı olarak kullanılabilmektedir. Fakat Anonymous bu aracı DDoS saldırıları gerçekleştirmek için kullanmaktadır. Low Orbit Ion Cannon yazılımını indiren Anonymous üyeleri belirlenen hedef adreslere DDoS saldırısı yapabilmektediler. Bu saldırılar LOIC ile **HTTP GET, TCP** ve **UDP flood** şeklinde gerçekleştiriliyor. [78] [77]



Şekil 4.3.5.1.2.13: Anonymous LOIC Saldırı Yazılımı Arayüzü

Anonymous grubu LOIC aracı ile yapılan saldırıların etkisin arttırmak ve daha fazla gönüllü üye ile saldırıyı gerçekleştirmek için bu aracı web üzerinden çalıştırabilecek hale getirdi. **Drive-by-download**\* saldırıları gibi herhangi bir web sitesine enjekte edilmiş bir kod ile ya da kullanıcıya içerisinde bu zararlı kodun olduğu bir siteye girdirmek sureti ile saldırı otomatik olarak başlayacak şekilde tasarlanmıştır. Kullanıcı herhangi bir siteden içerisinde LOIC javascript versiyonu enjekte edilmiş bir sitenin linkine tıkladığı andan itibaren DDoS saldırıları devam edecektir. [78]

Siteye giren kullanıcılar üst tarafta bulunan twitleri ya da yazılan mesajları okumaya başladığı andan itibaren alt tarafta bulunan JavaScript kod parçası belirlenen adreslere anlık olarak bağlantı kurmaya başlatmaktadır. Yapılan bu GET istekleri hedef olarak seçilen web sunucuyu cevap veremeyecek duruma sokmaktadır. Son kullanıcı hedef olarak belirtilen siteye girmeden herhangi bir etkileşime girmeden JS kodunda hedef olarak belirlenen sisteme DDoS atağı gerçekleşmektedir. Sitede o an kaç aktif kullanıcı var ise saldırının boyutu da lineer olarak artmaktadır. [78]

Kullanıcı eğer farkında olmadan bu saldırıya katılmış ise genellikle **msg** alanında herhangi bir değişiklik yapmayacaktır. Ama gönüllü olarak bu saldırıyı gerçekleştiriyor ise **msg** alanının değiştirip gönderebilir. Böyle bir durumda snort imzasını gelen ataklara göre güncellemek gerekir. Fakat bu değişiklik de atağı durdurmak için yeterli olamayabilir. Böyle bir durumda daha ayrıntılı ağ trafiği analizi ile IDS imzaları güncellenebilir. Hedef alınan servislere gelen istekler kısıtlanabilir. Örneğin belirli bir IP adresinden dakikada yapılacak HTTP GET isteklerini sınırlama gibi. [78]

Ayrıca son kullanıcıların bu saldırılara dahil olmalarını engellemek için internet tarayıcılarına [NoScript b](http://noscript.net/)enzeri tarayıcı eklentileri ile saldırıya istemsiz olarak katılımı engellenebilir. İstemci tarafında çalışacak güvenlik yazılımları ile kullanıcının erişim yapacağı sitelere olan istekler limitlenebilir. [78]

Giderek daha karmaşıklaşan bu tür ataklara karşı hem kullanıcıların istemsiz olarak saldırıya katılımını engellemek, hem de kendi sunucularımızı bu tür saldırılardan korumak zorlaşmaktadır. Mümkün olduğu kadar ağ trafiği analiz edilmeli ve bu atağa uygun Güvenlik Duvarı kuralları ve Saldırı Tespit/Engelleme Sistemleri imzaları güncellenmelidir. Son kullanıcılar bu tür ataklara karşı bilgilendirilmelidir. [78]

DOS/DDOS saldırıları internet dünyasının başlangıcından beri önemi gitgide atan bir tehdittir. Güvenlik açıklıkları kapatılsa da TCP/IP Protokolünün yapısı değişmeden bu soruna kesin bir çözüm bulunamayacaktır. [78]

HTTP-GET DDoS Atak Engelleme

1. Apache Web Sunucu
2. Alan ismi: www.xx.com

Yukarıda belirtildiği gibi üzerinde Apache Web Sunucusu çalışan bir sunucumuz bulunmakta. Web sunucumuz üzerinde çalışmakta olan www.xx.com adresine saniyede binlerce IP adresinden HTTP-GET isteği yapılmaktadır. [78]

Bu durumda Apache belli bir süre sonra bu isteklere yanıt verememeye başlayacaktır. Eğer istekte bulunulan sayfanın bağlandığı bir veritabanı sunucumuz mevcut ise, bu istek veritabanımızın da yanıt verememesine sebep olacaktır. [78] [77]

Öncelikle şunu bilmeliyiz ki; her bir HTTP-GET isteği için ayrı bir bağlantı oluşturulmasına gerek yoktur. Çünkü HTTP/1.1, açılan bir bağlantı içerisinden dilediğimiz kadar istek göndermemize izin verir. Bu bilindiği gibi **Request Pipelining** olarak adlandırılmaktadır. Bu da demek oluyor ki güvenlik duvarımızda (donanımsal ya da yazılımsal) TCP 80 portuna gelen sadece bir HTTP-GET isteği görebiliriz ama aslında bu istek içerisinden binlerce istek alıyor olabiliriz.

* Bir HTTP-GET atağında öncelikle yapmamız gereken şey web sunucumuzun loglarını incelemek olacaktır. Çünkü bu loglar içerisinde bizim IDP (Intrusion Detection & Prevention) sistemimiz üzerinden engelleyebileceğimiz sabit bir data bulabiliriz. Mesela sabit bir HTTP başlığı, referrer veya user-agent tespit edip IDP sistemimiz üzerinden engelleyebiliriz.
* Eğer gelen istekler değişik çerezler ile geliyorsa ve bu alanda yapabileceğimiz ekstra bir şey yoksa ikinci bir önlem olarak, bir dakika içerisindeki web server loglarına bakarak en çok isteği yapan IP adreslerini daha sistemimize ulaşmadan engelleyebiliriz. Ama örneğimizde olduğu gibi farklı kaynaklardan gelen istekleri bu şekilde engellememiz fazla mümkün olamayacaktır. Çünkü karşı karşıya olduğumuz atak türünde saldırılar binlerce farklı IP adresinden gelmekte ve bu IP adresleri sürekli değişmektedir.
* Bir sonraki aşama olarak IDP’ miz ya da güvenlik duvarımız üzerinde **TCP Connection Limit** koyarak ve threshold düşürerek saniyede gelen bu aşırı HTTP-GET isteklerini daha web sunucumuza ulaşmadan engelleyebiliriz. Bu genellikle etkili olan ve saldırganın başarısını azaltan bir engelleme mekanizmasıdır. Ama bu durumda gelen istek HTTP-GET isteği olduğu için güvenlik duvarımız ya da IDP'miz hangi isteğin doğru hangi isteğin yanlış olduğunu anlayamayacak ve bu durumda siteye normal olarak ulaşmak isteyen kişilerin isteklerinin de engellenme ihtimali söz konusu olacaktır. Ayrıca bu işlemde bile eğer atak çok büyük ise güvenlik sistemimizden kaçan istekler arka taraftaki web sunucumuza ulaşacak ve sitemizin sağlıklı çalışmasına engel olacaktır.

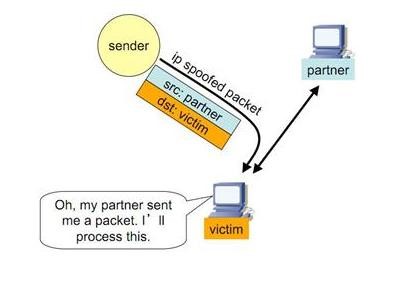
**TCP connection limit** işleminin yanı sıra Apache sunucumuz üzerine bir Reverse Proxy kurup, sayfaların ön belleklenmesini sağlayarak gelen bu isteklerin sunucu tarafında herhangi bir TCP bağlantı açmadan alınmasını sağlayabiliriz. **Nginx** bu amaçla kullanılabilecek faydalı bir yazılımdır.

Bu işlemlerin sonucunda connection limit (IDP ya da güvenlik duvarı) ile saniyede belirttiğimiz limitin üzerinde gelen istekler engellenecek ve ters vekil sunucumuzun sayesinde gelen istekler daha Apache’ye ulaşmadan ön bellek üzerinden verilecektir. Ters vekil sunucumuzu kurduktan sonra IDP veya güvenlik duvarımız üzerinde yaptığımız bağlantı limiti eşik değerini yukarılara çekerek testlerimizi yapabiliriz. Bu testlerin sonucunda saldırı amaçlı bağlantılar ile sitemize normal yollardan ulaşmak isteyen kullanıcılar arasında bir denge kurulacak ve hatalı engellemelerin önü alınacaktır. [77] [78]

##### 4.3.5.1.3 IP Spoofing

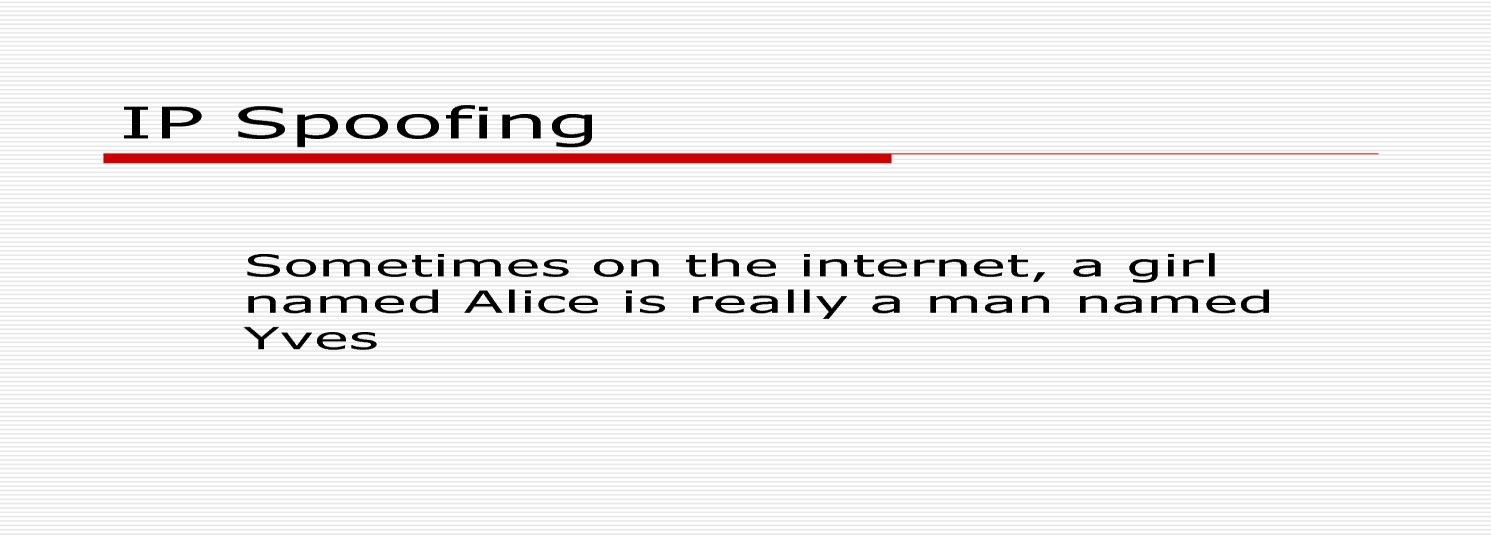
Bilgisayarlar arasındaki bağlantı çeşitli protokoller aracılığıyla sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kendi kimliğini karşı tarafa tanıtır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine **IP spoofing** denir. Sahte IP paketi alan bilgisayar, paketin gerçekten gönderilen adresten gelip gelmediğini bilemez. Bu genellikle başkasının IP adresinden mail gönderilmesi veya forumlara mesaj yazılması olarak karşımıza çıkmaktadır. Teoride bu durum mümkün olmakla birlikte pratikte karşıdaki sistem gerçekten ele geçirilmeden başkasının bilgisayarına farklı bir IP’den bağlanma gerçekleşemeyecektir. Günümüzde IP spoofing için kullanılan ticari ve ücretsiz yazılımlar bulunmaktadır. [78]

Aldatma genel olarak bir web sitesini işlemez hale getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır.



Şekil 4.3.5.1.3: IP Aldatması

Aldatma genel olarak bir web sit esini işlemez hale getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır. [78]



Şekil 4.3.5.1.3.a: IP Aldatması 2

###### Genel Anlamda (Spoofing’den) Korunma Yöntemleri

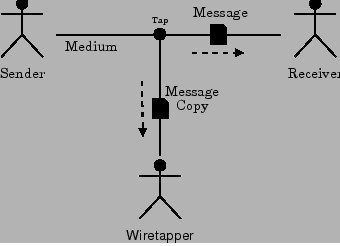
IP Spoofing olayını engelleyebilmek için öncelikli olarak Yönlendiricilerde, Kaynak Yönlendirme fonksiyonunu pasife alınmalıdır. Çünkü kaynak yönlendirme çok kısıtlı ve pek nadir kullanılır. Bu nedenle ağa giren ve çıkan bu trafik engellenmelidir. [78] [79]

Sisteminizde filtre uygulanmalı ve yetkiler kısıtlanmalıdır. Şöyle ki; sistemde IP adreslerini değiştirme hakkı kaldırılmalıdır. Dolayısıyla (IP) Spoofing’in önüne geçilebilir.

Bunlara ek olarak birtakım yazılımları kullanabilirsiniz. Bu yazılımlar Spoofing yapılırken uygulanan metotlara rastladığı zaman size haber verir. [78] [79]

##### 4.3.5.1.4 Kabloya saplama yapma

Kabloya saplama yapma, özellikle emniyeti alınmamış iletişim ağı kablolarına özel teçhizat kullanarak fiziksel olarak saplama yapılması ve bağlantı kurulmasıdır.



Şekil 4.3.5.1.4: Kabloya Saplama

Kabloya saplama yapıldığında, iki taraf arasındaki tüm trafiğin ele geçirilmesi mümkündür. [78] [77]

##### 4.3.5.1.5 Kriptografik Saldırılar

###### 4.3.5.1.5.1 Kriptanaliz ve Kriptosistemlere Saldırılar:

Kriptanaliz; uygun anahtarların bilinmeden şifrelenmiş iletişimlerin çözülmesi sanatıdır. En önemli kriptanaliz tekniklerinden bazıları aşağıda verilmiştir: [82]

###### 4.3.5.1.5.2 Cipher-Text Only Saldırısı

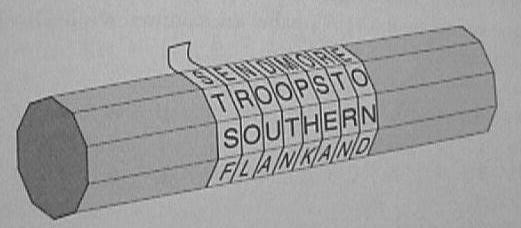
Bu saldırı tipinde, saldırıyı yapan kişi mesajın içeriği hakkında hiçbir şey bilmemektedir ve sadece şifreli-metni kullanarak çalışmalıdır. Uygulamada Plain text pek çok mesaj türü sabit başlık formatlarına olduğundan- ilişkin tahminler yapmak genelde olasıdır. Sıradan mektuplar ve belgeler bile kestirilebilir bir şekilde başlamaktadır. Örneğin, pek çok klasik saldırıda ciphertext’in frekans analizi kullanılmaktadır, ancak modern cipherlara karşı bu yöntem iyi çalışmamaktadır. Buna rağmen mesajlar bazen istatistiksel bir yanlılık içermektedirler. [82]

###### 4.3.5.1.5.3 Known-PlainText Attack

Saldırgan ciphertext’in bazı kısımlarından düz metni tahmin edebilir veya bölebilir. Geriye kalan iş bu bilgiyi kullanarak ciphertext bloklarını çözmektir. Bu işlem, veriyi şifrelemek için kullanılan anahtarın belirlenmesi ile yapılabilir. En sık kullanılan Known-PlainText Attack, blok cipher’lara karşı lineer kriptanaliz saldırısıdır. [82]

###### 4.3.5.1.5.4 Selected Plaintext Attack

Saldırgan bilinmeyen anahtar ile şifrelenmiş istediği her metni elde edebilmektedir. Buradaki iş, şifreleme için kullanılan anahtarı belirlemektir. Bu saldırı için iyi bir örnek blok cipherlara karşı uygulanabilen diferansiyel kriptanalizdir. Bazı kripto sistemler, özellikle RSA, seçilmiş-düz metin saldırılarına karşı açıktır. Bu tip algoritmalar kullanıldığında, uygulama (veya protokol) öyle tasarlanmalıdır ki saldırgan istediği düz metni şifrelenmiş olarak elde etmemelidir. [82]



Şekil 4.3.5.1.5.4: Selected Plaintext Attack Görseli

###### 4.3.5.1.5.5 Man in the Middle Attack:

Bu saldırı, kriptografik iletişim ve anahtar değişimi protokolleri ile ilgilidir. Fikir şudur; iki kişi güvenli iletişim için anahtarlarını değiş-tokuş ederken (örneğin Diffiehellman kullanarak), bir düşman kendisini iletişim hattındaki iki kişi arasına yerleştirir. Sonra bu düşman her iki kişi ile ayrı bir anahtar değiş-tokuşu gerçekleştirir. Her iki kişi farklı bir anahtar kullanarak işlerini tamamlayacaklardır ki bu anahtarlar düşman tarafından bilinmektedirler. Bu noktadan sonra saldırgan uygun anahtar ile herhangi bir iletişimi deşifre edebilecek ve bunları diğer kişiye iletmek için diğer anahtar ile şifreleyecektir. Her iki tarafta güvenli bir şekilde konuştuklarını sanacaklardır, ancak gerçekte saldırgan konuşulan her şeyi duymaktadır.



Şekil 4.3.5.1.5.5: Man in the Middle Attack

Ortadaki-adam-saldırısını engellemenin bir yolu dijital imzaları kullanabilen bir açık anahtar kripto sistemi kullanmaktır. Kurulum için her iki tarafta karşı tarafın açık anahtarını bilmelidir (ki bu bazen açık anahtar kripto sisteminin esas avantajını baltalamaktadır). Paylaşılan gizlilik oluşturulduktan sonra, taraflar kendi dijital imzalarını karşı tarafa göndermelidir. Ortadaki-Adam bu imzaları taklit etmeye çalışacak, fakat imzaların sahtesini yapamayacağı için başarısız olacaktır.

Bu çözüm, açık anahtarların güvenli bir biçimde dağıtımı için bir yolun varlığı halinde yeterlidir. Bu, örneğin, IPSec (Internet Protocol Security) 'de kullanılmaktadır. [79] [82]

###### 4.3.5.1.5.6 IPSec tanımı

İnternet Protocol Security (IPSec) güvenli haberleşmeler sağlamak ve IP ağları üzerinde kişisel gizliliği korumak için standartlar üzerine kurulmuş bir yapıdır. IPSec RFC (Requests for Comments) 2401-2411 de tanımlanmış olan bir IETF (Internet Engineering Task Force) standartıdır. Çoğu ağların güvensiz olduğu ve kablo üzerinde seyahat ederken verileri korumak için ek komponentler gerektirdiği düşüncesinden yola çıkarak IPSec kaynak kimlik tanılama, bütünlük kontrolü ve içerik gizliliği sağlamaktadır. [83]

##### 4.3.5.1.6 Sosyal Mühendislik



Şekil 4.3.5.1.6: Sosyal Mühendislik

Sosyal Mühendislik; temel olarak bilgisayar ya da bilgisayar ağlarındaki açıklıklardan faydalanarak bilgisayar sistemlerine zarar veren yaklaşımların aksine “sosyal mühendislik” yöntemi insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir. [79] [82]

##### 4.3.5.1.7 SQL Injection

SQL Injection veri tabanından yapılan sorgulama işlemini hedef alan bir saldırı şeklidir. Bu saldırı şeklinde sorgulama dili yapısı kullanılarak saldırı gerçekleştirilir. Bir web uygulamasının kullanıcı adı ve şifre ikilisi veri tabanına “SELECT \* FROM TABLE\_PERSONEL WHERE username = '" + kullanıcı adı + "' AND password= '" +şifre+ "‘” şeklinde gönderildiğinde (“”) işaretleri içindeki veri bir filtrelemeye tabi tutulmazsa kullanıcının buraya yazacağı (OR ''1=) eklinde bir ifade sorguyu “SELECT \* FROM TABLE\_PERSONEL WHERE username = '' OR ''1=1'' AND Password = '' OR ''1=1'‘” haline getirir. Bu durumda sorgudan var olan bütün kayıtlar dönecektir. [84]

##### 4.3.5.1.8 Command Injection

Genellikle shell enjeksiyon saldırılar SQL Injection ve XSS saldırılarının aksine doğrudan sunucuları hedefleyen bir saldırı tipidir. Web uygulamasının komut satırını kullanarak uzaktan erişimle işletim sistemi, veri tabanı yönetim sistemi ve sunucudaki bilgilere erişimi hedefler. [85]

##### 4.3.5.1.9 HTML Injection

Bu açık, programcıların kodlama sırasında yaptığı hatalı kodlamadan faydalanır. Web yazılımlarında veri tabanına giren verilerin ya da veri tabanından çekilen verilerin bir kontrol mekanizmasından geçirilmemesi açığa neden olmaktadır. XSS olarak da bilinen açıktan faydalanılarak session ve cookie çalması yapılır.

Uygulamalarda sayfaya gönderilen bir isteğe bir cevap döndürülmesi mantığı kullanılır. Sayfaya gönderilen istek sunucuda değerlendirilip bir cevap döndürülür. Ama eğer giriş yaptığınız sayfa kötü amaçlı bir url adresine yönlendirildiyse ya da Truva atı gibi araçlar yerleştirildiyse aldığınız yanıt beklenenden farklı olacaktır. Bu saldırı tipinde amaç web uygulamasına zarar vermek değil daha çok uygulamayın ziyaret eden kullanıcılara erişmektir. [86]

##### 4.3.5.1.10 Backdoors

Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde normal kimlik kanıtlama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler arka kapı olarak adlandırılmaktadır. Bir sisteme sızmak için oldukça zahmetli bir çaba harcayan korsanlar daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklemek isterler. En sık karşılaşılan arka kapı yöntemi hedef sistemde dinleme ajanı iliştirilmiş bir portu açık tutmaktır.

Bu açıdan bakıldığında bu tür bir açığa maruz kalındığından emin olmak için sistemde mevcut bulunan bütün portlar 1’den 65535’e kadar iki kere (bir kez TCP bir kez de UDP için) taranmalıdır. Arka kapılar çoğunlukla Truva atları ile karıştırılabilmektedirler. Her ikisi de hedef sisteme sızmaya yarayan kötü amaçlı yazılımlardan; Truva atı faydalı bir program gibi gözükürken; arka kapı sadece sisteme erişimi sağlayan gizli yapılardır. [87]

Birçok virüs bir bilgisayara bulaştığında mutlaka bir arka kapı açmayı denemektedir. Bu arka kapılar da virüs yayıncısı için çok kolay bir erişim imkânı sağlamaktadır.

Arka kapılar kimi zaman sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına varan kötü niyetli kişiler bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir.

Arka kapı konusunda en ünlü iddialardan biri de Microsoft’un Windows işletim sisteminin bütün sürümlerinde NSA (Amerikan National Security Agency) için bir arka kapı yerleştirdiği iddiasıdır. Bu iddia Microsoft’un bütün sürümlerinde bulunan CryptoAPI yapısında \_NSAKey adına ilave bir giriş anahtarın bulunmasıdır. [88]

##### 4.3.5.1.11 Phishing

Phishing kısaca online dolandırıcılık olarak tanımlanabilir. Phishing yönteminde temel amaç internet kullanıcısını kandırarak kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaralarından, bu hesaba ait online internet şifresine kadar birçok özel bilgileri ele geçirmektir.

###### 4.3.5.1.11.1 Neler Çalınıyor?

Phishing yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilen bilgileri çalıyorlar:

1. Kredi Debit/ATM Kart Numaraları/CVV2
2. Şifreler ve Parolalar
3. Hesap Numaraları
4. İnternet Bankacılığına Girişte Kullanılan Kullanıcı Kodu ve Şifreleri

###### 4.3.5.1.11.2 Bu dolandırıcılık işlemi nasıl gerçekleştirilmektedir?

Kullanılan yöntemlerin başında e-posta ile gönderilen sahte mesajlar gelmektedir. Bu e-posta bir ticari kurumdan (bankalar, alışveriş siteleri vb.) geliyormuş gibi bir izlenim yaratır. Bu kullanıcının kendisine ait bilgileri girmesi için kurumun internet adresine ilişkin bağlantıya tıklamasını içeren bir e-posta olabilir. E-posta içeriği kişisel bilgilerin güncellenmesi sistemdeki yeniliklerin hesabınızda aktif olması için şifrenizi girin gibi mesajlardır. Bunu gören kullanıcı e-posta ile gelen mesajdaki bağlantıya tıkladığında kurumun web sitesinin birebir kopyası olan başka bir sayfaya yönlendirilir. Burada girilen şifre gibi özel bilgiler artık başkasının eline geçer. [89]

E-posta kullanım oranının çok yüksek olması bu tür online dolandırıcılık işlemlerinin e-posta yoluyla gerçekleşmesinde temel etmenlerden biridir. E-posta içeriğinde belirtilen bağlantı (genellikle ticari kurumların web sitelerine yönelik sahte gösterim) kullanıcıların aldanmasında büyük rol oynar. İnternet kullanıcısı üyesi olduğu ticari bir kurum sitesine yönlendirildiğini sanıp kendisine belirtilen yönergeleri uygular. Phishing ataklarındaki önemli artış browser uygulamalarının (İnternet Explorer, Mozilla Firefox, Opera vb.) güvenlik sorunlarını da ön plana çıkarmıştır.

Örnek olarak [http://www.turkiyebankalarkurulu.com](http://www.turkiyebankalarkurulu.com/) adlı bir internet sayfası oluşturulmuştur. Ancak Türkiye Bankalar Birliği’nin resmi internet sitesi olan [www.tbb.org.tr](http://www.tbb.org.tr/) adresinden bunun bir internet üzerinden phishing türü dolandırıcılık yapma girişimi olduğu duyurusu yayınlanmıştır. Daha sonra bahse konu site yayından kaldırılmıştır. Bu gibi dolandırıcılık olaylarının engellenebilmesi maksadıyla internet bankacılığında kullanılması gerekli olan kullanıcı adı ve şifre bilgilerine ek olarak 2011 yılında BDDK tarafından zorunlu hale getirilen ve 2010 yılından itibaren uygulanmasına başlanan IBAN numarası ve GSM şebekeleri üzerinden tek kullanımlık şifre düzenlemeleri hayata geçirilmiştir.

Bu dolandırıcılık faaliyetlerine karşı; bankalardan geldiği düşünülen e-postaların içerisindeki linklere tıklanarak bankacılık işlemi yapılmamalıdır. İnternet bankacılığı işlemlerinde banka tarafından sunulan fare ile veri girişi, tuşlar üzerinde bekleyerek veri girişi, değişen karmaşık tuş takımı ve tek kullanımlık SMS ile şifre gönderilmesi gibi çözümleri kullanmak güvenlik açısından önemlidir.

Bu dolandırıcılık tipi sadece bankacılık sitelerinde değil arkadaşlık sitelerinde, sohbet sitelerinde, alışveriş sitelerinde, havayolu sitelerinde ve birçok sitede ortaya çıkabilmektedir. ATM cihazları kullanılırken şüpheci ve dikkatli olunmalıdır. ATM makineleri üzerine mikro kamera kart okuyucu ve PinPad düzenekler yerleştirilmesi ile karşılaşılmaktadır.

###### 4.3.5.1.11.3 Phishingten Nasıl Korunulur?

Unutulmaması gereken nokta her türlü online dolandırıcılık, sahtekarlık ve virüslere karşı en büyük korunma aracı bu konuda bilinçli ve bilgili olmaktır.

1. E-postaya gelen mesajların doğruluğunun ispatlanması. Tanımadığımız kimselerden gelen mesajları silinmesi gerekmektedir. "Aşağıdaki bağlantıya tıklayın" gibi e-posta isteklerine asla yanıt verilmemesi gerekiyor.
2. İşlemleri online yaparken işlem yapılan web sayfasının güvenli olup olmadığını mutlaka kontrol edilmesi lazım. İnternet tarayıcısının üst kısmında bulunan adres bölümünde bulunan adresin "https://" olup olmadığı kontrol edilmelidir. “https://”’in sonunda bulunan “s” harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptırdığını belirtir.
3. İnternet adresi olarak sayısal rakamlar içeren adresler ile karşılaşıldığında kullanmadan önce mutlaka kontrol edilmeli. Ziyaret edilen web sitelerinde; adresler çoğunlukla adres kısmı ardından firmanın ve şirketin ismine ek olarak com, org, net gibi uzantılar ile biter. Sahte sitelerde çoğu zaman sayısal adresler kullanılmaktadır.
4. E-posta adresine ulaşan e-posta’nın kimden geldiğinden ve doğruluğundan mutlaka emin olunmalıdır.
5. Bankadan gelen kart ekstreleri ve banka hesapları düzenli olarak kontrol edilmelidir.
6. Olası aksiliklerde banka ile kesinlikle irtibata geçilmeli ve zaman kaybedilmemelidir.
7. Sistemin düzenli olarak kontrol edilmesi gerekmektedir. İşletim sisteminin güvenlik yamalarının yüklenmesi, anti-virüs yazılımı varsa devamlı olarak güncellenmelidir.
8. Çeşitli kurumlardaki hesaplar veya birden fazla e-posta adresi kullanılıyorsa kesinlikle her biri için farklı şifreler belirlenmelidir.
9. Belirlenen şifreleri belli aralıklar ile muhakkak değiştirmelidir. [90] [91]

##### 4.3.5.1.12 Rootkits

Çalışan süreçleri dosyaları veya [sistem](http://tr.wikipedia.org/wiki/Sistem) bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur. Amacı yayılmak değil bulunduğu sistemde varlığını gizlemektir. Önceleri çok kullanıcılı sistemlerde sıradan kullanıcıların yönetim programlarına ve sistem bilgilerine erişimini gizlemek için geliştirilmiş ve kullanılmış olmasına rağmen kötü niyetli kullanımına da rastlamak mümkündür.

Tipine bağlı olmakla birlikte genelde erişim yetkiniz dâhilinde sisteminize kurabileceğiniz rootkit'ler bulmanız mümkündür. Bunun dışında güvenilir bir kaynaktan geldiğine inandığınız bir programı haddinden fazla yetki ile çalıştırmak (Örn: root) zararlı bir rootkit'in sisteme kurulmasına sebep olur. Aynı şekilde çok kullanıcılı bir sistemde kernel vs. açıkları kullanılarak sistemde root yetkisi kazanıp rootkit kurulması en yaygın görülen bulaşma şeklidir.

Adından da anlaşılabileceği gibi Rootkit iki parçadan oluşmaktadır; Root= Unix sistemlerinde her şeyi yapma yetkisine sahip olan kullanıcı ya da kullanıcı yetkisi Kit = Bu yetki sahibi olabilmek için kullanılan gerekli araç kutusu şeklinde ifade edilebilir.

Bunu yaparken sistem araçları ile yer değiştirmiş olmaları tanınmalarını engellemekte ve arka planda hiçbir kullanıcının ya da tarayıcının fark edemeyeceği biçimde çalışmalarını sağlamaktadır. Bu özellikleri zararlı yazılımları yazan programcılar (hacker) tarafından çok cazip bulunmakta ve ilk başlarda kötü amaçlarla kullanılmayan bu yazılımlardan yanlış kimselerin elinde çok tehlikeli olabilecekleri için günümüzde kötü niyetli yazılımlar olarak bahsedilmektedir. [92]

##### 4.3.5.1.13 Spyware

Bu programlar kullanımı masum görünen ve genelde internetten “bedava” diye reklamını görüp indirilen programlar ile bilgisayarlara bulaşan programcıklardır. Çoğunlukla dikkat edilmeyen EULA (End-User License Agreement) içerisinde (programla birlikte kurulacağı belirtilir ve “I Agree” kabul edildiğinde her şeyi kabul edilmiş olunuyor) bulunur. Tam anlamı ile virüs olarak adlandırılamayan bu programların temel amaçları kuruldukları bilgisayarda bilgi toplamak ve bu bilgileri bu programları yaratan kişilere göndermektir. Bu spyware/casus programların bilgisayar sistemlerine tehlikesi casusluk derecelerine göre değişir.

Casusluk yaptıkları konular nispeten masum olarak adlandırılabilecek olan “hangi siteye gidiyor, ne kadar orada kalıyor” gibi bilgilerden daha ciddi olan bilgisayarın veya sistemin kurulum şifreleri veya kullanılan kredi kartı bilgilerini edinerek bunları program yazıcılarına postalamaya kadar varabilen her türlü casusluk örneklerini kapsayabilirler. Sörf bilgilerini genelde google toolbar, alexa toolbar veya diğer benzeri toolbar ismiyle dağıtılan internet explorer eklentileri biriktirirler. Bu şekilde hangi sitelerin ziyaret edildiğini ölçerek ziyaret edilen sitelere puan veya benzeri değerlendirmeler verirler. Sonra bu verileri arama sitelerinde sonuçları sıralamak için kullanabilirler. Aynı şekilde GetRight, Gator ve benzeri internetten dosya indirmeye yarayan programlar da bu tür spyware içerirler. Ancak bunu kendileri tabiî ki kabul etmezler çünkü bu programları kurarken kabul ettiğiniz kullanım kurallarına göre bu veri aktarımını kabul ettiğinizi bildirdiğiniz için bunun casusluk olmadığını gönüllü veri paylaşımı olduğunu belirtirler.

Spyware veya casus programların daha tehlikeli olan türevleri ise bilgisayar veya internet ayarlarınızı kendi istedikleri gibi değiştirirler ve kendi istedikleri sitelere yönlendirirler bazıları bununla da yetinmeyip internet başlangıç sayfasını kendi istedikleri gibi değiştirirler hatta bazen bilgisayarda karşınıza nereden geldiğini bilmediğiniz ve anlayamadığınız reklam içerikli pencereler çıkarırlar. Bunlara Adware’de denir çünkü her ne kadar bir önceki casus programlar gibi casusluk yapıyor olsalar da bunun yanında ayrıca bir de bilgisayarınızda reklama yönelik oynamalar yapmaktadırlar.

Tabi bunlardan daha da tehlikeli olanları da vardır. Mesela bu türün en tehlikelileri olarak nitelendirilmesi mümkün olan Dialer programları bunlardandır. Telefon hattı üzerinden internete bağlananlar için bu dialer programlar bilgisayarın internet bağlantı ayarlarını değiştirerek ödemeli bir telefon hattına yönlendiren programlardır. Bu dialer programlar bulaştığı esnada her zamanki gibi internete bağlanırken telefon faturası gelince şoke olursunuz çünkü faturanız birden belki de 10 katı ile artmıştır. Bunun nedeni bu bilgisayara bulaşan dialer programlar internete bağlandığınız numarayı biraz önce belirttiğimiz gibi ücretli bir yurtdışı hattı veya 900 lü bir hat ile değiştirip sizi her internete girişinizde bu ücretli hatlar aracılığı ile internete bağlamıştır. [78]

##### 4.3.5.1.14 Viruses

Virüs, bilgisayar dünyasında on yıllardır karşılaşılan bir terimdir. Bu terim genellikle zararlı yazılımları ifade eden kapsayıcı genel bir ifade olarak kullanılmıştır, ancak bu kullanım yanlıştır. Her tür zararlı yazılım virüs olarak ifade edilemez. Virüs diğer dosyalara bulaşarak yayılan özel bir zararlı yazılım türünü ifade etmektedir.

Kayıtlara geçen ilk virüs 1986 yılında ortaya çıkan IBM-PC tabanlı “*Brain*” ismi verilen bir *boot sector* virüsüdür. [80]

Bilgisayarlara zarar vermek üzere hazırlanmış programlardır. E-postalar ve dosyalar ile bilgisayarlara bulaşan virüsler bilgisayarların çalışmasını engelleyebilmekte bilgilerin kaybolmasına, bozulmasına veya silinmesine neden olabilmektedir. Ayrıca bilgisayarları yavaşlatabilmektedirler. Bunlar bilgisayar belleğine yerleşen, çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen programlardır.

Virüslerin sistemleri yıkıcı etkileri bulunmaktadır. Virüsler bir dosyanın açılması, bir epostanın okunması veya virüs bulaşmış bir programın çalıştırılması gibi yöntemlerle yayılmaktadır.

Bir sistemdeki olası virüs belirtileri şunlardır:

* İnternette bir işlem ya da faaliyet yapılmayan zamanlarda veri trafiğinin devam etmesi: Buna göre başka kişi veya kullanıcılar sistemde aktif olabilirler ve kötü niyetli bir çalışma yapıyor olabilirler.
* Sistemde yapılandırılmış bir güvenlik duvarı olduğu taktirde bazı uygulamaların internetten bağlanma girişimleri
* İnternet sitelerinde dolaşırken reklam pencerelerinin açılması
* Bilgisayarın işlemez hale gelmesi
* Telefonlardaki kötü amaçlı yazılımlar

Bir sisteme virüs bulaşması durumunda güncel bir anti-virüs programıyla sistemi taramak gerekmektedir. Virüsler başlıca üç bölümden meydana gelmişlerdir. Bunlar sırasıyla kopyalama bölümü, gizleyici bölümü ve etki bölümüdür. Kopyalama bölümü ile virüs kendisini çalıştırılabilir dosyalara (.EXE file) ilave eder.

Gizleyici bölümü kendini gizleme görevi yapar. Anti-virüs programlarının tespit etmemesi için saklanır. Etki bölümü ise asıl işlemi gerçekleştirir. Örneğin dosyaların yapısını bozmak, silmek, değiştirmek, hard-diskin bir kısmına ulaşamamak gibi işlemleri yapar.

Genel olarak virüsleri tahrip edici ve sisteme rahatsızlık verici olarak ikiye ayırabiliriz. Tahrip edici virüsler verilerin veya programların bir kısmına veya tamamına zarar verip sistemin çalışmasını engellerken sisteme rahatsızlık verici virüsler ise geçici bir süre sistemin çalışmasına engel olan virüslerdir.

Bilgisayar virüslerinin yol açtığı zararlar küçük gibi gözükse de toplamda çok büyük zararlara yol açabilmektedirler. 3 Mayıs 2000 günü tüm dünyada yayılan ve elektronik postaya ekli olarak gelen “I Love You” veya “Love Bug” virüsü çok kısa bir zamanda 55 milyon bilgisayara ulaşmış ve bunların 2,5-3 milyonuna bulaşarak 8,7 milyar dolar zarara neden olmuştur. [80] [78]

##### 4.3.5.1.15 Trojans

Faydalı bir fonksiyonu varmış gibi görünen fakat aynı zamanda gizli ve güvenlik mekanizmalarını aşabilecek potansiyel zararlı fonksiyon içer en ve bazen bir sistem biriminin meşru olarak yetkilendirilmesini istismar eden bir bilgisayar programı olarak tanımlanmaktadır. [81].

Genellikle ücretsiz olarak sunulan yazılımlarla birlikte sisteme bulaşmaktadırlar. Truva atlarından korunmanın en iyi yolu kaynağı bilinmeyen yazılımların sisteme yüklenmemesidir.

Truva atı çeşitli zararlar vermek için dizayn edilmiş olsa da zararsız da olabilir. Truva atları sistemde nasıl gedik açabildiğine ve nasıl tahribat yaptığına göre sınıflandırılır. Truva atları 7 farklı amaca hizmet edebilir. Bunlar:

* Uzaktan Erişim
* E-posta Gönderme
* Veri yıkımı
* Proxy Truva
* Ftp Truva
* Güvenlik yazılımını devre dışı bırakma
* Hizmetin reddi servis saldırıları (DoS Saldırıları)
* URL truva (zararlı bulaşmış bilgisayarı sadece pahalı bir telefon hattı üzerinden internete bağlama)

Bazı örnekler;

* Veriyi silme ya da üzerine yazma
* Ustaca dosyalara zarar verme
* Bilgisayar kamerasını açarak kullanıcının görüntüsünü kaydetme
* Dosyaları internetten çekme veya internete aktarma
* Kurbanın bilgisayarına uzaktan erişime izin verme. Buna RAT denir.
* Diğer zararlı yazılımları üzerinde toplama. Bu noktada Truva atı dropper ve vector diye ikiye ayrılır.
* DDoS saldırısı yapabilmek veya spam e-posta göndermek için zombi bilgisayar ağı kurma
* Bilgisayar kullanıcısının alışkanlıklarını başka insanlara gizlice rapor etme kısacası casusluk
* Arkaplan resmi oluşturma
* Klavye tuşlarını şifreleri ve kredi kartı numaraları gibi bilgileri çalabilmek için kaydetme (keylogging)
* Suç aktivitelerinde kullanılabilecek banka ya da diğer hesap bilgileri için oltalama
* Bilgisayar sistemine arka kapı yerleştirme
* Optik sürücünün kapağını açıp kapama
* Spam posta göndermek için e-posta adreslerini toplama
* İlgili program kullanıldığında sistemi yeniden başlatma
* Güvenlik duvarını veya anti-virüs programına müdahale etmek veya devre dışı bırakma [93]

##### 4.3.5.1.16 Worms

Worms da tıpkı virüslerde olduğu gibi, kendini bir cihazdan başkasına kopyalamak üzere tasarlanmışlardır, ancak bunu kendi başlarına gerçekleştirmektedirler. Öncelikle bilgisayarda dosya veya veri transferi yapan fonksiyonların denetimini ellerine geçirip bir kez sisteme bulaştıktan sonra kendi kendine yollarına devam edebilirler. Worm’ların en göze batan tehlikesi, büyük miktarlarda çoğalma yetenekleridir. Kullanıcıların veri ve dosya alışveriş yöntemlerini kullanarak kendilerini, irtibat halinde olunan tüm bilgisayarlara, tüm e-posta adreslerine gönderebilmektedirler. Bu da ağ trafiğinin önemli derecede yavaşlamasına neden olabilmektedir. Bir worm yeni çıktığında, daha güvenlik yazılımları tarafından tanınmadığı için ilk etapta ağ trafiğini önemli oranda yavaşlatabilmektedir. [78]

Worms genel olarak kullanıcı müdahalesi olmadan yayılmakta ve kendilerinin birebir kopyalarını ağdan ağa dağıtmaktadırlar. Worms yayılmak için bir taşıyıcı programa veya dosyaya ihtiyaçları olmadığı için sistemde bir tünel de açabilmekte ve başkasının, bilgisayarınızın denetimini uzaktan eline geçirmesine olanak sağlayabilmektedir. Karıştırılan terimler oldukları için virüsleri, Truva atları ve worm’lardan ayıran özelliği burada vurgulamakta fayda bulunmaktadır: Truva atları zararsız birer yazılım gibi görünmekte ve bir sistemde istismar edeceği bir durum ortaya çıktığında (bilgisayarın İnternete bağlanması gibi) devreye girmekte, diğer zamanlarda sisteme herhangi bir müdahalede bulunmamaktadır. Solucanlar ise ağda kendilerini yayabilen kendi başlarına birer programdırlar. Bunların aksine virüs, bulaşmak için kendine ye tenbir program değildir. Kendini başka dosyalara ilave ederek yayılır ve eğer virüslü dosya açılmazsa virüs başka ortamlara yayılamaz. [93]

**İnternetteki worm örnekleri**

İnternette sörf yaparken karşımıza çıkan küçük pencerelerde ilgi çekici şeyler bulunmaktadır. Bunlara tıkladığımızda İnternet Explorer solucan virüsü taşıyan dosyalar indirir. Tıkladığımız andan itibaren virüs bilgisayarımızda etkinleşir. Bazı penceredeki yazıların örnekleri;

* Tebrikler 250 sms kazandınız telefonunuza indirmek için tıklayınız.
* Tebrikler Amerika'ya gitme hakkını yakalamak için ücretsiz çekiliş kazandınız.
* Tebrikler Amerika kapınızda.
* Visa kartınıza bonus kazandınız.
* Sitemize giren 1000000’uncu kişisiniz. Bizden hediye şarkı kazandınız.
* Bugün şanslı gününüzdesiniz. Bizden para ödülü kazandınız.
* Tebrikler bizden saat kazandınız.

Tübitak tarafından 2011 yılında yapılan bir açıklamada son yılların en büyük saldırılarından biri olan ve tüm dünyada 15 milyon bilgisayara bulaştığı tahmin edilen “Conficker” adlı solucanın zayıf şifreler sahip kullanıcı hesapları aracılığıyla ağ üzerindeki paylaşımlarla ve solucanın bulaştığı bilgisayarlara takılan taşınabilir bellekler vasıtasıyla yayıldığı belirtilmiştir. [93]

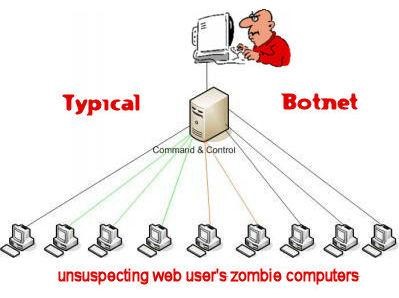
##### 4.3.5.1.17 Bot

Bot bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir. Pek çok bilgisayar işlemini yarı-otomatik olarak yapabilen robotlar bilişimin tüm alanlarında kullanılır. En ünlü oldukları alan arama motorları tarafından kullanıldıkları endeksleme teknolojisidir. Akıllı ajan teknolojilerinin İnternet ile birlikte hızla yaygınlaşması İnternet robotu ya da kısaca bot olarak adlandırılan ve özel olarak İnternet üzerinde hareket göstermek üzere geliştirilen bir ajan yazılımı grubunu ortaya çıkarmıştır. Bu grupta esasen web tabanlı arama motorlarının çekirdeklerinde yer alan örümcek yazılımları ve özel amaçlı tarayıcı yazılımlar gibi değişik türler de yer alır. Kesin bir çizgi olmamakla birlikte [Çek dilinde](http://tr.wikipedia.org/wiki/%C3%87ekce) iş anlamına gelen robota kelimesinden türeyen [robot](http://tr.wikipedia.org/wiki/Robot) kelimesinin kısaltılmışı olan bot kavramı akıllı ajan yazılımlarının İnternet üzerinde etkinlik gösterenlerine verilen bir ad olmuştur. Belki de bu adlandırmada gerçek dünyada robot davranışı olarak adlandırılabilecek türden davranışların sanal dünyadaki karşılığı olmaları beklentisi etkili olmuştur. [93]

Günümüzde pek çok değişik bot türünden söz edilmektedir. Ticari [veri madenciliği,](http://tr.wikipedia.org/wiki/Veri_madencili%C4%9Fi) e-posta, oyun, kamusal haber grubu, sohbet, alışveriş, hisse senedi, yazılım vb. gibi hedeflenen bilgi türüne göre adlandırılan pek çok bot türü mevcuttur. Bu türlerin hemen hepsi karakteristik olarak otonom bilgi ajanları/arabirimleri olarak ve özellikle İnternet üzerinde faaliyet göstermek üzere tasarlanmış ve geliştirilmiş yazılım türleridir. [93]

##### 4.3.5.1.18 Botnets

Zombi bilgisayarlar ya da botnetler bu tehdit grubunun en tehlikeli olanları olarak kabul edilebilir. Burada önemli olan nokta, bilgisayar kullanıcısının hiçbir haberi olmaksızın bilgisayarının çok ciddi suçlar işlenmesinde kullanılabilmesidir. Bu tür bilgisayarlar robot veya bot şeklinde de ifade edilmektedir.



Şekil 4.3.5.1.18: Basit Bir Bot-Net

Zombi ordunun bir parçası haline gelen bilgisayarlarda buna sebep olan nokta, genellikle bu tür bilgisayarların firewall denilen güvenlik duvarlarının olmamasıdır. Günümüzde bant genişliğinin artmasıyla beraber herhangi bir korunmaya sahip olmayan bir bilgisayar kolaylıkla bir botnet’in parçası haline gelebilir. Bir botnet, genellikle açık bır akılan bir kapıdan (port) bir bilgisayara, daha sonra aktif hale gelecek şekilde, truva atı bırakılması sonucu oluşturulmaktadır. Botnet’in parçası haline gelen bilgisayarlar mesela bir web sitesine aynı anda yönlendirilerek bu siteyi hizmet veremez hale getirmek için kullanılabilmektedir. [94] [93]

##### 4.3.5.1.19 Keyloggers

Keylogger’lar kısaca klavye işlemlerini kaydeden programcıklardır. Bu programcıklar, farkına varılmadan klavyede dokunulan her tuşu kaydedip, fırsatını bulduklarında daha önce belirlenen adreslere bunları göndermektedirler. Özellikle bankacılık işlemlerinde klavyeden şifre girilmemesi, rakamlara tıklanarak veya rakamların üzerlerinde beklenerek şifreler girilmesi ve ayrıca cep telefonu ile SMS şifreleri yoluyla ilave güvenlik desteği sunulabilmesine rağmen İnternet üzerinden ticaret yapan birçok site, alıcıların kredi kartı bilgilerini girmesi için güvenlik seviyesi yüksek bu tür platformlar oluşturmamaktadır. Bu da klavyeden girilen bu bilgilerin nasıl kolayca başkalarının eline geçebileceğini göstermektedir. Bu durum, sadece alışveriş ve bankacılık işlemleriyle sınırlı değildir. Klavye işlemlerini kaydeden bu tür yazılımlar nedeniyle, e-posta ve sosyal paylaşım siteleri gibi kullanıcıların özel bilgilerinin yer aldığı web sit elerine ait kullanıcı adları ve şifrelerin ne kadar büyük tehlike altında olduğu anlaşılabilmektedir. Günümüzde sosyal medya ve online oyunların ne kadar yaygın olduğu ve bunlar yüzünden meydana gelen cinayet ve intiharların ne kadar çok arttığı göz önünde bulundurulursa keylogger’ların meydana getirdiği asıl tehlike gerçek manasıyla anlaşılabilir.

Bu yazılımlar, aynı zamanda aldatan bir eşi takip etmede, işverenlerin çalışanlarını izlemesinde veya bir çocuğun bilgisayarda neler yaptığının gözlenmesinde kullanılabilmektedir. Bu programlar, maksatlı kişiler tarafından bilgisayarlara doğrudan fiziksel erişim sağlanarak veya İnternete bağlı olan bir bilgisayardaki açıklıklar kullanılarak sistemlerin içerisine kurulabilir. [28]

Keylogger’lar küçük programcıklardır ancak bunlar sadece yazılım olarak değil donanım olarak da var olabilmektedirler ve kullanıcılar ve sistemler bunların farkına varamamaktadırlar. Bu tür klavye hareketlerini kaydeden donanımlar fiziksel olarak klavye ile bilgisayar arasına monte edilmekte ve bilgisayar kasasının arka kısmına gizlenmektedir. Yapılan araştırmalarda ne kullanıcılar, ne de sistemler bu kaydedicileri fark etmiştir. Hazırlanmaları ve kurulumları çok basit olan bu tür cihaz ve yazılımların varlıklarına karşı dikkatli olunması gerekmektedir. [93]

#### 4.3.5.2.Saldırı Tespiti

Intrusion Detection System- IDS, bilgisayarların ve bilgisayar ağlarının faaliyetlerini izlemek, kaydetmek ve olası saldırıları tespit etmek amaçlı olarak tasarlanan sistemlerdir. İki tip saldırı tespit sistemi vardır:

1. **Network Based:** Bir bilgisayar ağının tamamını ya da belli bir kısmını izlerler. Ağ üzerinde herhangi bir noktadan çalıştırılabilirler.
2. **Host Based:** Belli bir bilgisayarı izlerler. Bu tür sistemler, izlenecek olan bilgisayar üzerinde çalışırlar. İzlenen bilgisayarı kullanan kullanıcıların yapacakları hatalardan dolayı oluşacak zararları önlemeye yöneliktirler.

Bu tür hatalar, sistem dosyalarının silinmesi, önemli ayarların değiştirilmesi gibi şekillerde karşımıza çıkabilirler.

İyi bir saldırı tespit sistemi, çok az kullanıcı müdahalesi ile çalışabilmeli, sistem kaynaklarını en az düzeyde kullanmalı, sistemde zaman içinde yapılacak değişikliklere karşı uyum sağlayabilir (adaptive) olmalı, sistemdeki normal davranış ile normal dışı davranışı ayırt edebilmelidir.

Saldırı tespit Sistemleri, temelde bilgi tabanlı ve imza tabanlı olmak üzere iki farklı mantığa göre kurulmaktadırlar.

Daha önce karşılaşılan saldırı şekilleri ayrıntılı olarak analiz edilerek elde edilen bilgiler, yani saldırının imzası, saldırı tespit sisteminin bilgi tabanına kaydedilir. Her tanımlanmış saldırının bir imzası vardır. Saldırı imzaları dışında kalan her faaliyet, normal olarak algılanır. Bu şekilde çalışan bir saldırı tespit sisteminin verimli çalışması için, sürekli saldırı imzalarını güncelleyerek sistemi, yeni saldırı tiplerini de tarayacak şekilde güncel tutmak gerekir.

Bilgi tabanlı saldırı tespitinde ise, sistem kullanıcılarının, normal davranışlarından farklı olarak gösterdikleri davranış şekillerine göre çalışma yapılır. Bu yöntem, tahmine dayalı bir sistemdir ve genellikle “uzman sistemler” ve “bulanık mantık” teknolojilerinden faydalanılır.

Bir saldırı tespit sisteminin, ağ üzerindeki faaliyetleri izlemek için ağ üzerindeki farklı noktalarda alıcı cihazlarını ve yazılımlarını kurmak gerekebilir. Bu cihaz ve yazılımların görevi, sorumlu oldukları ağ bölümü üzerinde gerçekleşen faaliyet bilgilerini, saldırı tespit sistemi merkezine aktarmaktır.

Bir Saldırı tespit Sistemi, bir hata yaptığında bu hata iki şekilde olabilir.

1. **False Positive:** Saldırı Tespit Sistemi, sistemdeki normal bir davranışı saldırı olarak algılayarak hata yapmıştır.
2. **False Negative**: Bu tür bir hata, yanlış pozitife göre çok daha vahim sonuçlar doğurabilir. Bir yanlışnegatif hatası, saldırı tespit sisteminin işini yapmadığı ve bir saldırıyı tespit edemediğinin bir ifadesidir.

Saldırı tespiti ve saldırgan davranışlarının ortaya çıkarılmasında son zamanlarda ortaya çıkarılan bir yöntem de *honey-pot* yöntemidir. Bu yöntemde ağ üzerinde kurulan bir bilgisayar, üzerinde çalışan hizmetler ve korunmasız görüntüsü ile saldırganların ilgisini çekerek bu bilgisayara saldırmaya özendirmektedir. Bu bilgisayar, gerçek operasyonel bir sistem görüntüsü vermekte ve aynı zamanda saldırganın tüm faaliyetleri kaydedilmektedir. Saldırı sonucu bu sistem devre dışı kalıp çökse dahi, tüm saldırgan davranışları kaydedilmiş olmakta, elde edilen bu veriler yardımıyla yeni saldırı imzaları ve yöntemleri keşfedilebilmektedir. [95]

### 4.3.6 Access Control

Bilişim güvenliğinde en önemli konularda biri, kaynaklara kimin nasıl eriştiğini kontrol etmek, bu sayede bilgi üzerinde yetkisiz değiştirme ve açığa çıkarma olaylarını engellemektir. Bu amaçla yapılan faaliyetlere genel olarak access control denir. Bir kullanıcı bilgisayarından ağ üzerindeki bir dizine ulaşmak istediğinde ona kullanıcı adı ve parola soran bir ekranla karşılaşması, erişim denetimine örnek olarak verilebilir. Erişim denetimi, yazılım ve donanım tabanlı olarak sağlanabilir.

Erişim denetimi yardımı ile kullanıcı ve sistemlerin, diğer sistemlerle nasıl etkileşimde bulundukları belirlenir. Erişim denetimi kontrolleri ile kaynaklara yetkisiz erişimler engellenir ve yetkili kullanıcıların da yetki derecelerine göre erişimleri sınırlandırılır. Erişim denetiminde karşımıza çıkan iki önemli kavram vardır: Bunlar kullanıcıları ifade eden *özneler* ve kaynakları ifade eden *nesnelerdir*. Erişim, bir özne ile bir nesne arası veri akışı olarak ifade edilir. Özneler, bir nesne içerisindeki bir veriye erişimi talep eden varlıklardır. Nesneler, bir bilgisayar programı, veritabanında saklanan veriler ya da bir bilgisayar olabilir. Erişim denetimi üç aşamalı olarak gerçekleştirilebilir:

1. Identification
2. Authentication
3. Authorization

Bölüm 4.3.6.1’de Identification, Bölüm 4.3.6.2’de Authentication, Bölüm 4.3.6.3’de ise Authorization konusuna değinilmiştir [95]

#### 4.3.6.1 Identification

Değerli bir kaynağa, yalnızca ona erişmeye hakkı olanlara erişim yetkisi verilmelidir. Bu erişim yetkisinin denetimi sırasında, kullanıcılardan iki tür bilgi istenir.

Birinci bilgi herkesin bildiği kullanıcıya ait ve kullanıcının kimliğini belirten bir bilgidir. Sosyal güvenlik numarası, çalıştığı kurumdaki sicil numarası, kullanıcının adı soyadı, sistemden tanımlanmış kullanıcı adı, kullanıcı kimliğine örnek olarak verilebilir.

İkinci tür bilgi ise, yalnızca kullanıcının bildiği özel bir bilgidir. Bu konu Bölüm 4.3.6.2’de ele alınmıştır. [95]

#### 4.3.6.2 Authentication

Authorization, bir kişinin Bölüm 4.3.6.1’de anlatılan kimliğe sahip kişi olduğunun tespit edilmesidir. Bu ispat bir parola, bir akıllı kartın kullanımı, tek seferlik bir parola, bir sayısal imza bilgisi, biyometrik bir özelliğin belirlenmesi şeklinde karşımıza çıkabilir.

Giriş parolası, en yaygın kullanılan kimlik sınama biçimidir. Kullanım kolaylığının yanında, başkalarının eline geçmesi kolay olduğundan güvenlik boşluğu oluşturmaya aday bir teknolojidir. Bununla beraber parolamızla ilgili uyulacak birkaç basit kural, parolamızın başkalarının eline geçmesini engelleyecektir:

1. **Parola Değiştirme:** Parolaları çok uzun süre kullanmamalı, belli aralıklarla değiştirmeliyiz.
2. **Sisteme Girişi Sınırlama:** Eğer bir kullanıcı kimliği yanlış parolayla defalarca sisteme girmeye çabalıyorsa, bu parolamızı tahmin etmeye yönelik bir çalışma olabilir. Sistem, belli bir sayıda yanlış girişten sonra bu kullanıcının erişim hakkını askıya alarak, kendini ve asıl bu kimliğe sahip olan kullanıcıyı korumuş olur.
3. **Parola Seçimi ve Saklama:** Kesinlikle boş parola kullanılmamalıdır. Parola en az 6 karakter olmalı içinde, harf, rakam, diğer özel karakterler (%,!, ?, = gibi) grubundan en az birer karakter içermelidir. Parola, bilinen ya da tahmin edilebilecek bir kelimeden (soyad, evcil hayvan adı, şehir adı gibi) ya da sözlüklerde bulunan sözcüklerden oluşmamalıdır.

Biyometrik tanıma, bir kişinin vücudunda bulunan ve yalnızca ona has özellikler taşıyan bir özelliğin sisteme tanıtılmasıdır. Bu özelliklere el ayası, el geometrisi, retina taraması, iris taraması, parmak izi, ses, yüz şekli, tuşlara basma hızı gibi örnekler verilebilir.

Sisteme verilecek özel bilgi olarak sahip olunan bir akıllı kart ya da jeton (hardware token) da kullanılabilir. Son yıllardaki hızlı gelişimleri ile akıllı kartlar, hem fiziksel hem de mantıksal erişim denetim sistemlerinde yaygın kullanım alanı bulmaktadırlar. Bir akıllı kart, kullanıcısına özel birtakım veriler taşır. Tek bir akıllı kart, çokluuygulama desteği sayesinde birden çok uygulamada kullanılabilir, böylece cüzdanımızın bir kart cennetine dönüşmesinden kurtuluruz. Örneğin bir üniversite kampüsü içerisinde, hem kapıdan girerken, hem otopark ücretini öderken, kütüphaneden ödünç kitap alırken, genel kullanımlı bir bilgisayara giriş yaparken, yemekhanede ücret öderken ve daha sayısız birçok uygulamada kullanılabilen akıllı kartlar mevcuttur.

Yukarıda belirtilen kimlik sınama yöntemlerinden birden fazlasının birlikte kullanılması, erişim denetim güvenliğini arttıracaktır. [95]

#### 4.3.6.3 Authorization

Aslında Authorization ile Authentication birbirine karıştırılabilir. Yetkilendirme, sisteme kendini kimliği ile tanıtmış ve kimlik sınaması yapılmış (yani belirttiği kimliğe sahip olan kişi olduğunu ispatlamış) kullanıcılara, sistem kaynaklarına erişim izni verilmesidir. Kullanıcı, kimlik sınaması yapıldıktan sonra, ağ üzerindeki bir kaynaktaki bir dosyaya erişmek istediğinde, öncelikle bu kullanıcının bu kaynağa erişim yetkisi olup olmadığı sınanır. Eğer yetkisi varsa, kaynağa erişmesine izin verilir. Yani bir kullanıcı, kimlik sınaması yapıldıktan sonra, tüm kaynaklara erişme yetkisine sahip olmaz. Erişim yetkisi, kendisine verilen yetki düzeyi ile sınırlıdır. [95]

### 4.3.7 Anti-Virüs Sistemleri

Bilgisayar virüsleri, “Kötü amaçlı program kodu” olarak tanımlanabilir. Korumasız bir bilgisayar ve bilinçsiz bir kullanıcı, bir bilgisayara virüs bulaşması için yeterlidir. Çünkü e-posta yoluyla gönderilen, kullanıcılara cazip öneriler sunan (erişkin sitelerine ücretsiz erişim hakkı ya da kılını kıpırdatmadan para kazanma gibi) ve tek yapmaları gerekenin ekteki programı kurmak olduğunu iddia eden e-postalar yoluyla virüsler, gerçek hayattaki virüslerden farksız bir hızla yayılmaktadırlar. Anti-virüs yazılımları, bilinen virüsleri tanıyabilen ve temizleyebilen programlardır. Bir anti-virüs yazılımı yalnızca bildiği tür virüsleri tanıyabilir. Yeni ortaya çıkmış bir virüsü tanıması imkansızdır. Örneğin 1999 yılında ortaya çıkan “Melissa” ve 2000 yılının ortaya çıkan “IloveYou” virüsleri anti-virüs programları kendilerini tanıyana kadar ciddi zararlara ve maddi kayıplara yol açmışlardır.

Bir virüsün kimliğine o *virüsün imzası* da denir. Bir kurum, elindeki anti-virüs yazılımlarını, üreticilerinin yeni yayınladığı virüs imza listeleri ile sürekli güncellemelidir. Yeni virüslere karşı da kullanıcı bilinçlendirmesi yoluyla önlem alınabilir. Kullanıcılar, tanımadıkları kimselerden gelen, cazip öneriler içeren e-postaları açmamalı, gerektiğinde sistem ve güvenlik yöneticilerini vakit kaybetmeden konu hakkında bilgilendirmelidirler. Bunun yanında anti-virüs programları, artık güvenlik duvarları ve e-posta sunucuları ile birlikte çalışabilmektedir. Bu şekilde tedbirlerin bütünleşik çalışması sonucu, virüs bulaşma riski en aza indirilmeye çalışılmaktadır.

Bu bölümde ele alınan teknolojilerin, birbirleri ile etkileşimli çalışacak şekilde kullanılması sonucu, kurumun daha etkin korunması gerçekleştirilebilir. Saldırganın karşısına her bir engeli ya da tedbiri aştığında çıkarılacak olan yeni bir tedbir, sistemin saldırganlara karşı caydırıcılığını arttıracak ve sistemin verdiği güvenlik hizmetlerini tamamlayıcı olacaktır. [95]

### 4.3.8 Eğitim

Bir kurumda bilişim güvenliğinin yerine getirilmesi amacıyla, politikalar, prosedürler oluşturulabilir. Bu prosedürleri yerine getirebilmek için yüksek miktarlarda paralar harcanarak tedbirler konulabilir. Tüm bunlarla birlikte, harcanan bu kadar paranın ve hazırlıkların anlamlı olabilmesi için, sistem içerisinde yer alacak olan kullanıcıların eğitilmesi ve kurulan güvenlik sistemi ile ilgili bilinçlendirilmesi gerekir. Eğitim programının amacı, kurumdaki her bireyin, güvenlik programının bir bütün olarak kurum için ve her bir birey için önemini kavraması olmalıdır.

Eğitimler, kurum içinde en azından üç farklı grup için tasarlanmalıdır: Yöneticiler, orta kademe yöneticiler ve teknik grup.

Yönetici eğitimleri, mümkün olduğu kadar kısa tutulmalıdır. İçerik olarak, kurumsal kaynaklardan, bunların değerinden, korunması ve saldırılara karşı alınan tedbirler için yapılan harcamadan bahsedilmelidir.

Orta kademe yöneticilere verilecek eğitimlerde, üst düzey yöneticilere verilenden farklı bir eğitim içeriği hazırlanmalıdır. Her orta kademe yöneticinin sorumlu olduğu bölümün, kurumsal güvenlik açısından önemine yer verilmeli, kurumsal güvenlik programının sürdürülmesi ve başarı kazanması için kendi sorumluluklarında çalışan personelin güvenli bir çalışma ortamında çalışması amacına nasıl katkıda bulunabilecekleri aktarılabilir.

Teknik bölümlerde çalışan insanlar için ise, güvenliğin onların günlük faaliyetlerini nasıl etkileyeceğine yönelik bir eğitim verilmelidir. Diğer gruplara göre, teknik gruba, üzerinde çalıştıkları sistemlerin nasıl etkileneceği, olası güvenlik ihlallerinin neler olabileceği bilgilerini içeren daha ayrıntılı bir eğitim verilmelidir.

Her üç grubun üyeleri de bir güvenlik ihlali ile karşılaşmaları durumunda, ne yapacakları, kime bilgi verecekleri konusunda bilgilendirilmelidirler. Hiçbir çalışan, bir saldırı ile karşılaştığında bununla kendisi mücadele etmeye ya da saldırıya karşı koymaya uğraşmamalıdır.

Kurulan güvenlik sisteminin ortadan kalkması durumunda kullanıcıların nasıl etkilenecekleri, sistemin yararı konusunda kullanıcıları bilinçlendirmek açısından uygun bir yöntem olacaktır. Bu tür eğitimlerde, uygun ve uygunsuz davranışlara birçok örnek verilerek, sistemin kullanışı ile ilgili bilgiler, örneklerle desteklenebilir. Bu örnekler arasında, yetkisiz bir personelin kurumun giriş/çıkış kontrollü bir bölgesinde neden bulunduğunun sorgulanması, e-postaların beklenen kullanım şekilleri, internetin doğru bir şekilde kullanılması, şirkete ait bilgi ve belgelerin kullanım şekilleri gibi konular olabilir.

Eğitimlerin sonunda, kullanıcılara, güvenlik konusunda aldığı eğitimde gördüğü konular hakkında bilgi sahibi olduğuna ve kurumun güvenliğini ihlal yönünde bir faaliyette bulunmayacağını taahhüt ettiğine dair bir belge imzalatılabilir. [95]

### 4.3.9 Bilişim Güvenliği Standartları

Kurumsal ölçekte bilişim güvenliğinin sağlanması, teknik bir problem olmanın yanısıra, yönetimsel bir problemdir. Bilişim güvenliğini sağlamaya yönelik tedbirler, teknolojiler, bunların kurum içinde kullanımı, işletilecek süreçler ve bunların sahipleri gibi pek çok konuda kalıcı ve etkin kararların verilmesi, bu karar ve bilgilerin belgelerle desteklenmesi ve konunun bir yaşam döngüsü bakış açısıyla canlı tutulması gereklidir. Bu amaçla çeşitli standartların oluşturulması ve uygulanması bir yöntem olarak benimsenmiştir.

BS 7799, güvenlik politikası geliştirme ve güvenlik denetlemesi yapma konularını kapsayan uluslararası bir standarttır. Bu Standart, 10 alt bölümden oluşur. Her bölümde, o bölümde anlatılan konunun, kurumsal güvenlik politikasına nasıl dahil edileceği ve bu faaliyetlerin nasıl denetleneceği ile ilgili bilgiler vardır.

ISO, BS 7799’u temel alarak ISO 17799 standardını hazırlamıştır.

Aşağıdaki listede, standardın her bölümünün kısa birer tanıtımı yer almaktadır:

**İş Sürekliliğinin Planlanması:** Kritik iş kaynakları tanımlanır ve bu kaynaklara zarar vermeye ve onların sürekliliğini etkilemeye yönelik olan faaliyetlerle mücadele için tedbirler alınır. Burada bahsedilen zarar, küçük ya da büyük bir zarar olabilir.

**Sistem Erişim Denetimi:** Erişim denetimine ihtiyacı olan kaynaklar belirlenir. Yetkisiz gerçekleşen faaliyetler tespit edilmeli ve uygun bir şekilde kotarılmalıdırlar.

**Sistem Geliştirme ve Sürdürme:** Bilginin gizliliği, bütünlüğü ve kimlik sınaması korunmalıdır. Tüm bilişim faaliyetleri güvenli bir şekilde gerçekleştirilebilmelidir. Uygulama yazılımların ve bunlara ilişkin verinin güvenliği de göz önünde bulundurulmalıdır.

**Fiziksel Güvenlik ve Çevre Güvenliği:** Kuruma ait bina ve benzeri yerlere giriş çıkışlar kontrol altında tutulmalıdır. Bu sayede verilerin, bilgisayar ve bilgisayar ağlarına ilişkin cihazların çalınmasını ve zarar görmesi engellenir.

**Uygunluk:** Yasal olarak yapılmış düzenlemelere, kurumsal olarak ortaya konulan politika ve kurallara uygunluk sağlanmalıdır.

**Kurum Çalışanlarının Güvenliği:** Kullanıcılar, potansiyel tehditler ve kurumsal güvenlik politikasını desteklemek üzere nasıl davranılacağı hakkında bilgi sahibi olmalıdırlar.

**Güvenlik Organizasyonu:** Kurum içinde bilgi güvenliğinin yönetimi yapılmalıdır. Bilgi-işlem hizmetleri, başka bir firma yardımıyla dış kaynaktan alınıyor olsa bile, kuruma özel bilgiler, yine kurum içersinde korunmalıdır.

**Bilgisayar ve Ağ Yönetimi:** Bilgi işlem ve iletişim kaynakları korunmalı ve bu kaynakların bütünlüğü ve sürekliliği sağlanmalıdır.

**Kaynak Sınıflandırması ve Kontrol:** Bilgi kaynakları için uygun sınıflandırma yapılmalı ve her sınıflandırma düzeyi için gerekli koruyucular devreye sokulmalıdır.

**Güvenlik Politikası:** Kurumsal güvenlik programının temeli olarak bir güvenlik politikası oluşturulmalıdır. [95]

# BÖLÜM 5: WIRED ve WIRELESS NETWORK’LERDE GÜVENLİK TEKNOLOJİLERİ ve PROTOKOLLERİ

Günümüzde, wired ve wireless network’lerde güvenlik konusunun, bu kadar kritik bir hal alması, bu konudaki güvenlik teknoloji ve protokollerinin de hayati derecede önem kazanmasını sağlamıştır. Wireless network, wired network’lere göre sağladığı birçok fayda (gezginlik, kolay kurulum, sağlamlık) nedeni ile günümüzde artık vazgeçilmez bir boyuttadır ve giderek wired network’lerin yerini daha çok almaktadır. Bu bölümde ilk olarak wired ve wireless network’lerin taşıdığı riskler incelenecektir. Sonrasında wireless network standartları incelenecek, ikinci olarak ise wireless network’ler için geliştirilen güvenlik protokolleri olan WEP (wireless equivalent protocol), WPA (wireless protected access) ve en yeni güvenlik protokolü olan RSN (robust security network) ayrıntılı şekilde incelenecektir. Üçüncü olarak da kablolu ağlarda güvenlik teknoloji ve protokolleri ele alınıp, son olarak konu akışı içersinde bahsedilmemiş olan Authentication Protokollerini de ele alarak bölüm sonlandırılacaktır.

## 5.1 Wired ve Wireless Network’lerin Taşıdığı Riskler

### 5.1.1 Wireless Network’e Sızma

Access point’ler, uygun güvenlik önlemleri alınmaması durumunda, saldırganlar için wired ve wireless network’lere bağlanmak için açık uç sağlar. Wired network’lerdeki mevcut önlemler saldırganın iç ağa direk erişiminin olmadığı, en azından bir güvenlik duvarı üzerinden geleceği varsayımına dayanmaktadır. EN üzerinden iç ağa erişim, geniş alan ağından gelen saldırganları önlemek için kullanılan güvenlik duvarının atlatılması ve güvenlik açığı bulunması muhtemel birçok servise direk erişim sağlanması riskini taşımaktadır. [122]

### 5.1.2 Trafiğin Dinlenip Verinin Çözülmesi

Access point’ler bir hub gibi davranırlar, gelen trafiği ortak transmisyon ortamına, yani havaya gönderirler ve bu trafik ortamdaki diğer bütün kablosuz cihazlar tarafından dinlenebilir ve kaydedilebilir. Kullanılan şifreleme algoritmasının açıklıklarının bulunması durumunda bu veri paketleri olası saldırganlar tarafından çözülebilir. Örneğin yerel ağda gönderilen Telnet / POP3 / SMTP parolaları, NTLM özetleri saldırganlar tarafından elde edilebilir, yazışmalar, epostalar, internette sörf yapan kişilerin ilgi alanları konusunda bilgiler açığa çıkabilir. [122]

### 5.1.3 Ağ Topolojisinin Ortaya Çıkması

Kablolu ağlara yapılan saldırılarda gerçekleştirilen önemli adımlardan biri ağ topolojisinin ortaya çıkarılmasıdır. Kablosuz iletişimde 2. katmanda gönderilen kontrol paketleri şifresiz olarak gönderilmektedir, bu durum kablosuz ağdaki bütün mevcut istemci ve varsa sunumcuların network bilgilerinin ortada olmasına neden olmaktadır. Ayrıca EN’in kablolu ağa bir hub üzerinden bağlanması durumunda kablolu ağın topolojisinin saldırganlar tarafından öğrenilmesi mümkün olabilmektedir. Kablosuz ağdaki şifrelemenin kırılması durumunda iç ağ ile yapılacak trafiğin incelenmesi ile iç ağ topolojisi switch cihazı kullanılsa dahi ortaya çıkarılabilir. [122]

### 5.1.4 İstemcilerin Yetkisiz Access Point’lara Bağlanması

Saldırganlar ortama sahte erişim noktaları yerleştirebilir, ya da kendi dizüstü bilgisayarlarını basit işlemler sonucunda bir EN’ye dönüştürebilir. Yetkili istemciler uygun şekilde konfigüre edilmezlerse, bu sahte erişim noktaları üzerinden farkında olmadan istenilmeyen bağlantı kurulmasına sebep olunabilir ya da **man-in-the-middle**türü ataklara maruz kalınabilir. Bölüm 4’te aytıntılı olarak incelenmişti. [122]

### 5.1.5 İstenmeyen Yerlere Servis Verme

Kablosuz haberleşme ortamının hava olması sebebiyle fiziksel erişim kontrolü mümkün değildir. Yetkisiz istemciler güvenli olmayan yetkilendirme ve şifreleme önlemlerini aşarak mevcut kablosuz ağın kaynaklarını kendileri için kullanabilirler. [122]

### 5.1.6 Denial of service (DoS)

Kablosuz ağa bağlı istemcilere gönderilecek sahte **deauthenticate** mesajları ile kablosuz ağa DoS ataklarının yapılması mümkündür. Ayrıca ortamın **jam** edilmesi (frekans bandının gürültü seviyesinin haberleşme yapılamayacak derecede yükseltilmesi), ya da aynı frekansta hizmet veren başka erişim noktalarının ortama konulması suretiyle de DoS atakları yapılabilir. Ayrıntılı inceleme için Bölüm 4’e göz atabilirsiniz. [122]

## 5.2. Wireless Network’lerde Güvenlik Protokolleri

### 5.2.1 WEP (Wireless Equivalent Privacy – 1999)

Wireless network’lerin ilk 5 yılı için IEEE 802.11’de geçerli olan tek güvenlik protokolüdür. 2000 yılında bu protokolün zayıflıkları ortaya çıkarılmaya başlanmıştır ve birçok zayıf yönleri vardır. Fakat WEP hiçbir güvenlik protokolü kullanmamaktan daha güvenlidir. Protokol tasarlanma aşamasında iken 802.11 standartları aşağıdaki koşulları ortaya koymaktaydı. [119] [120] [121]

* Makul bir şekilde güçlü olmalı. (Algoritma kolayca kırılmamalı)
* Etkili olmalı. (Donanım veya yazılım ile gerçeklenebilmeli)
* İhraç edilebilir olmalı (ABD hükümeti anahtar uzunluğu kısıtlaması)
* Kullanımı isteğe bağlı olmalı.

Bu yukarıdaki şartlar göz önüne alınarak WEP standardı oluşturulmuştur. Kullanılan şifreleme algoritması RC4, anahtar uzunluğu 40 bit veya 104 bit, IV (initialization vector) uzunluğu 24 bit, veri bütünlüğünü ICV (integrity check value) ile sağlanmaktadır. Kullanılan şifreleme algoritması RC4 (Rivest Cipher) bir akış şifreleyicisi olup simetrik anahtar kullanmaktadır.

#### 5.2.1.1 WEP’te Asıllama Yöntemleri

Veri iletişimi yapılmaya başlanmasan önce kullanıcılar ve erişim noktaları arasında ilişkilendirilme yapılması gereklidir. Bu ilişkilendirilme yapılmadan öncede asıllama yapılması gerekmektedir. IEEE 802.11 2 farklı yöntem uygulamaktadır fakat üretici firmalar kullandığı bir yöntemde sıkça kullanılmaktadır. [119] [120] [121]

**Açık güvenlik (SSID – Service Set Identifier):**

Bu yöntemde erişim noktasına SSID bilgisi ile gelen tüm asıllama istekleri kabul edilir. Erişim noktaları SSID bilgilerini açık bir şekilde yayınlayabilirler bu gelen tüm isteklerin kabul edileceği anlamına gelmektedir.



Şekil 5.2.1.1: Açık Güvenlik Asıllama Yöntemi

**STA:** Kullanıcı

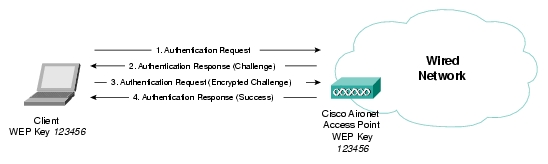
**AP:** Erişim Noktası

**Ortak Anahtarlı Asıllama:**

Asıllama paylaşılan bir anahtar sayesinde yapılır. Bu anahtar kullanıcıya daha önceden bildirilmiş olması gereklidir. [119] [120] [121]

Çalışma yapısına bakacak olursak:

1. Kullanıcı asıllama isteği gönderir.
2. Erişim noktası açık bir veri yollar.
3. Kullanıcı bu veriyi ortak anahtar ile şifreleyip geri yollar.
4. Erişim noktası bu şifreli veriyi açar ve gönderdiği veri ile karşılaştırıp asıllamayı gerçekleştirir.

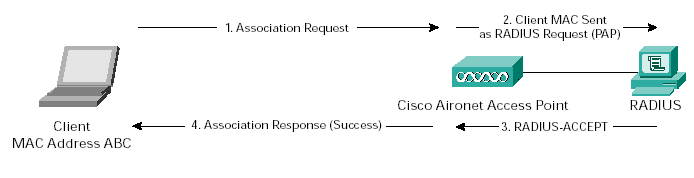
****

Şekil 5.2.1.1.a : Ortak Anahtarlı Asıllama

**MAC Adresi ile Asıllama**

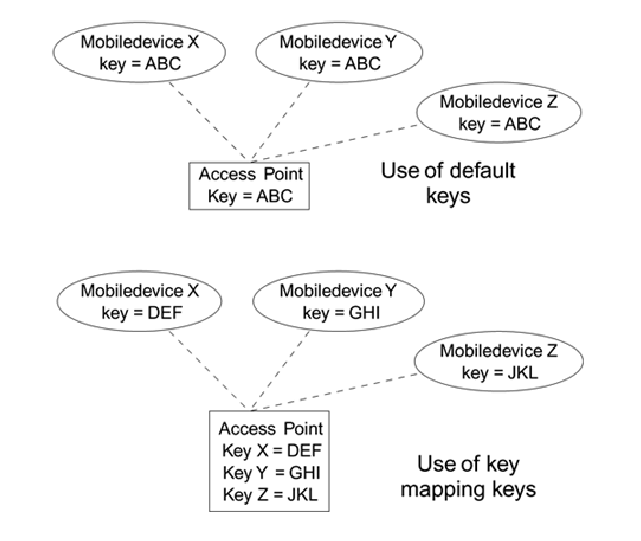
Erişim noktası üzerinden haberleşebilecek kullanıcıların MAC (Media Access Control) adresleri bir sunucuda RADIUS (Remote Authentication Dial-In User Service) tutulmaktadır. Sadece daha önceden belirlenmiş MAC adresine sahip kullanıcılar asılanmaktadırlar. Sistemin çalışma sistemine bakacak olursak. [121]

1. Kullanıcı Erişim noktasına asıllama isteği gönderir (MAC adresi de gönderilir).
2. Erişim noktası, kullanıcının MAC adresini RADIUS sunucusuna gönderir.
3. Sunucu kabul ya da ret cevabını erişim noktasına gönderir.
4. Erişim noktası kullanıcıyı asıllar.

****

Şekil 5.2.1.1.b : MAC Adresi ile Asıllama

#### 5.2.1.2 WEP’te Kullanılan Anahtarlar



WEP te kullanılabilecek anahtarlar iki gruba ayrılır. Bunlar ön seçili anahtarlar ve kullanıcıya özel anahtarlardır. Ön seçili anahtarlı yapıda erişim noktası ve kullanıcılar veri şifrelemede aynı anahtarı kullanır. Açıkça görüldüğü gibi bu yöntem kullanıldığında tüm kullanıcılar tüm verileri çözebilirler. İkinci yöntemde ise Erişim noktası her kullanıcıya karşılık farklı anahtarlar bulundurmaktadır bu sayede kullanıcı sadece kendine gelen verileri çözme yeteneğine sahip olacaktır.

Şekil 5.2.1.2: WEP’te kullanılan Anahtar

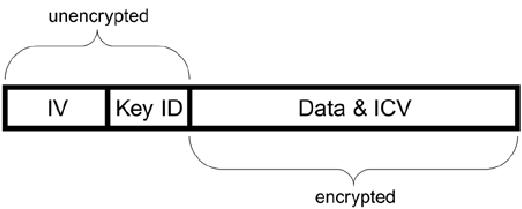
#### 5.2.1.3 Şifreleme ve Şifre Çözme

WEP şifreleme ve şifre çözme şu şekilde çalışmaktadır.24 bitlik başlangıç vektörü (IV) ,40 bitlik paylaşılan anahtara eklenir. Bu anahtardan RC4 algoritması kullanılarak şifrelenecek veri uzunluğunda akış şifresi elde edilir. IV vektörünün değişmesi ile her seferinde farklı akış şifreleri elde edilmektedir. Bu sırada veri bütünlüğü sağlamak için asıl veri üzerinden ICV hesaplanır ve verinin sonuna eklenir. Elde edilen akış şifresi ile (veri +ICV) dar veya işleminden geçirilerek şifreli metin hazırlanmış olur. Son adım olarak alıcı tarafın şifreyi çözmesi için bilmesi gerekli olan IV çerçevenin başına şifrelenmeden eklenir. Böylelikle gönderilecek çerçeve hazırlanmış olur.

Şifre çözmede ise alıcı taraf IV’yi çerçeve den okur zaten anahtar kendinde olduğu için akış şifresini elde edebilir. Şifreleme işlemlerini ters sıra ile gerçekleştirerek açık veriyi elde eder. [119] [120] [121]



Şekil 5.2.1.3: WEP Şifreleme ve Şifre Çözme



Şekil 5.2.1.3.a : WEP Çerçeve Yapısı

#### 5.2.1.4 WEP Zayıflıkları

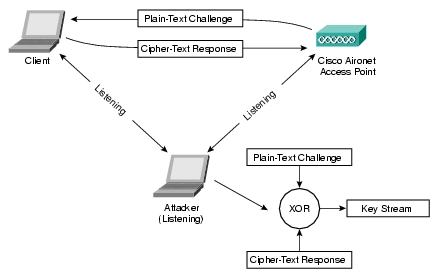
WEP güvenlik protokolü ile zayıflıklar çıktığı süreden itibaren yayımlanmaktadır. Bu protokol birçok yönden zayıf noktalara sahiptir. Aşağıda maddeler halinde bu zayıflıklar incelenmiştir. [121]

##### 5.2.1.4.1 Asıllama:

Açık güvenlikte SSID erişim noktası tarafından yayımlanmadığı durumlarda kullanıcıların SSID’yi bilmeleri gerektiğini söylemiştik. Fakat trafiği dinleyen herhangi biri de SSID değerini alıp kullanarak kendini erişim noktasına asılatabilir.

MAC adresi ile asıllamada da Yukarıdaki yönteme benzer şekilde kendini asılatan bir kullanıcının MAC adresi trafik dinlenerek ele geçirilebilir. Ve yine bu MAC adresi kullanarak kendini asıllatabilir.

Ortak anahtarla asıllamada ise belirli bir IV değeri için akış şifresi ele geçirilerek asıllama işlemi gerçekleştirilebilir. Bu işlem Şekil 5.2.1.4.1’de görüldüğü gibi hem açık metin hem de şifreli halinin ele geçirilmesi ile gerçeklenir. [119] [120] [121]



Şekil 5.2.1.4.1: Ortak Anahtarlı Asıllamadaki Zayıflık

##### 5.2.1.4.2 Tekrar Saldırısı

WEP te tekrar saldırıları için herhangi bir güvenlik önlemi yoktur. Aynı mesaj defalarca gönderilebilir ve bu alıcı tarafından anlaşılamaz. Bu zayıflığı açıklamak için bir örnek verilecek olursa: Sisteme giriş yapan bir kullanıcının mesajı asılayıcıya giderken dinlenebilir. Kullanıcı sistemden çıktıktan sonra dinlenilen mesajlar asıllayıcıya gönderilirse ara giren kişide kendini asıllatmış olacaktır. Burada önemli bir noktada olan araya girenin mesaj içeriğinin bilmesine gerek olmamasıdır. [119] [120] [121]

##### 5.2.1.4.3 Bit Flapping

Bu zayıflığın çıkış noktası ICV bütünlük kontrol verisinin oluşturulma şeklinden kaynaklanmaktadır. ICV lineer bir metotla oluşturulup asıl verinin sonuna eklenip şifrelenmektedir. Lineer bir metotla oluşturulduğu için şifreli olsa bile veri alanında bir değişiklik yapıldığında ICV de oluşacak değişiklik hesaplanabilmektedir. Bu zayıflığın oluşumu Şekil 5.2.1.4.3’de gösterilmiş ve aşağıda maddeler halinde belirtilmiştir. [119] [120]

**1)**Araya giren telsiz ağdan bir paket alır.

**2)**Dinlediği paketteki veri ve ICV alanlarını değiştirir.

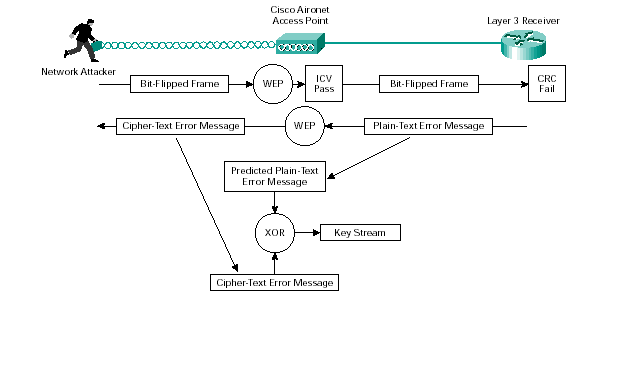
**3)** Bu paketi ağ dışına yollar.

**4)**Erişim noktası ICV değerini kontrol edip çerçeveyi gönderir.

**5)**3. katmanda CRC kontrol edilir ve belirli edilen bir hata döndürülür.

**6)**Erişim noktası bu hatayı şifreler ve gönderir.

**7)**Araya giren belirli hatanın hem şifreli hem de açık metnine sahip olur. Dar veya işlemi ile buradan akış şifresi elde edilir. [121]



Şekil 5.2.1.4.3: Bit Flapping

##### 5.2.1.4.4 IV’lerin Tekrar Kullanılması

IV nin kullanılma amacı aynı girişler olduğun da çıkışların oluşturulmak istenmesidir. IV nin 24 bit olduğunu 224 yaklaşık olarak 17 milyon farklı IV anlamına geldiğini biliyoruz. Tekrarlanmadan IV, 1 er artırarak kullanılsa bile. 802.11b standardına göre yaklaşık 7 saatte tüm IV ler kullanılmış olacaktır Aşağıdaki dar veya işlemi ve dilin yapısal özelliklerinde faydalanarak akış şifresi parça parça elde edilebilir. Ve akış şifresi çözüldükten sonra bu IV ile sahte çerçeveler oluşturulabilir. [119] [120] [121]



C şifreli metin, P açık metin, K akış şifresi

##### 5.2.1.4.5 RC4 Zayıf Anahtarlar Üretmesi (Fluhrer et al 2001) (FSM attack)

RC4 algoritması bazı anahtarlardan, zayıf akış şifreleri üretmektedir. Bu zayıflıktan faydalanarak şifrelenmiş metinden akış şifresini buradan da anahtarı elde etmek mümkün olabilir. [121]

#### 5.2.1.5 WEP Özet

* WEP tekrar saldırılarını önleyemez.
* WEP RC4 algoritmasında zayıf anahtarlar kullanılması şifreleme anahtarının ele geçmesine neden olabilir.
* WEP IV leri tekrar kullanır. Bazı kripto analiz yaklaşımları ile şifreleme anahtarı bilinmeden veri çözülebilir.
* ICV nin elde edilme yönteminin zayıflığı nedeni ile mesaj bütünlüğü araya giren tarafından bozulabilir. [119] [120]

### 5.2.2 WPA (Wireless Protected Access -2002)

Güvenlik standartları IEEE grupları tarafından belirlense bile bazı bölümler üretici şirketleri tarafından farklı gerçeklenebilir. Bu farklılığı önlemek ve üretilecek cihazların uyumluluğunu sağlamak için oluşturulan maddi amaç gütmeyen bir ortaklık kurulmuştur. Bu ortaklığın adı Wi-Fi’dır.

WEP deki kusurlar 2001 yılından beri açık bir şekilde biliniyordu. IEEE 802.11 deki sorunları çözecek standartları geliştirmek için çalışmalara başladı (802.11i) Fakat bu çalışmalar ancak 2004 te bitebileceği öngörülüyordu. Endüstrinin acil ihtiyacı için 802.11i standartlarına (draft 3.0) uygun geçici bir güvenlik sistemi Wi-Fi tarafından oluşturuldu. Ayrıca hızlı bir geçiş olacağı için maliyeti düşük, donanım değişikliği olmamalı idi. [121]

WPA, WEP in bilinen tüm zayıflıkları kapatılır. Donanım değişikliğine gidilmeden yükseltme yapılabiliyor. (Sürücü ya da firmware güncellemesi ile) WEP’e göre daha güçlü şifreleme Temporal Key Integrity Protocol (TKIP) ve asıllama (802.1x) yapısına sahiptir. Ayrıca WEP de olmayan anahtar yönetim mekanizmasına sahiptir. (802.1x), Aşağıda bu yeni özellikler açıklanacaktır. [119] [120]

#### 5.2.2.1 TKIP- Temporal Key Integrity Protocol

TKIP, RC4 akış şifreleyici algoritma üzerine kuruludur.4 yeni algoritma ile WEP şifreleme mekanizmasını sarar.

* IV 48 bite çıkarılmıştır ve paket numarası olarak kullanılmaktadır.
* Zayıf anahtarlar kullanılmamaktadır.
* Yeni bir mesaj bütünlük kontrol mekanizması MIC (Micheal) (Message integrity check)
* Anahtar eldesi ve dağıtımı ile yeni bir metot getirir. (802.1x)
* Her çerçeve için yeni bir anahtar oluşturulur.

Bu değişiklikler sayesinde kırılamayan bir mekanizma oluşturulması hedeflenmiştir. [119] [120]

#### 5.2.2.2 802.1x (EAP) ile Asıllama

802.1x EAP, IEEE nin EAP (Extensible Authentication Protocol) standartları üzerine kurduğu bir yapıdır. WLAN veya LAN larda kullanılmaktadır. Şekil 5.2.2.2’da sistemin işleyişi gösterilmiştir. Yapıdaki elemanlar ise

Supplicant

Asıllayıcı ya da Authenticator

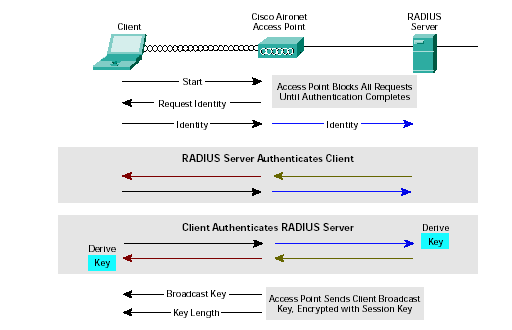
Asıllama Sunucusu (RADIUS Server) Remote Authentication Dial-In User Service

Adım adım sistemin çalışması incelenecek olursa

1. Kullanıcı Erişim noktasına başlangıç mesajı yollar.
2. Erişim Noktası kullanıcıdan kimlik bilgisi ister.
3. Kullanıcı kimlik bilgisini Asıllama sunucusuna gönderir.
4. Asıllama sunucusu asıllama işlemini gerçekleştirir. (Sayısal imza ya da başka yöntemlerle yapılabilir.)
5. Asıllama sunucusu kabul ya da ret cevabını Erişim Noktası gönderir.
6. Erişim Noktası bu cevabı kullanıcıya iletir ve kullanıcının ağa erişmesi için portlara izin verir.
7. Kullanıcı asıllama sunucusundan kimliğini ister.
8. Asıllayıcı sunucusu kimliğini kullanıcıya gönderir ve kullanıcı Asıllama Sunucusu asıllar ve veri trafiği başlar.

Görüldüğü gibi karşılıklı asıllama yapılmaktadır. Ayrıca Asıllama sunucusu ve kullanıcı tarafında bir Ana Anahtar üretilir. Bu anahtar daha sonra geçici anahtarların üretilmesinde kullanılacaktır. Bu anahtar Erişim Noktasına, asıllama sunucusu tarafından iletilir.

Eğer sistemde RADIUS yoksa paylaşılan anahtar üzerinden asıllamada desteklenmektedir. [119] [120]



Şekil 5.2.2.2: 802.1x ile Asıllama

#### 5.2.2.3 MIC (Message Integrity Code)

WEP teki ICV (integrity check value) nin zayıflıkları biliniyordu. WPA ile Michael olarak bilinen bir yöntem, 8 baytlık bir ileti bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir. Üretilmesi ise alıcı ve gönderen MAC adresleri ve mesaj bir hash fonksiyonuna tabi tutulur ve 8 byte lık bir çıktı oluşur. MIC, IEEE 802.11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir ve daha sonra çerçeve verileri ve ICV ile birlikte şifrelenir. MIC lineer bir algoritma ile edilmeyği için ICV gibi zayıflıkları yoktur. Bu da araya giren kişinin mesajı değiştirdiğinde anlaşılmasını sağlar. Şekil 5.2.2.3’da MIC yapısı gösterilmektedir. [119] [120] [121]

DA SA PAYLOAD

Anahtar

MIC

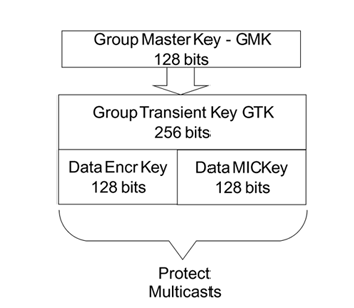
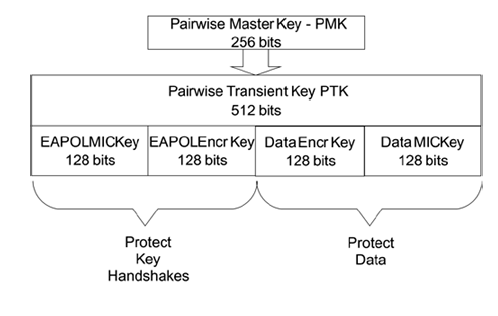
Şekil 5.2.2.3: MIC Mesaj Bütünlük Kontrolu

#### 5.2.2.4 Anahtar Yönetimi

WEP den önemli bir fark olarak Anahtar yönetimi gösterilebilir. WPA da 2 çeşit anahtar yapısı vardır.

1. Oturum Anahtar kümesi:2 telsiz cihazın haberleşmesinde kullanılır Genelde bir kullanıcı ve erişim noktası arasında kullanılır. (Unicast haberleşmeler)
2. Grup Anahtar kümesi: Ağ içinde herkesin bildiği ve yayım (braoadcast) yapılması için kullanılan anahtarlar. (Multicast)

Anahtarların bir özelliğide hiyerarşik bir yapıya sahip olmalarıdır. Şekil 5.2.2.4’de bu hiyerarşik gösterilmiştir.



Şekil 5.2.2.4: Oturum ve Grup Anahtarları Hiyerarşik Yapısı

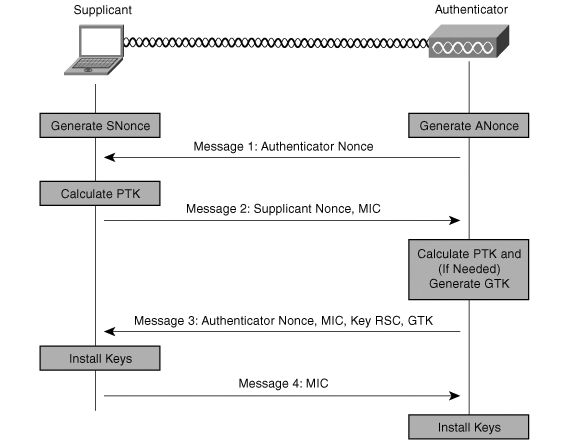
Oturum ana anahtarı ve grup ana anahtarı, ana anahtardan elde edilir. Ana anahtar da daha önceki bölümlerde belirttiğimiz gibi asıllama sırasında asıllama sunucusu tarafından üretilmiştir. Oturum ana anahtarı elde edilen anahtarlar geçicidir. Her yeni cihaz la bağlantı yeniden kurulduğunda ya da ağdan çıkılıp girildiğinde yeniden oluşturulur. Üretilen anahtarların ilk ikisi n grup anahtarları eldesinde, diğer ikisi ise şifreleme ve veri bütünlüğü için kullanılır.

Grup Ana Anahtarları da grup geçici anahtarı ile Erişim Noktaları tarafından belirlenip kullanıcılara dağıtılmaktadır. [119] [120] [121]

##### 5.2.2.4.1 Oturum Anahtar Kümesinin Üretilmesi

Bu anahtar kümesinin eldesi Erişim Noktası ve kullanıcı arasında belirlenir Belirlenme biçimi Şekil 5.2.2.4.1’de gösterilmiş ve aşağıda açıklanmıştır.

1. Erişim noktası rasgele sayı üretir ve kullanıcıya yollar.
2. Kullanıcı rasgele bir sayı belirler ve geçici anahtarları elde edip, rasgele sayıyı EN na yollar. MIC PMK anahtarını bildiğinin kanıtıdır. EN geçici anahtarları hesaplar
3. Buradan gerekirse grup anahtarlarını da hesaplayıp kullanıcıya gönderir.
4. Kullanıcı MIC i onayladıktan sonra anahtarları kullanmaya başlar ve bunu 4. mesaj ile bildirir.
5. EN de bu mesajı aldıktan sonra anahtarları kullanmaya başlar.



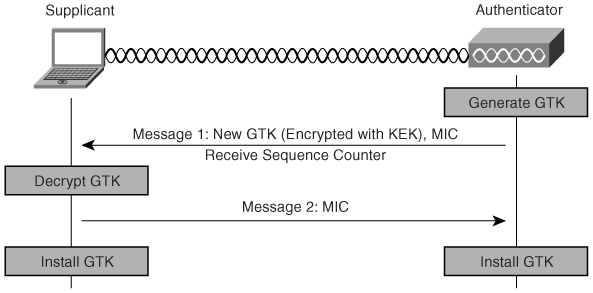
Şekil 5.2.2.4.1: Oturum Anahtarı Kümesi Eldesi

##### 5.2.2.4.2 Grup Anahtar Kümelerinin Üretilmesi

Tüm ağın haberleşileceği için farklı olan oturum anahtarları kullanılamaz. Herkesin paylaştığı bir anahtar olmalıdır ve buda grup anahtarlarıdır. Grup anahtar kümesinin eldesi Şekil 63’te gösterilmiş ve aşağıda açıklanmıştır.

1. Oturum anahtarları kümesi hesaplandıktan sonra, EN Grup geçici anahtarını kendi oluşturur.
2. Bir önceki aşamada elde edilmiş olan oturum şifreleme anahtarı ile şifreleyip kullanıcıya gönderir. MIC burada mesaj bütünlüğünü sağlar. Sayaç ise tekrar saldırılarını önlemek içindir.
3. Kullanıcı Grup geçici anahtarını şifreyi çözerek elde eder ve kullanmaya başlar.

EN’na sayacı bir artırarak MIC ile birlikte gönderir, EN de Grup geçici anahtarını kullanmaya başlar. [121]



Şekil 5.2.2.4.2: Grup Anahtarı Kümesi Eldesi

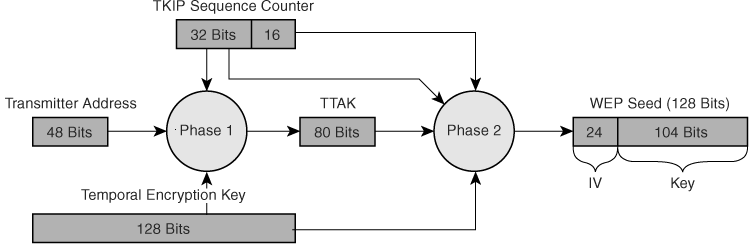
##### 5.2.2.4.3 Farklı Anahtar Üretimi

WEP te aynı anahtar ile şifrelenmiş çerçevelere dayalı saldırılar yapılabilmekteydi. WPA da bu saldırıları engellemek için her paket farklı anahtarlar üretilmesi öngörülmüştür.

Yeni anahtar hesaplamaları 2 aşamada gerçeklenir.2 aşama olmasının nedeni WEP tabanlı cihazların yüksek işlem yapabilme kapasitenden yoksun olması ve işlem sayısını en aza indirgenmek istenmesidir.

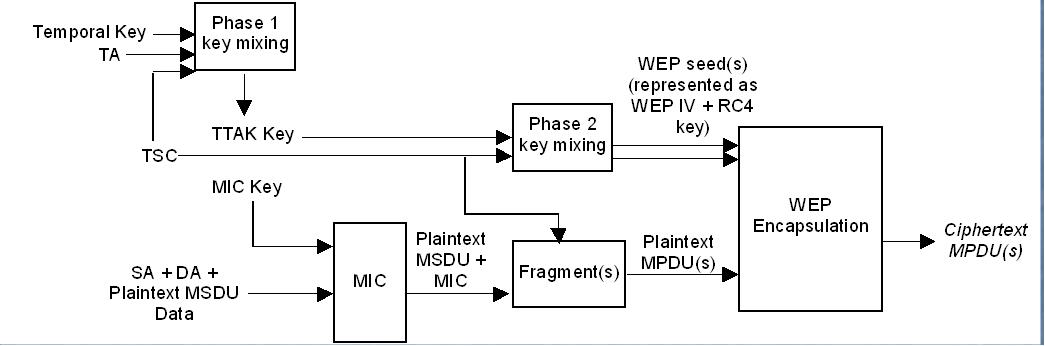
1. aşamada ileticinin MAC adresi, oturum ana anahtarından türetilen geçici oturum anahtarı ve IV değerinin yüksek anlamlı 32 biti DAR VEYA VE ve S-BOX lar gibi işlemlerden geçirilerek 80 bitlik ara anahtar elde edilir. Bu aşama 216 da bir çalışması yeterlidir. Çünkü sadece o periyotta farklı değerler üretir.2. aşamada ise bu 80 bitlik ara anahtar ile IV nin düşük anlamlı 16 biti kullanılır. Buradan 104 bitlik anahtar elde edilir.24 bitlik IV değeri IV nin düşük anlamlı bitlerinden türetilir.

Burada MAC adresinin kullanılma sebebi eğer A ve B, IV değerlerini 0’dan başlatacak olurlarsa kısa zamanda IV çatışması yaşanması engellemektir. Şekil 5.2.2.4.3’de farklı anahtar üretimi görülmektedir. [119] [120] [121]



Şekil 5.2.2.4.3: Farklı Anahtar Üretimi

TKIP in genel yapısına bakılacak olursa farklı anahtar üretme ile anahtar elde edilir. Mesaj bütünlük kodu hesap edilir ve mesajın sonuna eklenir. Mesaj parçalara ayrılır. Parçalar IV ve anahtardan elde edilmiş akış şifresi ile şifrelenir ve alıcıya gönderilir. [119] [120] [121]



DA – Destination Address TKIP – Temporal Key Integrity Protocol

ICV– Integrity Check Value TSC – TKIP Sequence Counter

MPDU – Message Protocol Data Unit TTAK– result of phase 1 key mixing of Temporal Key

MSDU – MAC Service Data Unit and Transmitter Address

WEP – Wired Equivalent Privacy

SA – Source Address WEP IV – Wired Equivalent Privacy Initialization Vector

TA – Transmitter Address initializatiion vector

Şekil 5.2.2.4.3.a: TKIP Yapısı

Buraya kadar WPA’nın özelliklerini gördük. Tablo 5.2.2.4.3 ’da WPA’nın WEP üzerindeki üstünlükleri gösterilmektedir.

|  |  |  |
| --- | --- | --- |
|  | **WEP** | **WPA** |
| **Şifreleme** | Şifreleme yapısı kırıldı.  RC4 algoritması | WEP in açıklarını kapatıyor.  TKIP/RC4 algoritması |
| **Anahtar Uzunluğu** | 40 bitlik | 128 bitlik |
| **IV uzunluğu** | 24 bitlik | 48 bitlik |
| **Anahtar Değişikliği** | Anahtar değişimi yoktur. | Anahtarlar her oturum, her paket için değişir. |
| **Anahtar yönetimi** | Anahtar yönetimi yoktur | 802.1x |
| **Asıllama** | Zayıf bir yöntem | 802.1x EAP ile güçlü bir yöntem |
| **Veri Bütünlüğü** | ICV | MIC |

Tablo 5.2.2.4.3: WEP ve WPA karşılaştırması

### 5.2.3 RSN (Robust Security Network, IEEE 802.11i, WPA2) 2004

WPA günümüzde kırılmamış olsa da WEP tabanlı bir yapı olduğu ve eksiklerinin çıkabileceği şüphesinden dolayı (RC4 algoritmasının zayıflıkları) IEEE 802.11 i standartlarına uygun yeni bir protokol geliştirilmiştir. Bu protokol WEP üzerine kurulmamış yeni ve farklı bir yapı olarak geliştirtmiştir. Standartlaşması 2004 Mayıs’ta tamamlanmıştır.2004 Ekim’den itibaren bunu destekleyen ürünler üretilmeye başlanmıştır. RSN WPA yı desteklemekte fakat WEP i desteklememektedir. Çünkü WEP i artık bir güvenlik unsuru olarak görülmemektedir. Piyasadaki ürünler WPA dan RSN e geçişi desteklememektedir çünkü farklı donanımsal özellikler gereklidir.

RSN asıllamayı ve anahtar yönetimini IEEE 802.1X standartları ile gerçekler. Veri bütünlüğü MIC ile sağlanır. Roaming sağlar. Gezginlik gerçek zamanlı iletişimlerde önem kazanır çünkü veri kaybını engeller. RSN gezginliği iki farklı şekilde gerçekler.

* Önceden asıllama: Öncende asıllamada kullanıcı bir erişim noktasına bağlı iken diğer bir erişim noktasının varlığının farkına varırsa 802.1x anahtar değişimi ile bu erişim noktası için de anahtarları elde eder ve saklar. Sinyal zayıflığı gibi nedenlerden önceden anahtarını elde ettiği EN na geçmek isterse 802.1x işlemlerini yapmaya kalmaz.
* Anahtar önbellekleme: Erişim noktası ile daha önceden anahtar belirlendi ise bu anahtarlar bellekte saklanır. Bu erişim noktası ile iletişime geçildiğinde 802.1x işlemlerini yapmaya kalmaz.

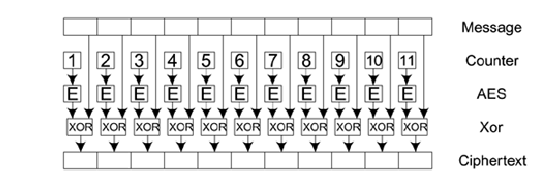
RSN de şifreleme Temporal Key Integrity Protocol (TKIP) veya Counter Mode with CBC-MAC Protocol (CCMP) ile gerçeklenir. CCMP zorunlu iken, TKIP ise seçeneklidir. [56] [119] [120] [121]

#### 5.2.3.1 CCMP (Counter Mode –CBC MAC Protocol)

CCMP içinde şifreleme algoritması AES (Advanced Encryption Standart) kullanır. AES güvenilir ve hızlı bir algoritmadır. Simetrik anahtar kullanır. CCMP içinde seçilen kullanım modu Counter Mode with CBC-MAC (CCM)dir. AES in birçok kullanım modu vardır. CCMP içinde olan kullanım modlarına bakacak olursak;

##### 5.2.3.1.1 Counter Mode:

Sayaç yönteminin kullanılma amacı aynı veri içeren bloklar aynı şifre ile şifrelendiğinde farklı çıkışların olmasının istenmesidir. Çünkü mesajın tekrar eden bloklardan oluştuğunun bilinmesi bir zayıflıktır. Şekil 5.2.3.1.1’da Counter mode gösterilmiştir.



Şekil 5.2.3.1.1: AES counter (sayaç) çalışma modu

Şekilden de görüldüğü gibi veri blokları şifrelenmiş sayılar ile dar veya işlemine tutulmaktadır. Burada kullanılan sayılar rasgele seçilmektedir çünkü aynı iki mesaj aynı çıkışları verecektir. Bu sayının başlangıcı karşı tarafa iletilmelidir. Bu modda 128 bitlik şifreleme anahtarı kullanılır. [121]

##### 5.2.3.1.2 CBC- MAC Mode:

CBC-MAC modu ise MIC hesabında kullanılır. Eğer mesajda 1 bit değişirse MIC de büyük değişiklikler olur ve tahmin edilemez. MIC hesabı geri dönülmez bir şekilde yapıldığı için araya girenin mesaja uygun bir MIC hesaplaması mümkün değildir. Aşağıda MIC in hesaplanma yöntemi verilmiştir.

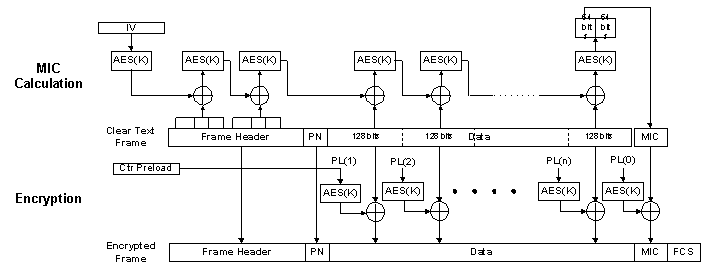
1. İlk veri bloğunu al ve AES i kullanarak şifrele.
2. Sonuç ile 2. bloğu dar veya işlemine tut ve şifrele
3. Çıkan sonucu bir sonraki blok ile dar veya işlemine tut ve şifrele

Şifreleme yöntemi adını bu iki modun birleşiminden almaktadır.

CBC- MAC + Counter mode = CCM

CCMP çalışma yapısına bakacak olursak öncelikle MIC hesabı için CBC-MAC (Cipher block chaninig message authentication code) kullanılır. Buradan oluşan 128 bitin 64 biti kullanılır.

Mesajın şifrelenmesinde de sayaçtan bir değer alınır ve AES algoritması ile şifrelenip daha sonra çıkan sonuç mesajın 128’lik ilk bloğu ile dar veya işleminden geçer. Daha sonraki bloklarda sayaç birer arttırılarak elde edilen sayılar kullanılarak şifrelenir. Şekil 5.2.3.1.2’de CCMP çalışma biçimi gösterilmiştir. [119] [120] [121]



Şekil 5.2.3.1.2: CCMP Çalışma Yapısı

|  |  |  |  |
| --- | --- | --- | --- |
|  | **WEP** | **WPA** | **RSN** |
| **Şifreleme** | Şifreleme yapısı kırıldı.  RC4 algoritması | WEP in açıklarını kapatıyor. TKIP/RC4 | CCMP/AES  CCMP/TKIP |
| **Şifreleme Anahtarı** | 40 bitlik anahtar | 128 bitlik anahtar | 128 bit |
| **IV** | 24 bit | 48 bit | 48 bit |
| **Anahtar Değişikliği** | Anahtar sabittir. | Anahtarlar her oturum, her paket için değişir. | Anahtar değişikliğine gerek yoktur. |
| **Anahtar yönetimi** | Anahtar yönetimi yoktur | 802.1x | 802.1x |
| **Asıllama** | Zayıf bir yöntem | 802.1x EAP | 802.1x EAP |
| **Veri Bütünlüğü** | ICV | MIC | MIC |

Tablo 5.2.3.1.2: WEP, WPA ve RSN Karşılaştırması5.3. Kablolu Ağlarda Güvenlik Protokolleri

### 5.3.1 Application Layer Güvenlik Protokolleri

#### 5.3.1.1 PGP (Pretty Good Privacy)

##### ****5.3.1.1.1 PGP Nedir?****

PGP Phil Zimmermann tarafından geliştirilmiş bir e-mail ve dosya şifreleme protokolüdür. [IDEA](http://www.bilgisayarkavramlari.com/2009/06/11/idea-uluslar-arasi-sifreleme-algoritmasi/),[RSA](http://www.bilgisayarkavramlari.com/2008/03/19/rsa/), DSA, MD5, [SHA-1](http://www.bilgisayarkavramlari.com/2009/11/02/secure-hasing-algorithm-sha/) gibi şifreleme algoritmalarını bünyesinde barındırır. PGP protokolünün veri trafiğinin korunmasıyla bir ilgisi yoktur. PGP’nin amacı sadece dosya ve e-maillerin korunmasıdır. PGP nin Dünya’daki en yaygın e-mail şifreleme protokolü olduğu söylenebilir. Bunu sebebi PGP’de verilerin karşılıklı kontrollerden geçtikten sonra erişilebilir duruma gelmesidir. PGP açık kaynak kodlu çalışmakta ve bu özelliği sayesinde he zaman geliştirilebilir durumdadır. Dünya’daki en güvenli protokollerden biridir. [98]

##### ****5.3.1.1.2 PGP’nin Çıkışı****

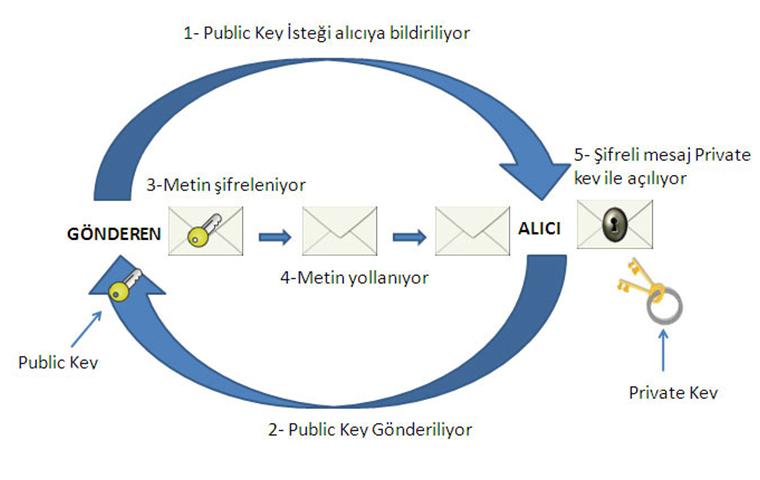
Phil Zimmermann 1991 yılında PGP’nin ilk sürümünü ücretsiz olarak piyasaya çıkarmıştır. PGP piyasaya çıktıktan sonra ABD hükümeti PGP’yi incelemiş ve ihracat yasalarını ihlal ettiği gerekçesiyle Zimmermann aleyhine soruşturma başlatmıştır. Bu soruşturma 3 yıl süreyle devam etmiş sonunda Zimmermann aklanmıştır. PGP’nin çözümünün çok zor olduğunu anlayan ABD hükümeti güvenlik açısından PGP’nin yurt dışına çıkmasını yasaklamıştır. Zimmermann PGP’yi, gerçek bir güvenlik ve kişisel haklara saygı istediğinden dolayı yazdığını “Why I wrote PGP” isimli yazısında açıklamıştır. [98]

##### ****5.3.1.1.3 PGP’nin Çalışma Prensibi****

PGP asimetrik/genel bir şifreleme protokolüdür. PGP tek bir anahtar yerine public ve private key kullanır. Bu iki anahtar birbirlerinin tanıyıcılarıdır. Bildiğimiz gibi bir public key ile şifrelenmiş veri ancak o anahtarın private keyi ile açılabilir. Bunun tam tersi olarak private key ile şifrelenmiş veriyi de ancak o anahtarın private keyiyle açılabilir. Bunun PGP’ye uyarlanması şöyledir; biri bize şifreli bir mail yollamak istiyorsa bizim private keyimize sahip olmalıdır. Private keye sahip olmadan bize şifreli mesaj yollayamaz. PGP’nin sağladığı bir diğer özellikise şudur; gönderici bizim Private keyimize sahip olsa bile bize gönderilen mesajları okuyamaz. Buna bize gönderdiği mesajda dahildir. Bizim public keyimizle şifrelenmiş bir maili açmanın tek yolu private keyimizi bilmektir. [98]

PGP ile şifreli mail gönderme işlemi şöyle gerçekleşir;

1. Mail gönderecek olan kullanıcı alıcı tarafın public keyini talep eder.
2. Talep üzerine alıcı public keyini alıcı tarafa yollar.
3. Public keye sahip olan gönderici mailini gönderilen public keyle şifreler ve alıcıya gönderir.
4. Şifrelenmiş mesajı alan alıcı kendisinin private keyi sayesinde şifrelenmiş maili deşifre eder. [98]



Şekil ****5.3.1.1.3****: PGP’nin Çalışma Prensibi

Anlaşıldığı üzere korsanlar gönderilen şifreli maili ele geçirse bile mail sadece alıcıda bulunan private key ile açılabileceği için boşa çabalamış oluyorlar. Aklımıza gelen bir diğer olumsuz koşul ise maili gönderecek olan kişiye gönderilen public keyin ele geçme olasılığı. PGP nin ön önemli özelliği zaten bu durumda ortaya çıkıyor. Yukarda devamlı olarak bahsettiğimiz public ve private keylerin her birinin sadece bir görevi var. [Public key](http://www.bilgisayarkavramlari.com/2008/03/19/acik-anahtarli-sifreleme-public-key-cryptography/) sadece maili şifrelemeye yarıyor, şifreyi açamıyor. Bu nedenle public key ele geçirilse bile deşifreleme açısından bir işe yaramaz. Zaten PGP’ye asimetrik özelliğini bu durum katmaktadır. [98]

PGP’de şifreleme üç adımda gerçekleşmektedir. Birinci adımda gönderen, mesajın özünü imzalar. İkinci adımda mesaj sıkıştırılır. Üçüncü ve son adımda ise mesaj şifrelenir. Alıcı taraf mesajı açmak istediğinde bu adımları tersten uygulamalıdır. PGP şifreleme algoritmaları olarak RSA ve IDEA algoritmalarını kullanmaktadır. Mesajın özü alınırken ise [MD5 algoritması](http://www.bilgisayarkavramlari.com/2008/04/30/md5-message-digest-mesaj-ozet/) kullanılır**.** [98]

##### ****5.3.1.1.4 PGP’nin Güvenliği****

PGP çok güvenli bir şifreleme algoritması olarak bilinir. Fakat yinede PGP yi zora sokabilecek bazı işlemler bulunmuş ve önlenilmiştir. Bunları şu şekilde sıralayabiliriz;

* Mesaj şifrelenmiş, imzalanmış bile olsa internet dinlenilerek mesaj kopyalanabilir. Daha sonra bu mesajı tekrar alıcıya gönderilir. Kopyalanan mesajın üzerindeki şifre ve imza doğru olduğu için alıcı mesajın gönderenden geldiğini zannedecektir. Bu durumu engellemek için PGP’de mesajın başına time stamp konur. Böylece alıcı mesaj ne zaman yollanıldığı hakkında bili sahibi olarak güvenliğini sağlamış olur.
* Gönderen çok gizli bir mesajı şifreleyip yolladıktan sonra mesajın yalın hali hala bilgisayarında mevcut olacaktır. Gönderen normal olarak bu mesajı silmek isteyecektir. Fakat bilgisayarlardaki silme işlemleri geri dönüşümlü işlemlerdir. PGP bu sorunu şifrelemeden sonra mesajın içeriğini tamamen “0” ile dolduraraktan çözüm bulmaktadır. [98]

#### 5.3.1.2 S/MIME (Secure Multi-Purpose Internet Mail Extensions)

S/MIME (Secure Multi-Purpose Internet Mail Extensions), Rivest-Shamir-Adleman şifreleme sistemini kullanan, e-posta göndermenin güvenli bir yöntemi olarak karşımıza çıkmaktadır. S / MIME, Microsoft ve Netscape'den gelen Web tarayıcılarının en son sürümlerine dahildir ve mesajlaşma ürünlerini üreten diğer satıcılar tarafından onaylanmıştır. RSA, Internet Engineering Task Force (IETF) gibi kurumlar S / MIME'yi bir standart olarak önerdi. S/MIME'ye bir alternatif de standart olarak önerilen PGP / MIME'dır.

MIME'nin kendisi, IETF standartlarında Request for Comment 1521 olarak adlandırılmıştır ve elektronik mesajın nasıl düzenleneceğini açıklar. S/MIME de, şifreleme bilgisinin ve dijital sertifikanın ileti gövdesinin parçası olarak nasıl eklenebileceğini tanımlar. Ayrıca S/MIME, Public-Key Cryptography standart biçimi # 7'de verilen sözdizimini izler. [97]

#### 5.3.1.3 S-HTTP (Secure HTTP)

S-HTTP, World Wide Web'de dosyaların güvenli bir şekilde değiş tokuşuna izin veren Köprü Metni Aktarım Protokolünün (HTTP) bir uzantısıdır. Her bir S-HTTP dosyası şifrelidir, bir dijital sertifika içerir veya her ikisi de. Belirli bir belge için, S-HTTP, başka bir tanınmış güvenlik protokolüne, Secure Sockets Layer'a (SSL) bir alternatiftir. En büyük fark, S-HTTP'in istemcinin kullanıcının kimliğini doğrulamak için bir sertifika göndermesine izin vermesine izin verirken, SSL kullanıldığında yalnızca sunucu doğrulanabilir. S-HTTP, sunucunun bir bankayı temsil ettiği durumlarda ve kullanıcı kimliği ve paroladan daha güvenli olan kimlik doğrulamasını gerektiren durumlarda kullanılır. [99]

S-HTTP tek bir şifreleme sistemi kullanmaz, ancak Rivest-Shamir-Adleman açık anahtar altyapısı şifreleme sistemini desteklemez. SSL, İletim Denetimi Protokolü (TCP) düzeyinden biraz daha yüksek bir program katmanında çalışır. S-HTTP, HTTP uygulamasının daha üst düzeyinde çalışır. Her iki güvenlik protokolü bir tarayıcı kullanıcısı tarafından kullanılabilir, ancak yalnızca bir tanesi belirli bir belgede kullanılabilir. Terisa Systems, İnternet güvenlik araç kitlerinde hem SSL hem de S-HTTP'yi içerir. [99]

Birçok popüler Web sunucusu hem S-HTTP hem de SSL'yi desteklemektedir. Yeni tarayıcılar hem SSL'yi hem de S-HTTP'yi desteklemektedir. S-HTTP, standart olarak dikkate alınması için Internet Mühendislik Görev Gücü'ne (Internet Engineering Task Force-IETF) gönderilmiştir. Request for Comments (RCFs) internet taslak 2660, S-HTTP'yi ayrıntılı olarak açıklamaktadır. [99]

#### 5.3.1.4 HTTPS (HTTP over SSL or HTTP Secure)

HTTPS (SSL üzerinden HTTP veya HTTP Güvenli), düzenli HTTP uygulama katmanlamasında alt katman olarak Güvenli Soket Katmanı (SSL) veya Aktarım Katmanı Güvenliği'ni (TLS) kullanmaktır. HTTPS, kullanıcı sayfasının isteklerini ve Web sunucusu tarafından döndürülen sayfaları şifreler ve şifresini çözer. HTTPS kullanımı gizlilik ve ortadaki adam saldırılardan korur. HTTPS, Netscape tarafından geliştirildi. [100]

HTTPS ve SSL, sunucudan X.509 dijital sertifikaların kullanılmasını destekler, böylece gerekirse bir kullanıcı gönderenin kimliğini doğrulayabilir. Farklı bir bağlantı noktası belirtilmediği sürece, HTTPS alt katman TCP / IP ile olan etkileşiminde HTTP bağlantı noktası 80 yerine 443 numaralı bağlantı noktasını kullanır. [100]

Çevrimiçi kataloğunu görüntülemek için bir Web sitesini ziyaret ettiğinizi varsayalım. Sipariş vermeye hazır olduğunuzda, https: // ile başlayan Tekdüzen Kaynak Konum Belirleyicisi (URL) içeren bir Web sayfası sipariş formu verilecektir. Sayfayı katalog satıcısına geri göndermek için "Gönder" e tıkladığınızda, tarayıcınızın HTTPS katmanı onu şifreleyecektir. Sunucudan aldığınız onay, ayrıca şifreli biçimde gezinecek, bir https: // URL'si ile gelecek ve sizin tarayıcınızın HTTPS alt katmanı tarafından şifresi çözülecek. [100]

HTTPS'nin etkinliği, tarayıcı veya sunucu yazılımının yetersiz uygulanması veya bazı algoritmalar için bir eksiklik nedeniyle sınırlı olabilir. Ayrıca, HTTPS, verilerin sunucu ile istemci arasında dolaşırken güvenliğini sağlamasına karşın, veriler bir defada hedefe şifre çözüldükten sonra, yalnızca ana bilgisayar kadar güvenli olur. [100]

#### 5.3.1.5 Secure Electronic Transaction (SET)

Güvenli Elektronik İşlem (Secure Electronic Transaction-SET), finansal işlemlerin internet üzerinde güvenliğini sağlamak için bir sistemdir. Başlangıçta Mastercard, Visa, Microsoft, Netscape ve diğerleri tarafından desteklenmiştir. SET ile bir kullanıcıya bir elektronik cüzdan verilir (dijital sertifika) ve alıcı, bir tüccar ve alıcı bankası arasında dijital sertifika ve dijital imza kombinasyonu kullanılarak bir gizlilik ve gizlilik sağlayacak bir işlem gerçekleştirip, doğrulama yapılır. SET, Netscape'in Güvenli Yuva Katmanı (Secure Sockets Layer-SSL), Microsoft'un Güvenli İşlem Teknolojisi (Secure Transaction Technology-STT) ve Terisa Sisteminin Güvenli Köprü Metni Aktarım Protokolünü (Secure Hypertext Transfer Protoco-S-HTTP) kullanmaktadır. SET, bir kamu anahtarı altyapısının (Public Key Infrastructure PKI) tüm özelliklerini değil ancak bir kısmını kullanmaktadır. [101]

SET'in işlevi şu şekildedir:

Bir müşterinin, Netscape veya Microsoft'un Internet Explorer gibi SET özellikli bir tarayıcısı olduğunu ve işlem sağlayıcısının (banka, mağaza vb.), SET özellikli bir sunucusu bulunduğunu varsayalım.

1. Müşteri bir Mastercard veya Visa banka hesabı açar. Herhangi bir kredi kartı ihracı, bir çeşit bankadır.
2. Müşteri bir dijital sertifika alır. Bu elektronik dosya, çevrimiçi satın alma işlemleri veya diğer işlemler için bir kredi kartı gibi işlev görür. Son kullanma tarihine sahip bir genel anahtar içerir. Geçerliliğini sağlamak bankaya dijital olarak geçirilir.
3. Üçüncü taraf tacirler de bankadan sertifika alır. Bu sertifikalar, tüccarın açık anahtarını ve bankanın genel anahtarını içerir.
4. Müşteri bir Web sayfasında, telefonla veya başka yollarla sipariş verir.
5. Müşterinin tarayıcısı, tüccarın geçerli olduğunu tüccarın sertifikasından alır ve teyit eder.
6. Tarayıcı, sipariş bilgilerini gönderir. Bu mesaj, tüccarın genel anahtarı, bankanın genel anahtarı (tüccar tarafından okunamayan) ile şifrelenmiş ödeme bilgileri ve ödeme yapılmasını sağlayan bilgilerin yalnızca bu siparişle kullanılabileceği şekilde şifrelenir.
7. Tüccar, müşterinin sertifikasındaki dijital imzayı kontrol ederek müşteriyi doğrular. Bu sertifika bankaya veya üçüncü parti doğrulayıcıya yönlendirilerek de yapılabilir.
8. Tüccar sipariş mesajını bankaya gönderir. Bu, bankanın genel anahtarını, müşterinin ödeme bilgilerini (tüccarın şifresini çözemez) ve tüccarın sertifikasını içerir.
9. Banka tüccar ve mesajı doğruluyor. Banka, mesajdaki sertifika üzerindeki dijital imzayı kullanır ve mesajın ödeme kısmını doğrular.
10. Banka, dijital olarak imzalar ve tüccara yetkilendirme gönderir ve tüccar siparişini doldurabilir. [101]

#### 5.3.1.5 Kerberos

Windows 2000'den bu yana Microsoft, Kerberos protokolünü Windows'ta varsayılan kimlik doğrulama yöntemi olarak dahil etti ve Windows Active Directory hizmetinin ayrılmaz bir bileşeni haline getirdi. Geniş bant servis sağlayıcıları, ağlarına erişen DOCSIS kablo modemlerini ve set üstü kutuları doğrulamak için Kerberos'u da kullanıyor.

Kerberos aslen Athena Projesi için Massachusetts Institute of Technology'de (MIT) geliştirildi. Kerberos adı Yunan mitolojisinden alınmıştır; Kerberos (Cerberus), Hades'in kapılarını koruyan üç başlı bir köpekti. Kerberos protokolünün üç başkanı bir istemci, bir sunucu ve Kerberos'un güvenilir üçüncü parti kimlik doğrulama hizmeti olarak işlev gören bir Anahtar Dağıtım Merkezi (KDC) temsil etmektedir.

Kerberos kullanan kullanıcılar, makineler ve hizmetler yalnızca tek bir işlemle çalışan ve iki hizmet sunan KDC'ye güvenmek zorundadır: kimlik doğrulama hizmeti ve bilet verme hizmeti. KDC "biletleri", düğümlerin kimliğini birbirlerine güvenli bir şekilde kanıtlamasına izin veren karşılıklı kimlik doğrulama sağlar. Kerberos kimlik doğrulaması, ağ üzerinden geçen paketlerin okunmasını ya da değiştirilmesini önlemek için geleneksel paylaşılan gizli şifreleme yöntemini kullanır ve iletileri dinlemeden ve tekrar dinlemeden korumak için kullanılır.

##### 5.3.1.5.1 Kerberos’un Çalışma Prensibi

Kerberos'un nasıl çalıştığını gösteren basit bir açıklama yapacak olursak;

Gerçek süreç daha karmaşıktır ve bir uygulamadan diğerine farklılık gösterebilir. Bu tartışmanın amaçları için, aşağıdaki senaryoda başlatıcı müşterimiz, Windows çalıştıran kurumsal bir dizüstü bilgisayardır ve son kullanıcı kurumsal ağa giriş yapmaya çalışmaktadır.

Kerberos kimlik doğrulama işlemini başlatmak için, başlatan istemci bir servise erişmek için bir kimlik doğrulama sunucusuna bir istek gönderir. İstekte hassas bilgi bulunmadığından, ilk istek salt metin olarak gönderilir.

Kimlik doğrulama sunucusu, başlatan müşterinin kullanıcı adı KDC veritabanında olduğu varsayılarak, başlatan istemcinin özel anahtarını alır. Başlatan istemcinin kullanıcı adı KDC veritabanında bulunamazsa, istemci kimlik doğrulaması yapılamaz ve kimlik doğrulama işlemi durdurulur. İstemcinin kullanıcı adı KDC veritabanında bulunabilirse, kimlik doğrulama sunucusu bir oturum anahtarı ve bilet verme bileti oluşturur. Bilet verilen bilet, başlangıç ​​talebinin şifresiyle birlikte kimlik doğrulama sunucusu tarafından zaman damgalı olarak şifrelenir. İstek, istekte bulunur.

Başlangıç müşterisine bir şifre girilmesi istenir, grilen şifre KDC veritabanındaki parolayla eşleşirse, kimlik doğrulama sunucusundan gönderilen şifreli bilet sağlayıcı şifresi çözülür ve istenen hizmet için bilet verme sunucusundan bir kimlik bilgisi istemek için kullanılır. İstemci, fiziksel olarak kimlik doğrulama sunucusu ile aynı donanımda çalışan, ancak farklı bir rol gerçekleştiren bilet verme sunucusuna, bilet verme bileti gönderir.

Bilet verme hizmeti, kimlik doğrulama sunucusu tarafından yapılana benzer bir kimlik denetimi gerçekleştirir, ancak bu kez kimlik bilgilerini ve istenen hizmete erişmek için bir bilet gönderir. Bu iletim, erişilen kullanıcıya ve servise özgü bir oturum anahtarı ile şifrelenir. Bu kanıt belgesi, bir zamanlar orijinal talebin doğrulanmasıyla talep edilen sisteme kimliğini doğrulayacak istenen "Kerberlenmiş" hizmete erişmek için kullanılabilir. [102]

Bilet verme hizmeti tarafından gönderilen zaman damgalı bilet, talep eden sistemin yeniden kimlik doğrulaması yapılmaksızın belirli bir süre tek bir bilet kullanarak servise erişmesine izin verir. Biletin sınırlı bir zaman diliminde geçerli hale getirilmesi, bir başkasının daha sonra kullanmasına imkân tanımaz; Maksimum ömrü 0 olarak ayarlamak mümkündür, bu durumda servis biletlerinin süresi geçmez. Microsoft, servis biletleri için maksimum ömrü 600 dakikalık önerir; Kerberos'un Windows Server uygulamalarında varsayılan değer budur.

MIT Kerberos Konsorsiyumu Eylül 2007'de Kerberos'u geliştirmek için kuruldu. 2013'te konsorsiyum genişletildi ve MIT Kerberos ve Internet Güven Konsorsiyumu olarak yeniden adlandırıldı. [102]

### 5.3.2 Transport Layer Security Protocols

#### 5.3.2.1 SSL VPN (Secure Sockets Layer Virtual Private Network)

SSL VPN (Güvenli Yuva Katmanı sanal özel ağ), standart bir Web tarayıcısı ile kullanılabilen bir VPN biçimidir. Geleneksel Internet Protocol Security (IPsec), VPN’nin aksine, SSL VPN, son kullanıcının bilgisayarında özelleştirilmiş istemci yazılımının yüklenmesini gerektirmez. Uzak kullanıcılara Web uygulamalarına, istemci / sunucu uygulamalarına ve dahili ağ bağlantılarına erişmek için kullanılır. [103]

VPN, iki uç nokta arasında iletilen veri ve diğer bilgiler için güvenli bir iletişim mekanizması sağlar. SSL VPN, kullanıcının Web tarayıcısını kullanarak bağladığı bir veya daha fazla VPN aygıtı içerir. Web tarayıcısı ile SSL VPN cihazı arasındaki trafik, SSL protokolü veya onun halefi olan Transport Layer Security(TLS) protokolüyle şifrelenir.

Bir SSL VPN, çok sayıda bilgisayardaki bir dizi kullanıcıya, çok yönlülük, kolay kullanım ve ayrıntılı kontrol sağlar, birçok lokasyondaki kaynaklara erişir. İki büyük SSL VPN türü vardır:

5.3.2.1.1 SSL Portal VPN: Bu tür bir SSL VPN, bir Web sitesine tek bir SSL bağlantısı sağlar ve böylelikle son kullanıcı birden çok ağ hizmetine güvenli bir şekilde erişebilir. Site, bir portal olarak adlandırılır, çünkü başka kaynaklara götüren tek bir kapıdır (tek sayfa). Uzak kullanıcı herhangi bir modern Web tarayıcısı kullanarak SSL VPN ağ geçidine erişir, ağ geçidi tarafından desteklenen bir kimlik doğrulama yöntemini kullanarak kendisini ağ geçidi ile tanımlar ve sonra diğer servislere portal olarak görev yapan bir Web sayfası sunulur. [103]

5.3.2.1.2 SSL Tunel VPN: Bu SSL VPN türü, bir Web tarayıcısının Web tabanlı olmayan uygulamalar ve protokoller de dahil olmak üzere SSL altında çalışan bir tünel aracılığıyla birden fazla şebeke hizmetine güvenli bir şekilde erişmesini sağlar. SSL tünel VPN'leri, Web tarayıcısının, SSL portal VPN'ler tarafından erişilemeyen işlevsellik sağlamasına izin veren etkin içeriği işleyebilmesini gerektirir. Aktif içerik örnekleri, Java, JavaScript, Aktif X veya Flash uygulamaları veya eklentileri içerir. [103]

#### 5.3.2.2 Transport Layer Security (TLS)

Transport Layer Security(TLS), iletişim kuran iki uygulama arasında gizlilik ve veri bütünlüğü sağlayan bir protokoldür. Bugün kullanılan en yaygın güvenlik protokolüdür ve veri aktarımı, VPN bağlantıları, anında mesajlaşma ve IP üzerinden ses gibi bir ağ üzerinden güvenli bir şekilde veri alışverişi yapılması gereken Web tarayıcıları ve diğer uygulamalar için kullanılır.

TLS, Netscape'in SSL protokolünden evrimleşti ve SSL veya SSL / TLS terimleri bazen hala kullanılsa da onu geçersiz kıldı. TLS'yi daha güvenli ve etkili bir protokol haline getiren SSL ve TLS arasındaki temel farklar, daha yeni ve daha güvenli algoritmaları destekleyen TLS ile, ileti kimlik doğrulaması, temel malzeme üretme ve desteklenen şifreleme paketleri. Eski Sistemlerle çalışmak için TLS şu anda geriye dönük uyumluluk sağlayan TLS ve SSL birlikte çalışabilir değildir.

Protokol belirtimine göre, TLS iki katmandan oluşur: TLS Kayıt Protokolü ve TLS İletişim Protokolü. Kayıt Protokolü, bağlantı güvenliğini sağlarken El Sıkışma Protokolü, sunucu ve istemcinin birbirlerini doğrulamasına ve herhangi bir veri değiştirilmeden önce şifreleme algoritmaları ve şifreleme anahtarlarını müzakere etmesine izin verir.

Uygulama kusurları her zaman herhangi bir şifreleme teknolojisi ile büyük bir sorun oluşturmuştur ve TLS'de bir istisna değildir. Mesela, Rezil Halbleed hatası, hiçbir veri iletilmediğinde bile bağlantıları canlı tutmak için tasarlanan TLS kalp atışı mekanizmasının, OpenSSL'nin uygulanmasıyla ilgili bir mantık parçasındaki şaşırtıcı derecede küçük bir hatanın sonucuydu. [104]

### 5.3.3 Network Layer Security Protocols

#### 5.3.3.1 IPsec (Internet Protocol Security)

Internet Protocol Security(IPsec), ağdaki güvenlik veya paket iletişimin ağ iletişimi katmanı için bir dizi protokol için bir çerçevedir. [106]

Daha önce yapılmış güvenlik yaklaşımları, iletişim modelinin uygulama katmanına güvenlik eklemiştir. Fakat IPsec'in sanal özel ağları uygulamak ve özel ağlara çevirmeli bağlantı yoluyla uzak kullanıcı erişimi için özellikle yararlı olduğu söylenebilir. IPsec'in büyük bir avantajı da güvenlik düzenlemelerinin tek tek kullanıcı bilgisayarlarında değişiklikler yapılmasına gerek kalmadan ele alınabilmesidir. Cisco, IPsec'i standart (veya standartlar ve teknolojilerin birleşimi) olarak önermek konusunda liderdir ve buna, ağ yönlendiricilerinde destek dahildir. [106]

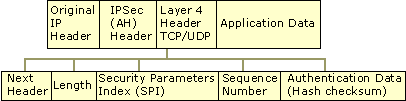
IPsec, iki güvenlik hizmeti seçeneği sunar: Temel olarak verilerin göndereninin kimlik doğrulamasına izin veren Kimlik Doğrulama Başlığı (Authentication Header-AH) ve gönderenin kimlik doğrulamasını ve verilerin şifrelemesini de destekleyen Kapsüllenen Güvenlik Yükü (Encapsulating Security Payload-ESP). Bu hizmetlerin her biriyle ilişkili özel bilgiler, paketin içine, IP paket başlığını takip eden bir başlığa eklenir. Ayrı anahtar protokolleri, ISAKMP / Oakley protokolü gibi seçilebilir. [106]

##### 5.3.3.1.1 Authentication Header

Authentication Header(AH), tüm paket için kimlik doğrulama, bütünlük ve oynatma önleme sağlar (hem IP üstbilgisi hem paket içinde taşınan veri yükü). Verileri şifrelemediği anlamına gelen gizlilik sağlamaz. Veriler okunabilir ancak değişiklikten korunuyor. AH, paketin bütünlüğünü imzalamak için HMAC algoritmalarını kullanır. [105]

Örneğin, Computer A'daki Alice, Computer B'deki Bob'a veri gönderir. IP başlığı, AH başlığı ve veriler bütünlük ile korunur. Bu, Alice'in veriyi gönderen Bob olduğunun ve verilerin değiştirilmediğinden emin olabileceği anlamına gelir. [105]

Dürüstlük ve kimlik doğrulama, Şekil 5.3.3.1.1'de TCP / UDP olarak gösterilen IP üstbilgisi ile taşıma (katman 4) protokol başlığı arasındaki AH üstbilgisinin yerleştirilmesiyle sağlanmaktadır. AH IP üstbilgisinde kendini tanımlamak için 51 IP protokolü kimliğini kullanır. [105]



Şekil 5.3.3.1.1: Authentication Header

**Length:** AH başlığının uzunluğunu belirtir. [105]

**Security Parameters Index (SPI):** İletişim için doğru güvenlik ilişkisini tanımlamak için hedef adres ve güvenlik protokolü (AH veya ESP) ile birlikte kullanılır. Alıcı, bu pakette hangi güvenlik ilişkisine ait olduğunu belirlemek için bu değeri kullanır.

**Sequence Number (SA):SA** için anti-tekrarlama koruması sağlar. Çevrimine izin verilmeyen, art arda artan 32 bitlik (1'den başlayarak) sayıdır ve iletişim için güvenlik ilişkisi üzerinden gönderilen paket numarasını belirtir. Alıcı, bu sayı ile bir güvenlik ilişkisi için bir paketin önceden alınmadığını doğrulamak için bu alanı denetler. Bir kişi alınırsa, paket reddedilir. [105]

**Authentication Data:** Verileri İletinin bütünlüğünü doğrulamak için kullanılan Integrity Check Value(ICV) içerir. Alıcı, karma değerini hesaplar ve bütünlüğü doğrulamak için onu (gönderen tarafından hesaplanan) bu değeri kontrol eder. [105]

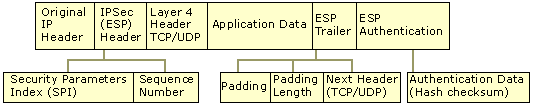
##### 5.4.3.3.1.2 Encapsulating Security Payload(ESP)

Security Payload'unu (ESP) kapsayan, kimlik doğrulama, bütünlük ve tekrar oynatmanın yanı sıra gizlilik de sağlar. ESP tek başına veya AH ile birlikte kullanılabilir.

ESP, normalde paketin tamamını imzalamaz; normalde, IP veri yükü korunur, IP başlığı korunmaz.

Örneğin, Computer A'daki Alice, B Bilgisayarındaki Bob'a veri gönderir. Veri yükü, bütünlük için şifrelenir ve imzalanır. Makbuz üzerine, bütünlük doğrulama işlemi tamamlandıktan sonra, paketteki veri yükü şifresi çözülür. Bob, verileri gönderen, veri değiştirilmemiş olduğunu ve hiç kimsenin onu okuyamadığının gerçekten Alice olduğuna emin olabilir.

ESP, IP üstbilgisinde 50 IP protokol kimliğini kullanarak kendini gösterir. Şekil 70'de gösterildiği gibi, ESP başlığı aktarım katmanı başlığından (TCP veya UDP) önce veya diğer IP protokol türleri için IP yük veri verilerinde yer alır. [107]



Şekil 5.4.3.3.1.2: ESP

**Security Parameters Index**: Hedef adres ve güvenlik protokolü (AH veya ESP) ile birlikte kullanıldığında, iletişim için doğru güvenlik ilişkisini tanımlar. Alıcı, bu paketin tanımlanması gereken güvenlik ilişkisini belirlemek için bu değeri kullanır.

**Sequence Number:** SA için anti-tekrarlama koruması sağlar. İletişim için güvenlik ilişkisi üzerinden gönderilen paket numarasını belirten 32 bitlik, art arda artan sayı (1'den başlayarak). Sıra numarası asla devir işlemine izin verilmez. Alıcı, bu sayı ile bir güvenlik ilişkisi için bir paketin önceden alınmadığını doğrulamak için bu alanı denetler. Bir kişi alınırsa, paket reddedilir. [107]

**Padding:**32 bitlik hizalama ve blok şifre bloğu boyutu için 0 ila 255 bayt kullanılır.

**Padding Length**: Dolgu alanının bayt cinsinden uzunluğunu belirtir. Bu alan, alıcı tarafından, Dolgu alanını atmak için kullanılır. [107]

**Next Header: TCP veya UDP gibi yükün niteliğini tanımlar.** [107]

**Authentication Data:** Bütünlük Kontrolü Değerini (Integrity Check Value-ICV) ve gönderenin kimliğini ve mesaj bütünlüğünü doğrulamak için kullanılan bir mesaj doğrulama kodunu içerir. ICV, ESP başlığı, yük durumu verileri ve ESP römorku üzerinden hesaplanır. [107]

#### 5.3.3.2 Virtual Private Network (VPN)

Virtual Private Network(VPN), daha az güvenli bir ağ üzerinden şifreli bir bağlantı oluşturan teknolojidir. Güvenli bir VPN kullanmanın yararı, alttaki ağ altyapısı tek başına yetersiz geldiğinde, bağlı sistemlere uygun güvenlik düzeyini sağlamaktır. Özel bir ağ yerine VPN erişimini kullanmanın gerekçesi genellikle maliyet ve fizibiliteye dayanır. Özel bir ağa sahip olma, örneğin seyahat eden bir satış temsilcisi için mümkün değildir ya da bunu yapmak çok maliyetlidir. En yaygın VPN türleri uzaktan erişim VPN'leri ve siteler arası (siteden siteye) VPN'lerdir.

**Uzaktan erişim VPN**, uzak kullanıcılara kuruluş ağına güvenli erişim sağlamak için internet gibi bir kamu telekomünikasyon altyapısını kullanır. Çalışanlar interneti kullanmak ve şirket ağına bağlanmak için bir genel Wi-Fi hotspot'u veya başka yollar kullandığında, bu özellikle önemlidir. Uzak kullanıcının bilgisayarındaki veya mobil cihazındaki VPN istemcisi, kuruluş ağındaki bir VPN ağ geçidine bağlanır. Ağ geçidi tipik olarak cihazın kimliğini doğrulamasını gerektirir. Ardından, iç ağ kaynaklarına (örneğin, dosya sunucuları, yazıcılar ve intranet'ler) sanki o ağda sanki yerel olarak erişmesine izin veren, cihaza geri dönen bir ağ bağlantısı oluşturur.

Uzaktan erişim VPN, genellikle güvenliğini sağlamak için IPsec veya Secure Sockets Layer(SSL) kullanır, ancak SSL VPN'ler genelde tüm dahili ağdan ziyade tek bir uygulamaya güvenli erişim sağlamaya odaklanmıştır. Bazı VPN'ler hedef ağa Katman 2 erişimi sağlar; Bunlar, temel IPsec bağlantısı üzerinden çalışan PPTP veya L2TP gibi bir tünel protokolünü gerektirir.

**Siteler arası VPN** ise, bir ağdaki tüm şebekeyi başka bir şebekedeki şebekeye bağlamak için bir ağ geçidi cihazı kullanır (genellikle bir veri merkezine bağlanan küçük bir şube). Uzak konumdaki son düğüm aygıtları, VPN istemcilerine ihtiyaç duymaz; çünkü ağ geçidi bağlantıyı yönetir. İnternet üzerinden bağlanan siteden siteye VPN'lerin çoğunun IPsec'i kullanır. Ayrıca, halka açık internet yerine taşıyıcı MPLS bulutları, siteden siteye VPN'ler için taşıma aracı olarak kullanmaktır. Burada da taban aktarımında Katman 3 bağlantısı (MPLS IP VPN) veya Katman 2 (Virtual Private LAN Service veya VPLS) çalıştırmak mümkündür.

VPN'ler, veri alışverişi için güvenlik gereksinimleri, kurumsal ağın sağlayabileceğini aştığında, belirli bilgisayarlar arasında, genellikle farklı veri merkezlerinde bulunan sunucular arasında da tanımlanabilir. Kuruluşlar giderek artan bir şekilde, kamuya açık altyapıya hizmet etmiş bir ortamda kaynaklara bağlanmak ya da bağlantı kurmak için uzaktan erişim modunda ya da site-to-site modunda VPN bağlantıları kullanmaktadır. Daha yeni hibrid erişim senaryoları, bulut servis sağlayıcıdan dahili ağa güvenli bir bağlantı ile VPN ağ geçidinin kendisini buluta yerleştirir. [108]

### 5.3.4 Data Link Layer Güvenlik Protokolleri

#### 5.3.4.1 PPP (Point-to-Point Protocol)

Noktadan Noktaya Protokolü (Point-to-Point Protocol-PPP), noktadan noktaya bağlantılar üzerinden çok protokollü verileri taşımanın standart bir yolunu sağlayan, bilgisayar ağı protokol ailesini belirtir. PPP'nin üç ana bileşeni vardır: Çoklu protokol datagramlarını kapsayan bir yol; Veri bağlantısı bağlantısı kurmak, yapılandırmak ve test etmek için bir Bağlantı Kontrol Protokolü Ve farklı türde ağ katmanı protokolleri kuran ve yapılandıran bir grup ağ kontrol protokolü.

PPP ayrıca IP veya diğer ağ Katmanı 3 verilerini, fiziksel bağlantı üzerinden doğrudan bağlı iki düğüm arasında veya doğrudan bağlantı üzerinden tünel oluşturur. IP ve TCP noktadan noktaya bağlantıları desteklemediğinden, PPP'nin kullanılması Ethernet ve diğer fiziksel ortamlar üzerinde onları etkinleştirebilir.

OSI modeli açısından PPP, Katman 2'yi veya veri bağlantısı hizmetini sunar. PPP, bükümlü çift bakır tel, fiber optik hatlar veya uydu bağlantıları da dahil olmak üzere çeşitli fiziksel ortamlarda kullanılabilen tam çift yönlü bir protokoldür. PPP, çevirmeli modem bağlantısı ile Secure Sockets Layer(SSL) şifreli VPN bağlantısına kadar her konuda hizmet sağlayabilir. PPP, paket kapsüllemesi için bir High Level Data Link Control(HDLC) varyasyonu kullanır.

Örneğin, bir şirket ağı üzerindeki yüksek güvenlikli bir uygulama, VPN üzerinden ağa bağlanır ve bir SSL bağlantısı oluşturur. Uygulama için istemci bunun üzerine, uygulamanın sunucusuna IP paketleri taşıyacak bir PPP tüneli oluşturabilir. [109]

#### 5.3.4.2 RADIUS (Remote Authentication Dial-In User Service)

Remote Authentication Dial-In User Service(RADIUS), uzaktan erişim sunucularının bir çevirmeli kullanıcıların kimliğini doğrulamak ve istenen sisteme veya hizmete erişimlerini yetkilendirmek için merkezi bir sunucu ile iletişim kurmasını sağlayan bir istemci / sunucu protokolü ve yazılımıdır.

RADIUS, bir şirketin tüm uzak sunucuların paylaşabileceği merkezi bir veritabanında kullanıcı profillerini korumasına izin verir. Bir şirketin tek bir yönetilen ağ noktasında uygulanabilecek bir politika oluşturmasına izin vererek daha iyi güvenlik sağlar. Merkezi bir hizmete sahip olmak, faturalandırma ve şebeke istatistiklerinin tutulması için kullanımı izlemenin daha kolay olduğu anlamına gelir. Livingston tarafından (şimdi Lucent'a ait) düzenlenen RADIUS, bir dizi ağ ürün şirketinin kullandığı fiili endüstri standardıdır ve önerilen bir IETF standardıdır. [110]

#### 5.3.4.3 TACACS (Terminal Access Controller Access Control System)

Terminal Access Controller Access Control System(TACACS), bir uzaktan erişim sunucusunun belirli bir sisteme erişime izin verilip verilmeyeceğini belirlemek için bir kullanıcının oturum açma parolasını bir kimlik doğrulama sunucusuna iletmesine olanak tanıyan UNIX ağlarında ortak olan daha eski bir kimlik doğrulama protokolüdür. TACACS bir şifreleme protokolüdür ve bu nedenle daha sonraki TACACS + ve Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti protokollerinden daha az güvenlidir. TACACS'in sonraki bir sürümü XTACACS (Extended TACACS) 'dır. Her ikisi de Request for Comments 1492'de açıklanmıştır.

TACACS+, ismine rağmen tamamen yeni bir protokoldür. TACACS + ve RADIUS, genellikle daha yeni yapılan veya güncellenen ağlardaki önceki protokolleri değiştirmiştir. TACACS +, TCP kullanır ve RADIUS, User Datagram Protocol(UDP) kullanır. Bazı yöneticiler, TCP daha güvenilir bir protokol olarak görüldükleri için TACACS + kullanmanızı önerir. RADIUS bir kullanıcı profilinde kimlik doğrulama ve yetkilendirmeyi birleştirirken, TACACS + iki işlemi birbirinden ayırır. [111]

TACACS ve XTACACS hala birçok eski sistemde çalışıyor. [111]

## 5.4. Diğer Authentication Protokolleri

### 5.4.1 CHAP (Challenge-Handshake Authentication Protocol)

Challenge-Handshake Authentication Protocol (CHAP), bir sisteme PAP bağlanmak için daha güvenli bir prosedürdür.

**CHAP nasıl işliyor:**

1. Bağlantı yapıldıktan sonra, sunucu bağlantı isteği yapan kişiye bir hata mesajı gönderir. İstekte bulunan kişi, tek yönlü bir karma işlev kullanarak elde edilen bir değerle yanıt verir.
2. Sunucu, beklenen karma değerin kendi hesaplamasını karşılaştırarak yanıtı denetler.
3. Değerler eşleşirse, kimlik doğrulama kabul edilir; Aksi takdirde bağlantı genellikle sonlandırılır.

Sunucu, istediği zaman, bağlı taraftan yeni bir zorlama mesajı göndermesini isteyebilir. CHAP tanımlayıcıları sık sık değiştirildiğinden ve sunucu tarafından herhangi bir zamanda kimlik doğrulama istenebileceğinden, CHAP PAP'den daha fazla güvenlik sağlar. Hem RFC1334 hem de CHAP, PAP'ı tanımlar. [112]

### 5.4.2 Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol(EAP), bir bilgisayarı İnternet'e bağlarken sıklıkla kullanılan bir protokol olan PPP tarafından kullanılan kimlik doğrulama yöntemlerinde genişleyen wireless network’leriçin bir protokoldür. EAP, belirteç kartları, akıllı kartlar, sertifikalar, bir kerelik parolalar ve genel anahtar şifreleme kimlik doğrulaması gibi birden çok kimlik doğrulama mekanizmasını destekleyebilir. [113]

**Nasıl Çalışır?**

Kullanıcı, EAP kullanarak iletişimde, bir erişim noktası (bazen alıcı verici olarak bilinen veriyi ileten ve alan bir istasyon) yoluyla bir kablosuz ağa bağlantı ister. Access Point, kullanıcıdan kimlik verileri istemekte ve bu verileri bir kimlik doğrulama sunucusuna iletmektedir. Kimlik doğrulama sunucusu, erişim noktasına Kimliğin geçerliliğini kanıtlamasını ister. Erişim noktası kullanıcıdan bu doğrulama edildikten sonra tekrar kimlik doğrulama sunucusuna gönderir, kullanıcı ağa istenen şekilde bağlanır. [113]

### 5.4.3 Password Authentication Protocol (PAP)

Password Authentication Protocol(PAP), verileri şifrelemeyen ve parola ve kullanıcı adını kimlik doğrulama sunucusuna düz metin olarak gönderen basit bir kullanıcı kimlik doğrulama protokolüdür. PAP, kimlik doğrulama sunucusu ve kullanıcının makine arasında değiştirilen PPP veri paketlerinden okunmaya karşı çok savunmasızdır. Bu öncelikle, daha gelişmiş şifreleme protokolleri için hiçbir desteği olmayan eski Unix tabanlı sunuculara bağlanırken kullanılmıştır. [114]

### 5.4.4 Shiva Password Authentication Protocol (SPAP)

Shiva Password Authentication Protocol(SPAP), Shiva tarafından kullanılan tersine çevrilebilir bir şifreleme mekanizmasıdır. Windows XP Professional çalıştıran bir bilgisayar, Shiva LAN Rover'a bağlanırken Yönlendirme ve Uzaktan Erişim çalıştıran bir sunucuya bağlanan bir Shiva istemcisi gibi SPAP kullanır.

Bu kimlik doğrulama biçimi, salt metinten daha güvenlidir, ancak CHAP veya MS-CHAP'den daha az güvenlidir.

Bu kimlik doğrulama biçimi de ne yazık ki zayıflıklara sahiptir. Güvenli ve şifreli olmasına rağmen, tekrar çalma saldırıları denilen saldırı türüne karşı zayıf olabilmektedir.

Bu duyarlılığın nedeni, kullanıcı oturum açmaya çalıştığında her yöne aynı kimlik bilgilerinin gönderilmesidir. "Sunucu veya sanal ağı dinleyen bir bilgisayar korsanı" bu sinyali kesebilir ve bu sinyale sızmak için sistemi kullanabilir.

Güvenlik için bu ciddi tehdit nedeniyle, bu kimlik doğrulama biçimi şimdi yaygın bir şekilde cesaretini kırmış durumda. Çoğu sanal ağ, bu kimlik doğrulama biçimini kullanmayı bırakmıştır. [115]

### 5.4.5 Data Encryption Standard (DES)

DES, veri şifrelemesinin güncel olmayan simetrik anahtar bir yöntemidir. DES, bir iletiyi şifrelemek ve şifre çözmek için aynı anahtarı kullanarak çalışır, bu nedenle hem gönderen hem de alıcı aynı özel anahtarı bilmeli ve kullanmalıdır.

Başlangıçta 1970'lerin başında IBM'deki araştırmacılar tarafından tasarlanan DES, 1977'de ABD hükümeti tarafından ticari ve hassas henüz sınıflandırılmamış devlet bilgisayar verilerinin şifrelenmesi için bir FIP standardı olarak kabul edildi. ABD hükümeti tarafından kamunun aydınlatması için onaylanan ilk şifreleme algoritmasıydı. Bu, DES'nin güçlü şifreleme ihtiyacının yüksek olduğu mali hizmetler gibi endüstriler tarafından çabucak benimsenmesini sağlamıştır. DES'nin sadeliği, çok çeşitli gömülü sistemler, akıllı kartlar, SIM kartlar ve modemler, set üstü kutular ve yönlendiriciler gibi şifreleme gerektiren ağ aygıtlarında kullanıldı.

#### 5.4.5.1 DES anahtar uzunluğu ve kaba kuvvet saldırıları

Veri Şifreleme Standardı bir blok şifrelidir, yani şifreleme anahtarı ve algoritma aynı anda bir bit yerine aynı anda bir veri bloğuna uygulanır. Bir düz metin mesajı şifrelemek için DES, 64 bitlik bloklara ayırır. Her blok, permütasyon ve değiştirme yoluyla gizli anahtarı kullanarak 64-bit şifreleme içine şifrelenir. İşlem 16 tur içerir ve dört farklı modda çalışabilir, blokları tek tek şifreleyebilir veya her bir şifre bloğunu önceki blokların tamamına bağımlı hale getirir. Şifre çözme, şifrelemenin tersi, aynı adımları takip ederek, ancak anahtarların uygulanma sırasını tersine çevirmektir. Herhangi bir şifre için en temel saldırı yöntemi, doğru olanı bulana kadar her anahtarı denemeyi içeren kaba kuvvettir. Anahtarın uzunluğu, bu tür saldırıların olası anahtar sayısını ve dolayısıyla fizibilitesini belirler. DES, 64 bitlik bir anahtar kullanır, ancak bu bitlerden sekizi eşlik kontrolleri için kullanılır ve bu sayede anahtarı 56 bitlik bir şekilde sınırlar. Dolayısıyla, en fazla 2 ^ 56, veya 72.057.594.037.927.936, doğru anahtar bulmaya çalışır.

DES şifrelemesi kullanılarak şifrelenen birkaç mesajın bu tür kod kırma çabalarına maruz kalması muhtemel olsa da pek çok güvenlik uzmanı DES'nin bir standart olarak kabul edilmeden önce bile 56 bit anahtar uzunluğunun yetersiz olduğunu düşünüyor. (NSA'dan kaynaklanan müdahalenin IBM orijinal algoritmasını zayıflattığından hep şüphe edilmiştir). Buna rağmen, DES 1990'ların ortalarında güvenilir ve yaygın olarak kullanılan bir şifreleme algoritması olarak kaldı. Bununla birlikte, 1998 yılında Electronic Frontier Foundation (EFF) tarafından inşa edilen bir bilgisayar, DES tarafından kodlanmış bir mesajın şifresini 56 saat içinde çözdü. Ağa bağlı binlerce bilgisayarın gücünden yararlanarak, ertesi yıl EFF şifre çözme süresini 22 saate düşürdü.

Bazı durumlarda geriye dönük uyumluluk sağlamaktan başka, veri gizliliği için bugün DES'ye güvenmek, herhangi bir bilgisayar sisteminde ciddi bir güvenlik tasarım hatasıdır ve kaçınılmalıdır. AES gibi çok daha güvenli algoritmalar mevcuttur. Ucuz bir bavul kilidi gibi, DES de içten içeriği dürüst insanlardan koruyacaktır, ancak belirli bir hırsızı durdurmaz.[116]

#### 5.4.5.2 DES için halefler

Şifreleme gücü doğrudan anahtar boyutuna bağlıdır ve 56 bit anahtar uzunlukları, modern bilgisayarların işlem gücü ile karşılaştırıldığında çok küçük olur. 1997'de NIST, DES için bir halef seçme girişimini ilan etti; 2001'de Gelişmiş Şifreleme Standardı'nı bir yedek olarak seçti. Veri Kriptolama Standardı (FIPS 46-3) Mayıs 2005'te resmen kaldırıldı, ancak Triple DES (3DES) hassas hükümet bilgileri için 2030 yılına kadar onaylanmıştır. 3DES, DES algoritmasının üç iterasyonunu gerçekleştirir; Birinci anahtarlama seçeneği seçilirse, anahtar uzunluğunu 168 bit'e arttırmak için her seferinde farklı bir anahtar kullanılır. Bununla birlikte, karşılama-içi saldırı olasılığı nedeniyle, sağladığı etkin güvenlik sadece 112 bittir. 3DES şifreleme açık DES'den daha açıktır. [116]

### 5.4.6 S/Key Authentication

Bellecore tarafından geliştirilen bir güvenlik sistemi. S/Key, verilere erişimi doğrulamak için kullanılan bir kerelik zorlama-yanıt şifre şemasıdır. S/Key’in amacı, her erişim için bir şifre gerektiğinde bir ağ üzerinden aynı şifrenin iletilmesi gereğini ortadan kaldırmaktır. Bir kerede bir parola oluşturulur ve her parola yalnızca bir kez kullanılır; Bu nedenle, parola alan bir kişi bu bilgileri kullanamaz çünkü ilk kez parola geçildiğinde geçersiz olur. [117]

### 5.4.7 MS-CHAP Authentication

MS-CHAP v1, CHAP'ye çok benzer şifrelenmiş bir kimlik doğrulama mekanizmasıdır. CHAP'ta olduğu gibi, uzaktan erişim sunucusu uzak istemciye bir oturum kimliği ve keyfi bir zorlama dizesinden oluşan bir sorun gönderir. Uzak istemci, kullanıcı adı ve zorlama dizesinin, Message ID4 (MD4) karmasını, oturum kimliğini ve MD4 ile karışık parolayı döndürmelidir.

CHAP ve MS-CHAP v1 arasındaki farklardan biri, CHAP'de, zorlama yanıtını doğrulamak için şifrenin düz metin sürümünün mevcut olmasıdır. MS-CHAP v1 ile uzaktan erişim sunucusu, zorlama yanıtını doğrulamak için yalnızca parola MD4 karmasını gerektirir. Windows 2000'de, kullanıcının parolası MD4 karması olarak ve geri dönüşümlü olarak şifrelenmiş biçimde depolanır. CHAP kullanıldığında uzaktan erişim sunucusu, uzaktan erişim istemcisinin yanıtını doğrulamak için geri alınabilir biçimde şifrelenmiş parolayı çözer.

MS-CHAP v1 kimlik doğrulaması, üç ileti alışverişinde bulunur:

1. Uzaktan erişim sunucusu, bir oturum kimliği ve keyfi bir sorun dizesi içeren bir MS-CHAP Challenge iletisi gönderir.
2. Uzaktan erişim istemcisi, kullanıcı adını düz metin olarak içeren bir MS-CHAP Yanıt iletisi ve sorun dizesi, oturum kimliği ve istemcinin parolasının MD4 karmasını MD4 tek yönlü karma algoritmasını kullanarak döndürür.
3. Uzaktan erişim sunucusu karmayı çoğaltır ve karma MS-CHAP yanıtıyla karşılaştırır. Karmalar aynı ise, uzaktan erişim sunucusu bir MS-CHAP Başarı iletisi gönderir. Karmalar farklıysa, bir MS-CHAP hata İletisi gönderilir.

MS-CHAP v1'in kullanımı, LCP seçeneği (tür 3), kimlik doğrulama protokolü 0xC2-23 ve 0x80 algoritması belirterek LCP anlaşması sırasında müzakere edilir. LCP anlaşması tamamlandığında, MS-CHAP v1 iletileri 0xC2-23 PPP protokol KIMLIĞINI kullanır.

MS-CHAP v1 ayrıca bir "şifre süresi dolmuş" kodu ve şifre değişiklikleri de dahil olmak üzere hata kodlarına izin verir. MS-CHAP v1, kimlik doğrulama girişimi başına keyfi bir zorlama dizesi kullanarak tekrarlama saldırılarına karşı koruma sağlar. MS-CHAP v1, uzak sunucunun kimliğe bürünülmesine karşı koruma sağlamaz.

Kimlik doğrulama protokolü olarak MS-CHAP v1 kullanılırsa ve MPPE görüşülürse, paylaşılan gizli şifreleme anahtarları her PPP eş tarafından üretilir. MS-CHAP v1 ayrıca, kullanıcıların kimlik doğrulama işlemi sırasında şifrelerini değiştirmesine olanak tanıyan bir dizi ileti de sağlar. [118]

# BÖLÜM 6: WIRED ve WIRELESS NETWORK’LERDE ÇALIŞMA GRUPLARI ve ULUSLARARASI STANDART BELİRLEYEN KURUMLAR

Ağ standartları, bilgisayar ağlarında gerekli prensipleri / karakteristikleri / özellikleri tanımlayan, zorlukları belirtmek amacıyla oluşturulan kurallar bütünü olarak tanımlanabilir. Ağ standartları "De Facto" ve "De jure" olmak üzere iki sınıfta gruplandırışır:

**De facto:** Yasal bir yetkiye sahip olmayan şirketlerin geliştirdikleri (IBM PC, UNIX vb) ve genel kullanımları nedeni ile referans kabul edilen standartlardır.

**De jure**: Yasal olarak kabul edilmiş kurumlarca geliştirilen ulusal veya uluslararası standartlardır.

Geçtiğimiz 20 yıl içerisinde bilgisayarlarda olan gelişmelere benzer şekilde bilgisayar ağlarının sayıları ve boyutları ile ilgili inanılmaz gelişmeler yaşandı.

Bu süreç içerisinde oluşturulan / kurulan ağların çoğu, farklı donanım ve yazılım uygulamaları kullanılarak geliştirildi. Bilgisayar ağlarının ilk yıllarında her bilgisayar üreticisi kendi protokollerini geliştiriyoırdu. Sonuçta biribiri ile uyumsuz birçok bilgisayar ağı oluştu ve farklı standartlar kullanan bu ağların biribirleri ile iletişim kurmaları güçleşti. Bu problemi çözmek amacıyla, Uluslararası Standartlar Organizasyonu (International, Standarts Organization-ISO) ağ kurucularının iletişim kurabilmelerine ve birlikte çalışabilmelerine yardımcı olabilmek için gerekli bir ağ modeli geliştirme ihtiyacını ortaya koydu, ortaya konulan ihtiyaçların karşılanmasına yönelik çalışmalarn sonucu olarak ISO tarafından "Açık Sistem Bağlantıları (Open System Interconnection- OSI)" referans modeli yayınlandı. [123]

OSI referans modeli kullanılarak veya kullanılmadan oluşturulan ağ standartları, genellikle belli kurumlar ve komiteler tarafından oluşturulur, onaylanır. Biz de çalışmanın bu bölümünde, uluslararası ağ standartlarını belirleyen kurumlardan ve bu kurumların belirlediği bilgisayar ağlarında güvenlik konusunu içeren standartlarıdan bahsedeceğiz. [123]

## 6.1. ISO (International Organization for Standardization)

### 6.1.1 ISO Nedir?

ISO uluslararası standartlar örgütü yani (International Organization for Standardization) kelimesinin baş harflerinin kısaltılmasıdır. Bu bağımsız, sivil toplum örgütü Uluslararası Standartların dünyadaki en büyük geliştiricisidir.

Genel Merkezi İsviçre’nin Cenevre şehrindedir ve 165 üye ülkenin biraraya gelmesiye oluşmuştur. [123]

### 6.1.2 ISO Tarihçe

25 ülkeden gelen delegelerin Londra İnşaat Mühendisleri Enstitüsünde bir araya gelerek ve endüstriyel standartların uluslararası koordinasyonu ve birleşmesini kolaylaştırmak için yeni bir uluslararası organizasyon oluşturmak için karar vermesi sonucu, ISO hikâyesi 1946 yılında başladı. Şubat 1947 yılında yeni organizasyon, ISO, resmen faaliyete başladı.

O zamandan beri, teknoloji ve üretim hemen hemen tüm yönlerini kapsayan 19500 Uluslararası Standart yayımlanmıştır. [123]

### 6.1.3 ISO Standartları Nelerdir?

Uluslararası ISO Standartları, kalite, güvenlik ve verimliliği sağlamak için ürün, hizmet ve sistemlere yönelik dünya çapında setifika vererek, uluslararası ticaretin kolaylaştırılmasında etkili bir rol üstlenir.[123]

ISO tarım ve sağlık, teknoloji, gıda güvenliği, hemen hemen her sanayi kapsayan 19500’den fazla Uluslararası Standart yayınlamıştır.[123]

Bir uluslararası standart üye kuruluşların anlaşmasıyla onaylanır ve ülkelerde ya doğrudan, ya da ulusal standartlara dönüştürülerek uygulanır.[123]

Standardın ön çalışmaları uzaktan haberleşme ile sürdürülür. Standart son halini aldığında onay çalışmaları için bir araya gelinir. Onaylanan standartlar en geç beş yıl içinde gözden geçirilir ve gerekiyor ise, güncellenir. Yayınlanan bütün standartlar ISO katalogunda yer alır.

### 6.1.4 ISO Yönetim Standartları

– Kalite – ISO 9001

– Çevre – ISO 14001

– Risk yönetimi – ISO 31000

– İş sürekliliği – ISO 22301

– Enerji yönetimi – ISO 50001

– Bilgi güvenliği – ISO 27001

– Sosyal sorumluluk – ISO 26000

– Gıda Güvenliği – ISO 22000

Yönetim Sistemi, Ürün Belgelendirmesi, Muayene Raporlaması, Laboratuvarlar ve diğer tüm sistemlerin yüzlerce standardı vardır. Ancak standartları birbirinden ayırt ederken 9000’den başlayarak 60000 bin küsurlara kadar sistem, ürün, analiz, standartları vardır. Bunlardan bazıları da 17000 serisi olarak sayılabilen tüm bu belgelendirmeleri yapan kuruluşların akredite (yetkinliğinin teyidi) edilmesi için uygulaması gerekli standartlardır. [123]

Şimdi artık, ISO’ya dair bu genel tanımları aldıktan sonra bu tezin konusunu ilgilendiren bilgi güvenlik standartlarını inceleyebiliriz. Wired ve wireless network’lerde güvenliğin sağlanması, bilgi güvenliğinin sağlanması temellerine dayanır. ISO’nun güvenliğe dair 27000 serisi standartları aşağıda incelenmiştir. [123]

#### 6.1.4.1 ISO 27001 Bilgi Güvenliği Yönetim Sistemi:

Bilgi, teknoloji ve iletişim alanında yaşanan tüm gelişmeler kurumları birbirlerine göre yarış yapmak ve rekabet ederken en önemli kriter olan bilgiyi güvenli bir şekilde korumak zorunda kalmışlardır. [123]

Bilgi Güvenliği sağlanırken diğer tüm yönetim sistemleri standartları gibi kurumda bilginin nasıl erişildiğine, korunduğuna, yedeklendiğine, bilgiye erişim izinlerine ve hatta sürekli kontrol altında tutmaya yarayan yönetim sistemi standardına ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ denir.

Kuruluş bir 27001 belgesi sahibi ise bu standardı uyguladığı ve kendi değerlendirmeleri dışında bir belgelendirme kuruluşunun denetimlerinden geçtiği ve bunu süreklilik haline getirebildiği anlaşılmaktadır. [123]

21. yüzyılın en güçlü rekabet anahtarı olan bilginin de bu şekilde korunma altına alınması bir firmayı oldukça güçlü bir konuma getirir. Önemli bir prestij göstergesi olan ISO 27001 Belgesi artık uluslararası ticarette yer alan lojistik, müşavirlik, sigortacılık, depoculuk, ihracat veya ithalat gibi faaliyetleri bulunan kuruluşlar için özel olarak aranmaktadır. [123]

#### 6.1.4.2 ISO 27000 Serisi Standartları

Bu firmaların yetkili yükümlülük sertifikası başvurusundaki en önemli belgelerden olan ISO 27001, devlet ihalelerinde, yerel yönetimlerin veya Bilgi Teknolojileri Kurumunun da özellikle istediği bir sertifikalandırma biçimi olmuştur. Wired ve wireless network’lerde güvenliğin sağlanmasında güvenilir referans olarak gösterilebilecek ISO bilgi-ağ güvenlik standartlarından aşağıda bahsedilmektedir.

1. TS ISO / IEC 27000 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Genel Bakış ve Sözlük
2. TS ISO / IEC 27001 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler
3. TS ISO / IEC 27002 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri
4. TS ISO / IEC 27003 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri Uygulama Klavuzu
5. TS ISO / IEC 27004 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetimi – Ölçümler
6. TS ISO / IEC 27005 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Risk Yönetimi
7. TS ISO / IEC 27006 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemlerinin Tetkik ve Belgelendirmesini Yapan Kuruluşlar için Şartlar [123]

## 6.2. ANSI (American National Standards Institute)

ANSI, özel, kâr amacı gütmeyen bir kuruluştur. ABD'nin gönüllü standartlarını ve uygunluğunu yöneten ve koordine eden bir değerlendirme sistemidir. 1918'de kurulan bu enstitü, standartları belirlemek ve geliştirmek için sanayi ve hükümetten paydaşlar ile çalışmaktadır. Ulusal ve küresel önceliklere uygunluk temelli çözümler üretmek üzere standartlar geliştirir ve  [Amerika Birleşik Devletleri](https://tr.wikipedia.org/wiki/Amerika_Birle%C5%9Fik_Devletleri) federal devletinin standart enstitüsü NIST ile ilgilenir.

ANSI, Birleşik Devletler'de teknoloji standartlarının geliştirilmesini destekleyen birincil kuruluş olarak bugun faaliyetlerine geliştirerek devam etmektedir. ANSI ayrıca, endüstri gruplarıyla çalışır ISO ve IEC üyesidir. [124]

Wired ve wireless network’lere dair belirlediği standartlar şöyledir;

* Screen-display attributes
* Digital telecommunications
* Fiber-optic cable transmissions

## 6.3. NIST (National Institute of Standards and Technology)

NIST, ABD Ticaret Bakanlığı'nın bir birimi olan Ulusal Standartlar ve Teknoloji Enstitüsüdür. Ulusal Standartlar Bürosu olarak bilinen eski NIST, ölçüm standartlarını geliştirir ve korur. Aynı zamanda, bu standartları geliştirmek ve kullanmak için endüstri ve bilimde cesaretlendirici ve destekleyici aktif programlar da vardır. [125]

Akıllı elektrik güç şebekesi ve elektronik sağlık kayıtlarından atom saatlerine, ileri nanomalzemelere ve bilgisayar yongalarına kadar sayısız ürün ve hizmetler, Ulusal Standartlar ve Teknoloji Enstitüsü tarafından sağlanan teknoloji, NIST ölçüm ve standartlarına güvenir.

1901'de kurulan NIST, ABD Ticaret Bakanlığı bünyesinde düzenleyici olmayan bir federal ajansdır (bağlantı harici). NIST'in görevi, ABD'nin yenilikçiliğini ve endüstriyel rekabet gücünü, ekonomik güvenliği artıran ve yaşam kalitemizi artırıcı yöntemlerle ölçüm bilimi, standartları ve teknolojiyi geliştirerek teşvik etmektir. [126]

NIST misyonunu aşağıdaki programlar vasıtasıyla yürütür:

1. NIST Laboratuarları, ulusların teknoloji altyapısını geliştiren ve ABD'li şirketlerin ürün ve hizmetleri sürekli iyileştirmesine yardımcı olan, genellikle endüstri ile yakın iş birliği içerisinde birinci sınıf bir araştırma yürüterek;
2. Küçük üreticilere iş yaratma ve bunları koruma, karları artırma ve zamandan ve paradan tasarruf etmelerine yardımcı olmak için teknik ve ticari yardım sunan, ülke çapında yerel merkezlerden oluşan bir ağ olan Hollings Manufacturing Extension Partnership; ve
3. ABD üreticileri, hizmet şirketleri, eğitim kurumları, sağlık hizmeti sunucuları ve kar amacı gütmeyen kuruluşlar arasındaki performans mükemmelliğini destekleyen Baldrige Performans Mükemmellik Programı, sosyal yardım programları yürütme, Performansta mükemmellik ve kalite başarısını tanıyan yıllık Malcolm Baldrige Ulusal Kalite Ödülü'nü yönetir. [126]

NIST, bilgisayar / siber / bilgi güvenliği ve yönergeler, tavsiyeler ve referans malzemeleri yayınlamak için üç NIST Özel Yayın alt dizini kullanır:

1. **SP 800, Bilgisayar Güvenliği (Aralık 1990'dan bugüne):** NIST’in birincil bilgisayar / siber / bilgi güvenliği yönergeleri, tavsiyeleri ve referans malzemeleri yayınlama biçimi; [127]
2. **SP 1800, NIST Siber Güvenlik Uygulamaları Kılavuzları (2015-yılı):** SP 800'leri tamamlamak için oluşturulan yeni bir alt seriler; Kamu ve özel sektördeki belirli siber güvenlik konularını hedeflemektedir; Siber güvenliğe yönelik standartlara dayalı yaklaşımların benimsenmesini kolaylaştıran pratik, kullanıcı dostu kılavuzlar; [127]
3. **SP 500, Bilgisayar Sistemleri Teknolojisi (Ocak 1977-şimdiki):** Genel IT alt bölümleri, NIST-ITL tarafından daha geniş bir şekilde kullanılır; bu sayfada, NIST'in bilgisayar güvenlik çabaları ile ilgili seçilmiş SP 500'ler listelenir. (SP 800 alt bölümlerinden önce, NIST bilgisayar güvenlik yayınları için SP 500 alt bölümlerini kullandı; bir liste için Arşivlenmiş NIST SP'lere bakın.) [127]

### 6.3.1 Wired ve Wireless Network’lerde Güvenliğe Dair NIST’in Belirlediği SP 800 Seri Standartlar Listesi [127]

|  |  |  |
| --- | --- | --- |
| **SP 800-188**  (Draft) | December 2016 | **DRAFT De-Identifying Government Datasets (2nd Draft)** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-188) |
| **SP 800-187**  (Draft) | November 2016 | **DRAFT Guide to LTE Security** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-187) |
| **SP 800-185** | December 2016 | **SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash** |
|  |  |  |
| **SP 800-184** | December 2016 | **Guide for Cybersecurity Event Recovery** |
|  |  |  |
| **SP 800-183** | July 2016 | **Networks of 'Things'** |
|  |  |  |
| **SP 800-182** | July 2016 | **Computer Security Division 2015 Annual Report** |
| **SP 800-181**  (Draft) | November 2016 | **DRAFT NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education** |
| **SP 800-180**  (Draft) | February 2016 | **DRAFT NIST Definition of Microservices, Application Containers and System Virtual Machines** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-180) |
| **SP 800-179** | December 2016 | **Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist** |
|  |  |  |
|  |  |  |
| **SP 800-178** | October 2016 | **A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)** |
| **SP 800-177** | September 2016 | **Trustworthy Email** |
|  |  |  |
| **SP 800-176** | August 2015 | **Computer Security Division 2014 Annual Report** |
| **SP 800-175A** | August 2016 | **Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies** |
|  |  |  |
| **SP 800-175B** | August 2016 | **Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms** |
|  |  |  |
| **SP 800-171 Rev. 1** | December 2016 | **Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations** |
|  |  |  |
| **SP 800-171** | June 2015 (Updated 1/14/2016) | **Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations** |
|  |  |  |
| **SP 800-170** | June 2014 | **Computer Security Division 2013 Annual Report** |
| **SP 800-168** | May 2014 | **Approximate Matching: Definition and Terminology** |
| **SP 800-167** | October 2015 | **Guide to Application Whitelisting** |
|  |  |  |
| **SP 800-166** | June 2016 | **Derived PIV Application and Data Model Test Guidelines** |
| **SP 800-165** | July 2013 | **Computer Security Division 2012 Annual Report** |
| **SP 800-164**  (Draft) | October 2012 | **DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-164) |
| **SP 800-163** | January 2015 | **Vetting the Security of Mobile Applications** |
|  |  |  |
| **SP 800-162** | January 2014 | **Guide to Attribute Based Access Control (ABAC) Definition and Considerations** |
|  |  |  |
| **SP 800-161** | April 2015 | **Supply Chain Risk Management Practices for Federal Information Systems and Organizations** |
| **SP 800-160** | November 2016 | **Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems** |
|  |  |  |
| **SP 800-157** | December 2014 | **Guidelines for Derived Personal Identity Verification (PIV) Credentials** |
| **SP 800-156** | May 2016 | **Representation of PIV Chain-of-Trust for Import and Export** |
|  |  |  |
| **SP 800-155**  (Draft) | December 2011 | **DRAFT BIOS Integrity Measurement Guidelines** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-155) |
| **SP 800-154**  (Draft) | March 2016 | **DRAFT Guide to Data-Centric System Threat Modeling** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-154) |
| **SP 800-153** | February 2012 | **Guidelines for Securing Wireless Local Area Networks (WLANs)** |
|  |  |  |
| **SP 800-152** | October 2015 | **A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)** |
|  |  |  |
| **SP 800-150** | October 2016 | **Guide to Cyber Threat Information Sharing** |
| **SP 800-147B** | August 2014 | **BIOS Protection Guidelines for Servers** |
| **SP 800-147** | April 2011 | **BIOS Protection Guidelines** |
|  |  |  |
| **SP 800-146** | May 2012 | **Cloud Computing Synopsis and Recommendations** |
|  |  |  |
|  |  |  |
| **SP 800-145** | September 2011 | **The NIST Definition of Cloud Computing**] |
|  |  |  |
|  |  |  |
| **SP 800-144** | December 2011 | **Guidelines on Security and Privacy in Public Cloud Computing**. |
|  |  |  |
|  |  |  |
| **SP 800-142** | October 2010 | **Practical Combinatorial Testing** |
| **SP 800-137** | September 2011 | **Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations** |
|  |  |  |
| **SP 800-135 Rev. 1** | December 2011 | **Recommendation for Existing Application-Specific Key Derivation Functions** |
|  |  |  |
| **SP 800-133** | December 2012 | **Recommendation for Cryptographic Key Generation** |
|  |  |  |
|  |  |  |
| **SP 800-132** | December 2010 | **Recommendation for Password-Based Key Derivation: Part 1: Storage Applications** |
| **SP 800-131A Rev. 1** | November 2015 | **Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths**] |
| **SP 800-130** | August 2013 | **A Framework for Designing Cryptographic Key Management Systems** |
| **SP 800-128** | August 2011 | **Guide for Security-Focused Configuration Management of Information Systems** |
| **SP 800-127** | September 2010 | **Guide to Securing WiMAX Wireless Communications** |
|  |  |  |
|  |  |  |
| **SP 800-126A**  (Draft) | July 2016 | **DRAFT SCAP 1.3 Component Specification Version Updates: An Annex to NIST Special Publication 800-126 Revision 3** |
| **SP 800-126 Rev. 3**  (Draft) | July 2016 | **DRAFT The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3** |
| **SP 800-126 Rev. 2** | September 2011 (Updated 3/19/2012) | **The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2** |
|  |  |  |
| **SP 800-126 Rev. 1** | February 2011 | **The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1** |
| **SP 800-126** | November 2009 | **The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0** |
| **SP 800-125A**  (Draft) | October 20, 2014 | **DRAFT Security Recommendations for Hypervisor Deployment** |
| **SP 800-125B** | March 2016 | **Secure Virtual Network Configuration for Virtual Machine (VM) Protection**] |
| **SP 800-125** | January 2011 | **Guide to Security for Full Virtualization Technologies** |
|  |  |  |
| **SP 800-124 Rev. 1** | June 2013 | **Guidelines for Managing the Security of Mobile Devices in the Enterprise** |
|  |  |  |
|  |  |  |
| **SP 800-123** | July 2008 | **Guide to General Server Security** |
|  |  |  |
| **SP 800-122** | April 2010 | **Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**] |
|  |  |  |
| **SP 800-121 Rev. 2**  (Draft) | October 2016 | **DRAFT Guide to Bluetooth Security** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-121-Rev-2) |
| **SP 800-121 Rev. 1** | June 2012 | **Guide to Bluetooth Security** |
|  |  |  |
| **SP 800-120** | September 2009 | **Recommendation for EAP Methods Used in Wireless Network Access Authentication** |
| **SP 800-119** | December 2010 | **Guidelines for the Secure Deployment of IPv6** |
| **SP 800-117 Rev. 1**  (Draft) | January 2012 | **DRAFT Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.2** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-117-Rev.%201) |
| **SP 800-117** | July 2010 | **Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0** |
| **SP 800-116 Rev. 1**  (Draft) | December 2015 | **DRAFT A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-116-Rev.%201) |
| **SP 800-116** | November 2008 | **A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)** |
| **SP 800-115** | September 2008 | **Technical Guide to Information Security Testing and Assessment**] |
|  |  |  |
| **SP 800-114 Rev. 1** | July 2016 | **User's Guide to Telework and Bring Your Own Device (BYOD) Security**. |
| **SP 800-113** | July 2008 | **Guide to SSL VPNs** |
| **SP 800-111** | November 2007 | **Guide to Storage Encryption Technologies for End User Devices** |
| **SP 800-108** | October 2009 | **Recommendation for Key Derivation Using Pseudorandom Functions (Revised)** |
| **SP 800-107 Rev. 1** | August 2012 | **Recommendation for Applications Using Approved Hash Algorithms** |
| **SP 800-106** | February 2009 | **Randomized Hashing for Digital Signatures** |
| **SP 800-102** | September 2009 | **Recommendation for Digital Signature Timeliness** |
| **SP 800-101 Rev. 1** | May 2014 | **Guidelines on Mobile Device Forensics** |
| **SP 800-100** | October 2006 (Updated 3/7/2007) | **Information Security Handbook: A Guide for Managers** |
| **SP 800-98** | April 2007 | **Guidelines for Securing Radio Frequency Identification (RFID) Systems** |
| **SP 800-97** | February 2007 | **Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i** |
| **SP 800-96** | September 2006 | **PIV Card to Reader Interoperability Guidelines** |
| **SP 800-95** | August 2007 | **Guide to Secure Web Services** |
| **SP 800-94 Rev. 1**  (Draft) | July 2012 | **DRAFT Guide to Intrusion Detection and Prevention Systems (IDPS)** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-94-Rev.%201) |
| **SP 800-94** | February 2007 | **Guide to Intrusion Detection and Prevention Systems (IDPS)** |
| **SP 800-92** | September 2006 | **Guide to Computer Security Log Management** |
|  |  |  |
| **SP 800-90A Rev. 1** | June 2015 | **Recommendation for Random Number Generation Using Deterministic Random Bit Generators** |
|  |  |  |
| **SP 800-90B**  (Draft) | January 2016 | **DRAFT Recommendation for the Entropy Sources Used for Random Bit Generation** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-90-B) |
| **SP 800-90C**  (Draft) | April 2016 | **DRAFT Recommendation for Random Bit Generator (RBG) Constructions** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-90-C) |
| **SP 800-89** | November 2006 | **Recommendation for Obtaining Assurances for Digital Signature Applications** |
| **SP 800-88 Rev. 1** | December 2014 | **Guidelines for Media Sanitization** |
| **SP 800-87 Rev. 1** | April 2008 | **Codes for Identification of Federal and Federally-Assisted Organizations** |
| **SP 800-86** | August 2006 | **Guide to Integrating Forensic Techniques into Incident Response** |
| **SP 800-85A-4** | April 2016 | **PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)** |
| **SP 800-85B-4**  (Draft) | August 2014 | **DRAFT PIV Data Model Test Guidelines** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-85-B-4) |
| **SP 800-85B** | July 2006 | **PIV Data Model Test Guidelines** |
| **SP 800-84** | September 2006 | **Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities** |
|  |  |  |
| **SP 800-83 Rev. 1** | July 2013 | **Guide to Malware Incident Prevention and Handling for Desktops and Laptops** |
| **SP 800-82 Rev. 2** | May 2015 | **Guide to Industrial Control Systems (ICS) Security** |
|  |  |  |
| **SP 800-81-2** | September 2013 | **Secure Domain Name System (DNS) Deployment Guide** |
| **SP 800-79-2** | July 2015 | **Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)** |
| **SP 800-78-4** | May 2015 | **Cryptographic Algorithms and Key Sizes for Personal Identity Verification** |
| **SP 800-77** | December 2005 | **Guide to IPsec VPNs** |
| **SP 800-76-2** | July 2013 | **Biometric Specifications for Personal Identity Verification** |
| **SP 800-73-4** | May 2015 (Updated 2/8/2016) | **Interfaces for Personal Identity Verification** |
|  |  |  |
| **SP 800-72** | November 2004 | **Guidelines on PDA Forensics** |
| **SP 800-70 Rev. 3** | November 2015 (Updated 12/8/2016) | **National Checklist Program for IT Products: Guidelines for Checklist Users and Developers** |
|  |  |  |
| **SP 800-69** | September 2006 | **Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist** |
| **SP 800-68 Rev. 1** | October 2008 | **Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist** |
| **SP 800-67 Rev. 1** | January 2012 | **Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher** |
| **SP 800-66 Rev. 1** | October 2008 | **An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule** |
| **SP 800-65** | January 2005 | **Integrating IT Security into the Capital Planning and Investment Control Process** |
| **SP 800-64 Rev. 2** | October 2008 | **Security Considerations in the System Development Life Cycle** |
| **SP 800-63-3**  (Draft) | May 8, 2016 | **DRAFT Digital Authentication Guideline (Public Preview)** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-63--3) |
| **SP 800-63-2** | August 2013 | **Electronic Authentication Guideline** |
|  |  |  |
| **SP 800-61 Rev. 2** | August 2012 | **Computer Security Incident Handling Guide** |
|  |  |  |
| **SP 800-60 Vol. 2 Rev. 1** | August 2008 | **Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices** |
| **SP 800-60 Vol. 1 Rev. 1** | August 2008 | **Guide for Mapping Types of Information and Information Systems to Security Categories** |
| **SP 800-59** | August 2003 | **Guideline for Identifying an Information System as a National Security System** |
| **SP 800-58** | January 2005 | **Security Considerations for Voice Over IP Systems** |
| **SP 800-57 Part 1 Rev. 4** | January 2016 | **Recommendation for Key Management, Part 1: General** |
|  |  |  |
| **SP 800-57 Part 2** | August 2005 | **Recommendation for Key Management, Part 2: Best Practices for Key Management Organization** |
| **SP 800-57 Part 3 Rev. 1** | January 2015 | **Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance** |
| **SP 800-56A Rev. 2** | May 2013 | **Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** |
|  |  |  |
| **SP 800-56B Rev. 1** | September 2014 | **Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography** |
| **SP 800-56C** | November 2011 | **Recommendation for Key Derivation through Extraction-then-Expansion** |
| **SP 800-55 Rev. 1** | July 2008 | **Performance Measurement Guide for Information Security** |
| **SP 800-54** | July 2007 | **Border Gateway Protocol Security**] |
| **SP 800-53A Rev. 4** | December 2014 (Updated 12/18/2014) | **Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans** |
|  |  |  |
|  |  |  |
|  |  |  |
| **SP 800-53 Rev. 5**  (Draft) | February 23, 2016 | **DRAFT PRE-DRAFT Call for Comments: Security and Privacy Controls for Federal Information Systems and Organizations** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-Rev.%205) |
| **SP 800-53 Rev. 4** | April 2013 (Updated 1/22/2015) | **Security and Privacy Controls for Federal Information Systems and Organizations** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **SP 800-52 Rev. 1** | April 2014 | **Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations** |
|  |  |  |
| **SP 800-51 Rev. 1** | February 2011 | **Guide to Using Vulnerability Naming Schemes** |
|  |  |  |
| **SP 800-50** | October 2003 | **Building an Information Technology Security Awareness and Training Program** |
| **SP 800-49** | November 2002 | **Federal S/MIME V3 Client Profile** |
| **SP 800-48 Rev. 1** | July 2008 | **Guide to Securing Legacy IEEE 802.11 Wireless Networks**] |
| **SP 800-47** | August 2002 | **Security Guide for Interconnecting Information Technology Systems** |
| **SP 800-46 Rev. 2** | July 2016 | **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** |
| **SP 800-45 Version 2** | February 2007 | **Guidelines on Electronic Mail Security** |
| **SP 800-44 Version 2** | September 2007 | **Guidelines on Securing Public Web Servers** |
| **SP 800-43** | November 2002 | **Systems Administration Guidance for Securing Windows 2000 Professional System** |
| **SP 800-41 Rev. 1** | September 2009 | **Guidelines on Firewalls and Firewall Policy** |
| **SP 800-40 Rev. 3** | July 2013 | **Guide to Enterprise Patch Management Technologies**] |
|  |  | [Press Release](http://www.nist.gov/itl/csd/guides-082013.cfm) |
| **SP 800-39** | March 2011 | **Managing Information Security Risk: Organization, Mission, and Information System View** |
|  |  |  |
| **SP 800-38A Addendum** | October 2010 | **Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode** |
| **SP 800-38A** | December 2001 | **Recommendation for Block Cipher Modes of Operation: Methods and Techniques** |
| **SP 800-38B** | May 2005 (Updated 10/6/2016) | **Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication** |
| **SP 800-38C** | May 2004 (Updated 7/20/2007) | **Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality** |
| **SP 800-38D** | November 2007 | **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** |
| **SP 800-38E** | January 2010 | **Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices** |
| **SP 800-38F** | December 2012 | **Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** |
| **SP 800-38G** | March 2016 | **Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption** |
|  |  |  |
| **SP 800-37 Rev. 1** | February 2010 (Updated 6/5/2014) | **Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach** |
|  |  |  |
|  |  |  |
| **SP 800-36** | October 2003 | **Guide to Selecting Information Technology Security Products** |
| **SP 800-35** | October 2003 | **Guide to Information Technology Security Services** |
| **SP 800-34 Rev. 1** | May 2010 (Updated 11/11/2010) | **Contingency Planning Guide for Federal Information Systems** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **SP 800-33** | December 2001 | **Underlying Technical Models for Information Technology Security** |
| **SP 800-32** | February 26, 2001 | **Introduction to Public Key Technology and the Federal PKI Infrastructure** |
| **SP 800-30 Rev. 1** | September 2012 | **Guide for Conducting Risk Assessments** |
|  |  |  |
|  |  |  |
| **SP 800-29** | June 2001 | **A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2** |
| **SP 800-28 Version 2** | March 2008 | **Guidelines on Active Content and Mobile Code** |
| **SP 800-27 Rev. A** | June 2004 | **Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A** |
| **SP 800-25** | October 2000 | **Federal Agency Use of Public Key Technology for Digital Signatures and Authentication** |
| **SP 800-24** | April 2001 | **PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does**] |
| **SP 800-23** | August 2000 | **Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products** |
| **SP 800-22 Rev. 1a** | April 2010 | **A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications** |
| **SP 800-20** | October 1999 (Updated 3/1/2012) | **Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures** |
| **SP 800-19** | October 1999 | **Mobile Agent Security** |
| **SP 800-18 Rev. 1** | February 2006 | **Guide for Developing Security Plans for Federal Information Systems** |
| **SP 800-17** | February 1998 | **Modes of Operation Validation System (MOVS): Requirements and Procedures** |
| **SP 800-16 Rev. 1**  (Draft) | March 2014 | **DRAFT A Role-Based Model for Federal Information Technology/Cybersecurity Training** |
| **SP 800-16** | April 1998 | **Information Technology Security Training Requirements: a Role- and Performance-Based Model** |
| **SP 800-15** | January 1998 | **MISPC Minimum Interoperability Specification for PKI Components, Version 1** |
| **SP 800-14** | September 1996 | **Generally Accepted Principles and Practices for Securing Information Technology Systems** |
| **SP 800-13** | October 1995 | **Telecommunications Security Guidelines for Telecommunications Management Network** |
| **SP 800-12** | October 1995 | **An Introduction to Computer Security: the NIST Handbook** |
| **SP 800-1** | December 1990 | **Bibliography of Selected Computer Security Publications, January 1980 - October 1989** |

Tablo 18: Wired ve Wireless Network’lerde NIST SP 800 Güvenlik Standartları

### 3.2 Wired ve Wireless Network’lerde Güvenliğe Dair NIST’in Belirlediği SP 1800 Seri Standartlar Listesi [127]

Bu seri standartlar, Wired ve Wireless Network’lerde güvenlikte, NIST SP 800 serisini standartlarını tamamlamak adına oluşturulan devam niteliğindeki standartlardır.

|  |  |  |
| --- | --- | --- |
| **SP 1800-6**  (Draft) | November 2016 | **DRAFT Domain Name Systems-Based Electronic Mail Security** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-6) |
| **SP 1800-5**  (Draft) | October 2015 | **DRAFT IT Asset Management: Financial Services** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-5) |
| **SP 1800-4**  (Draft) | November 2015 | **DRAFT Mobile Device Security: Cloud and Hybrid Builds** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-4) |
| **SP 1800-3**  (Draft) | September 2015 | **DRAFT Attribute Based Access Control** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-3) |
| **SP 1800-2**  (Draft) | August 2015 | **DRAFT Identity and Access Management for Electric Utilities** [Announcement and Draft Publication](http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-2) |
| **SP 1800-1**  (Draft) | July 2015 | **DRAFT Securing Electronic Health Records on Mobile Devices** |

Tablo 6.3.1: Wired ve Wireless Network’lerde NIST SP 1800 Güvenlik Standartları

## 6.4. ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union)

ITU Telecommunication Standardization Sector of the International Telecommunications Union, ITU’nün üç sektöründen (bölümler veya birimler) biridir ve telekomünikasyon standartlarını koordine eder.

Merkezi, İsviçre'nin Cenevre kentindeki olan kurum, buradaki daimî sekreterliği olan TSB’de faaliyetlerini yürütmektedir. ITU'nun standartlaştırma çabaları, 1865 yılında ITU kurulmasıyla başlamıştır. 1947'de de Birleşmiş Milletlerin İhtisas ajansı oldu. CCITT, (Fransızca'dan: Comité Consultatif International Téléphonique et Télégraphique) 1956'da kuruldu ve 1993'de ITU-T olarak yeniden adlandırıldı.

"CCITT" ‘nin yeniden yapılanması ile oluşturulan 'international telecomunication union', bugün veri haberleşmesi konusunda standartların çok büyük bir kısmını geliştirilmektedir. [128] [129]

### 6.4.1 ITU TarafındanYayınlanmış Kilit Standartlar

* [ASN.1](https://en.wikipedia.org/wiki/ASN.1) (Abstract Syntax Notation One)
* Coding of audio [G.711](https://en.wikipedia.org/wiki/G.711) and G.72x series
* Coding of still images [JPEG](https://en.wikipedia.org/wiki/JPEG) T.80 and [JPEG 2000](https://en.wikipedia.org/wiki/JPEG_2000) T.800 series
* Coding of video coding [H.262](https://en.wikipedia.org/wiki/H.262)/MPEG2-Video, [H.264](https://en.wikipedia.org/wiki/H.264)/MPEG-4 AVC and [H.265](https://en.wikipedia.org/wiki/H.265)/HEVC
* Construction, installation and protection of cables and other elements of outside plant, L-series
* [Data communication](https://en.wikipedia.org/wiki/Data_communication) over the telephone network, [V-series](https://en.wikipedia.org/wiki/ITU-T_V-Series_Recommendations)
* [Fax](https://en.wikipedia.org/wiki/Fax) standards T.2 – T.4, [T.30](https://en.wikipedia.org/wiki/T.30_(ITU-T_recommendation)), [T.37](https://en.wikipedia.org/wiki/T.37_(ITU-T_recommendation)), [T.38](https://en.wikipedia.org/wiki/T.38)
* [G.hn](https://en.wikipedia.org/wiki/G.hn) (Next generation wired home networking over powerlines, phonelines and coaxial cable)
* Green ICT standards and supplements ( L.1000 series)
* [H.323](https://en.wikipedia.org/wiki/H.323) family of standards for multimedia and [VoIP](https://en.wikipedia.org/wiki/VoIP)
* Interconnection rate harmonization, D-series
* International Emergency Preference Scheme E.106
* [IMSI](https://en.wikipedia.org/wiki/International_mobile_subscriber_identity) codes used in [SIM](https://en.wikipedia.org/wiki/Subscriber_Identity_Module) cards [E.212](https://en.wikipedia.org/wiki/E.212)
* [ISDN](https://en.wikipedia.org/wiki/ISDN) and [PSTN](https://en.wikipedia.org/wiki/PSTN)/[3G](https://en.wikipedia.org/wiki/3G) videoconferencing systems, [H.320](https://en.wikipedia.org/wiki/H.320) and [H.324](https://en.wikipedia.org/wiki/H.324)
* ISDN (Integrated Services Digital Network) [Q.931](https://en.wikipedia.org/wiki/Q.931)
* [Open Systems Interconnection](https://en.wikipedia.org/wiki/Open_Systems_Interconnection)
* [Optical Transport Network](https://en.wikipedia.org/wiki/Optical_Transport_Network) (OTN) [G.709](https://en.wikipedia.org/wiki/G.709), [G.798](https://en.wikipedia.org/wiki/G.798), G.872
* [Passive optical networks](https://en.wikipedia.org/wiki/Passive_optical_network) (PON) [G.983](https://en.wikipedia.org/wiki/G.983), [G.984](https://en.wikipedia.org/wiki/G.984), [G.987](https://en.wikipedia.org/wiki/G.987)
* [Public Key Infrastructure](https://en.wikipedia.org/wiki/Public_Key_Infrastructure) (PKI) [X.509](https://en.wikipedia.org/wiki/X.509)
* Public telecommunication numbering plan, [E.164](https://en.wikipedia.org/wiki/E.164)
* Security framework X.805
* [Signalling System 7](https://en.wikipedia.org/wiki/Signalling_System_7) Q.7xx series
* Standards relating to [Quality of Service](https://en.wikipedia.org/wiki/Quality_of_Service) (QoS)
* [Specification and Description Language](https://en.wikipedia.org/wiki/Specification_and_Description_Language)
* [Synchronous Digital Hierarchy](https://en.wikipedia.org/wiki/Synchronous_Digital_Hierarchy) (SDH) G.707, [G.783](https://en.wikipedia.org/wiki/G.783), G.803
* [Wavelength-division multiplexing](https://en.wikipedia.org/wiki/Wavelength-division_multiplexing) (WDM)
* [X.25](https://en.wikipedia.org/wiki/X.25)
* (x)[DSL](https://en.wikipedia.org/wiki/DSL) (Digital Subscriber Line) series of standards for broadband telecoms
* [128] [129]

## 6.5. ISOC (internet society)

The Internet Society, internet'in açık, şeffaf ve kullanıcılar tarafından tanımlanan şekliyle kalmasını sağlamaya adanmış çeşitli müttefikler kurulu tarafından yönetilen, nedene dayalı bir organizasyondur.

İnternet politikası, teknoloji standartları ve geleceğin geliştirilmesi için dünyanın güvenilir bağımsız liderlik kaynaklarından biridir. Teknolojinin ilerlemesinden öte, internet'in yenilik, ekonomik kalkınma ve dünya çapında insanlar için sosyal ilerleme için bir platform olarak büyümeye ve gelişmeye devam etmesini sağlamak için çalışmalar yürütür. 80.000'in üzerinde üye ve destekçisi olan bu kurum, dünyanın her tarafında 113 Bölüm ve 143'ü aşkın organizasyon üyesi tarafından desteklenmekte, politika, teknoloji ve iletişim alanında ortaklık ve uzmanlık yoluyla değişim sağlamaktadır.

Internet Society üç ana kategoride, yani standartlar, kamu politikası, erişim ve eğitim altında çok çeşitli faaliyetler yürütür. Ağ altyapısını kendi bölgelerinde kurabilen ve koruyabilen bireyler yetiştirmenin yanı sıra, ağ geliştirme, arabağlantı ve internet trafik alışverişini desteklemek için ülkeler ve topluluk ortaklarıyla birlikte çalışır.

Standartlar kategorisinde Internet Society, örgütsel ev olduğu standart ayar organlarının çalışmalarını desteklemekte ve desteklemektedir. Bu standart ayar organları;

1. [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF),
2. [Internet Architecture Board](https://en.wikipedia.org/wiki/Internet_Architecture_Board)(IAB),
3. [Internet Engineering Steering Group](https://en.wikipedia.org/wiki/Internet_Engineering_Steering_Group)(IESG)
4. [Internet Research Task Force](https://en.wikipedia.org/wiki/Internet_Research_Task_Force)(IRTF).

### 6.5.1 [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) –IETF

Internet Engineering Task Force (IETF), internet protokol paketini (TCP / IP) oluşturan standartlar olmak üzere gönüllü internet standartlarını geliştirir ve destekler. Resmi bir üyelik ya da üyelik gerekliliği olmaksızın, açık bir standart organizasyonudur. Tüm katılımcılar ve yöneticiler gönüllüdür, ancak çalışmalar genellikle işverenler veya sponsorlar tarafından finanse edilmektedir.

IETF, ABD federal hükümeti tarafından desteklenen bir etkinlik olarak başladı ancak 1993'ten beri, uluslararası üyelik tabanlı kar amacı gütmeyen bir organizasyon olan İnternet Topluluğu'nun himayesinde bir standart geliştirme fonksiyonu olarak faaliyet gösterdi. [130]

### 6.5.2 The Internet Architecture Board-IAB

The Internet Architecture Board (IAB), IETF ve ISOC bir danışma organı olan komitesi olup, IETF faaliyetlerinin mimari gözetimi, internet standartları süreci gözetim ve temyizi, RFC Editörünün atanması ve IETF protokol parametre kayıtlarının yönetimi gibi faaliyetleri yürütür. Bu konulardaki tek sorumlu birim olarak görevlendirilmiştir. [131]

Eninde sonunda IAB haline gelen bu birim ilk olarak Birleşik Devletlerinin Defense's Defense Advanced Research Projects Agency Kurumu tarafından 1979'da Internet Yapılandırma Kontrol Kurulu adı altında oluşturuldu, sonunda Eylül 1984'te Internet Danışma Kurulu'na, sonra da Mayıs 1986'da İnternet Faaliyetleri Kurulu'na (adı kısaltıp aynı kısaltmayı değiştirmedi) döndü. Nihayet, İnternet'in ABD hükümet teşkilatından uluslararası, kamuya açık bir kuruluşa geçişinin bir parçası olarak, Ocak 1992'de ISOC bünyesinde İnternet Mimarlık Kurulu haline geldi. [132]

### 6.5.3 Internet Engineering Steering Group-IESG

Internet Engineering Steering Group, IETF başkanı ve bölge müdürlerinden oluşan bir organtır. İnternet standartlarının nihai teknik incelemesini yapar ve IETF'nin günlük yönetiminden sorumludur. Çalışma gruplarının kararlarının temyiz edilmesini ve IESG’nin belgelerin standartlar doğrultusunda ilerleme kararı vermesini sağlamaktadır. [133]

### 6.5.4 The Internet Research Task Force -IRTF

The Internet Research Task Force, internetle ilgili uzun vadeli araştırma konularına odaklanırken, paralel organizasyon olan IETF, mühendislik ve standartların hazırlanmasıyla ilgili daha kısa vadeli konularda yoğunlaşır. IRTF, internet protokolleri, uygulamaları, mimarisi ve teknolojisi ile ilgili konular üzerine çalışan odaklı, uzun vadeli araştırma grupları oluşturarak internetin evrimine önem veren araştırmaları desteklemektedir. [134]

### 6.5.5 RFC (Request for Comments)

RFC, internet'in temel teknik gelişme ve standart belirleme organları olan IETF ve Internet Society (ISOC) tarafından yapılan bir standart yayın türüdür.

RFC, internet ve internet'e bağlı sistemlerin çalışması için uygulanabilir yöntemler, davranışlar, araştırma veya yenilikleri açıklayan bir mutabakat formunda mühendisler ve bilgisayar bilimcileri tarafından yazılmıştır. Akran değerlendirmesi için veya sadece yeni kavramlar, bilgi ya da (zaman zaman) mühendislik mizahı iletmek için yayınlanır. IETF, RFC olarak yayınlanan bazı önerilerini internet standardları olarak kabul etmektedir.

Request for Comments belgeleri 1969'da ARPANET'in gelişimi hakkında resmi olmayan notlar kaydetmek için Steve Crocker tarafından icat edildi. RFC'ler o zamandan beri internet spesifikasyonlarının, iletişim protokollerinin, prosedürlerinin ve olaylarının resmi belgeleri haline gelmiştir. [135]

Günümüzde, internet alanının sık kullanılan terimlerinden biri haline gelen RFC, bizler tarafından da internet standartlarını belirtirken kullanılmaktadır. Her bir internet protokolü mekanizması için bu protokolleri ve bu mekanizmaları tanımlayan bir RFC vardır. Örnek verecek olursak TCP RFC 793’de tanımlanmıştır. Bazı diğer tanımlamalar aşağıda verilmiştir. Fakat biz bu bölümde genel anlamda daha çok bilgisayar ağları ve bu ağlarda güvenlik ile ilgili standart örneklerini verdik. Bundan daha fazla RFC standartları mevcuttur.

* [RFC 1](https://tools.ietf.org/html/rfc1)
* [RFC 768](https://tools.ietf.org/html/rfc768) (UDP)
* [RFC 791](https://tools.ietf.org/html/rfc791) (IP)
* [RFC 792](https://tools.ietf.org/html/rfc792) (ICMP)
* [RFC 793](https://tools.ietf.org/html/rfc793) (TCP)
* [RFC 959](https://tools.ietf.org/html/rfc959) (FTP)
* [RFC 1006](https://tools.ietf.org/html/rfc1006) (ISO on TCP – ISO Transport Service on top of the TCP)
* [RFC 1034](https://tools.ietf.org/html/rfc1034) (DNS)
* [RFC 1035](https://tools.ietf.org/html/rfc1035) (DNS)
* [RFC 1094](https://tools.ietf.org/html/rfc1094) (NFS)
* [RFC 1166](https://tools.ietf.org/html/rfc1166) (IP adresi)
* [RFC 1321](https://tools.ietf.org/html/rfc1321) (MD5)
* [RFC 1459](https://tools.ietf.org/html/rfc1459) (IRC)
* [RFC 1661](https://tools.ietf.org/html/rfc1661) (PPP)
* [RFC 1738](https://tools.ietf.org/html/rfc1738) (URL)
* [RFC 1813](https://tools.ietf.org/html/rfc1813) (NFS)
* [RFC 1855](https://tools.ietf.org/html/rfc1855)
* [RFC 1939](https://tools.ietf.org/html/rfc1939) (POP3)
* [RFC 2131](https://tools.ietf.org/html/rfc2131) (DHCP)
* [RFC 2222](https://tools.ietf.org/html/rfc2222) (SASL)
* [RFC 2251](https://tools.ietf.org/html/rfc2251) (LDAP)
* [RFC 2440](https://tools.ietf.org/html/rfc2440)
* [RFC 2445](https://tools.ietf.org/html/rfc2445) (iCalendar)
* [RFC 2460](https://tools.ietf.org/html/rfc2460) (IPv6)
* [RFC 2613](https://tools.ietf.org/html/rfc2613) (Remote Network Monitoring)
* [RFC 2616](https://tools.ietf.org/html/rfc2616) (HTTP)
* [RFC 2821](https://tools.ietf.org/html/rfc2821) (SMTP)
* [RFC 2822](https://tools.ietf.org/html/rfc2822) (Elektronik posta-Format)
* [RFC 3174](https://tools.ietf.org/html/rfc3174) (SHA)
* [RFC 3501](https://tools.ietf.org/html/rfc3501) (IMAP Version 4)
* [RFC 3530](https://tools.ietf.org/html/rfc3530) (NFS)
* [RFC 3986](https://tools.ietf.org/html/rfc3986) (URI)

## 6.6 ETSI (European Telecommunications Standards Institute)

European Telecommunications Standards Institute(ETSI), Avrupa için telekomünikasyon standartlarını belirleyen kar amacı gütmeyen bir kuruluştur. ETSI kuralları gönüllüdür ve neredeyse her zaman uluslararası organların ürettiği standartlara uygundur. [137]

ETSI girişimleri, havacılık radyo, API, ATM, elektromanyetik uyumluluk, elektronik imza, Genel Adresleme ve Taşıma protokolü, deniz telsizi, servis sağlayıcı erişimi, TMN, TETRA, VoIP ve xDSL gibi alanlara değinmektedir. ETSI'nin yapısı genel kurul, yönetim kurulu, teknik organizasyon ve bir sekretarya içerir. Teknik organizasyon, standartlar tasarlamakla birinci derecede sorumlu olan organdır. [137]

ETSI'nin merkezi güney Fransa'da yer almaktadır ve halen bünyesinde 68 ülke ve beş kıtadan 800 üye barındırmaktadır. Üyelik listesinde IBM Avrupa, Microsoft Avrupa, Hewlett-Packard France, Motorola ve Lucent Technologies gibi teknolojideki en büyük isimlerin bazıları bulunmaktadır. Üyelik, Avrupa telekomünikasyonuna ilgi duyan herhangi bir firmaya açıktır. Her üye, ETSI'ye katılmak için yıllık bir ücret ödemektedir. [137]

### 6.6.1 ETSI Standartları

6.6.1.1 European Standard, telecommunications series (EN): Bu belge Avrupa'ya özgü gereksinimleri karşılamak ve ulusal standartlara aktarılmasını gerektirdiği veya belgenin taslağının bir AT / EFTA yetkisi altında istenmesi durumunda kullanılır. [136]

6.6.1.2 ETSI Standard (ES): Bu belge normatif gereklilikler içerildiğinde kullanılır ve onay için belgeyi tüm ETSI üyeliğine teslim etmek gerekir. [136]

6.6.1.3 ETSI Guide (EG): Bu belgede teknik standartlaştırma faaliyetlerinin yürütülmesine ilişkin rehberlik varsa, onay için tüm ETSI üyeliğine sunulur. [136]

6.6.1.4 Special Report (SR): Bir teknik komitede üretilmeyen bilgilere halkın erişebilmesini sağlamak da dahil olmak üzere çeşitli amaçlarla kullanılır. ETSI SR'ler "sanal" belgeler için de kullanılır, örn. Web üzerinden bir veritabanına bir sorgu tarafından dinamik olarak üretilen dokümanlar. Bir SR, üretildiği teknik komite tarafından yayınlanır. [136]

6.6.1.5 ETSI Technical Specification (TS): Belge normatif gereklilikleri içerdiğinde ve kısa pazarlama zamanı, geçerlilik ve bakım şartlarının önemli olduğu durumlarda kullanılır, taslak hazırlanan teknik komite tarafından onaylanır. [136]

6.6.1.6 ETSI Technical Report (TR): Bu belgede esas olarak bilgilendirici öğeler bulunduğu zaman, taslak hazırlanan teknik komite tarafından onaylanmıştır. [136]

6.6.1.7 ETSI Group Specification (GS): Grup'un Görev Tanımı'nda tanımlanan karar verme prosedürlerine göre Sanayi Spesifikasyon Grupları tarafından kullanılır. Bu teslim edilebilir tip, taslak hazırlanan Endüstri Spesifikasyon Grubu tarafından onaylanmış ve kabul edilmiştir. [136]

## 6.7 OMTP (Open Mobile Terminal Platform)

Open Mobile Terminal Platform (OMTP), mobil şebeke operatörleri tarafından cep telefonları ve diğer mobil cihaz üreticileri ile standartları görüşmek üzere hazırlanan bir forum olarak ortaya çıkmıştır.

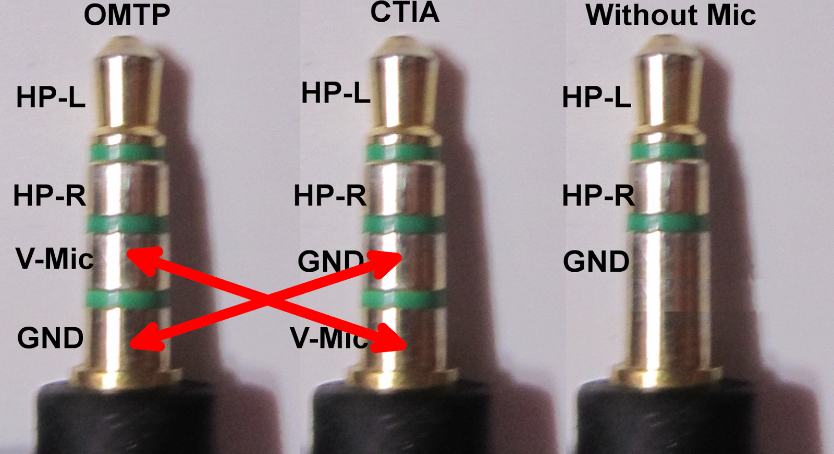
OMTP önerileri mobil operatör terminal gereksinimlerini standartlaştırmaya büyük ölçüde yardımcı olmuş ve çalışmalarını operatör önerilerini birleştirip deoptionalize etmeye yardımcı olmak için geliştirmiştir. OMTP'nin odak noktası mobil terminal gereksinimlerini toplamak ve kullanmak, bulgularını ise Tavsiyelerinde yayınlamaktır. OMTP, teknoloji platformlarından, işletim sistemlerinden (OS) ve ara katman katmanlarından istifade etmeyi amaçlayan önerileri ile teknoloji açısından tarafsız bir politika izlemektedir.

OMTP, belki de en iyi cep telefonu güvenliği alanında yaptığı çalışmalarla bilinir ve çalışmalarının neredeyse tümü mobil cihaz yeteneklerini kapsamaktadır. OMTP, Positioning Enablers, Advanced Device Management, IMS ve Mobil VoIP gibi alanlarda 2007 ve 2008 yılının başında öneriler yayınlamış, daha sonra Advanced Trusted Environment: OMTP TR1 [138] ve Birleşik Krallık İç Sekreteri Jacqui Smith'in onayını alıp, Gömülü Tüketici Cihazları Üzerindeki Güvenlik Tehditlerini [139] destekleyici bir belge yayınlamıştır. [140]

OMTP ayrıca gelişmiş SIM kartlar için destek talebi dokümanlarını yayınladı. Bu belge, Akıllı Kart Web Sunucusu, Yüksek Hızlı Protokol, Mobil TV ve Temassız için gelişmiş profilleri tanımlamaktadır. [141]

OMTP, veri ve güç için standart bir konektör olarak mikro USB kullanımına destek verilmesinde önemli ilerleme kaydetmiştir. [142]

Şekil 6.7’de OMTP standardı ve diğer standart şekilleriyle karşılaştırılması gösterilmiştir.



Şekil 6.7: OMTP Standard Örneği

## 6.8 GSMA (The GSM Association)

GSM Association (genelde 'GSMA' olarak anılır), dünya genelindeki mobil operatörlerin çıkarlarını temsil eden bir ticaret kurumudur. 1995 yılında GSM mobil standardı kullanan mobil operatörleri desteklemek ve tanıtmak için bir kuruluş olan 'GSM MoU Birliği' olarak kurulan bu kurum [144], yaklaşık 800 mobil operatörü tam üye,300 şirketi de ortak üye olarak bünyesinde barındırmaktadır. GSMA üyelerini endüstri programları, çalışma grupları ve endüstri savunuculuğu girişimleri aracılığıyla temsil eder. Aynı zamanda, mobil endüstrinin en büyük yıllık sergi ve konferansını, GSMA Mobil Dünya Kongresi'ni ve diğer birçok etkinliği organize etmektedir.

GSMA'nın merkezi Londra olmak üzere, Atlanta, Hong Kong, Şangay, Barselona, Brüksel, Brasilia, Nairobi ve Yeni Delhi'de de bölge müdürlükleri mevcuttur. [143]

GSMA, yeni mobil teknolojiler için ölçek ve birlikte çalışabilirlik sağlamak amacıyla endüstri programlarını üyeleriyle iş birliği içinde yönetir. Dört aktif programı vardır: Kişisel Veriler; Bağlı Yaşam (Nesnekerin Internetine Odaklanmış); Ağ 2020 (RCS ve VoLTE gibi standartların geliştirilmesi); Ve Dijital Ticaret.

Ayrıca dolaşım ve arabağlantı, dolandırıcılık, güvenlik ve fikri mülkiyet gibi alanlarda ve çeşitli diğer uzman komitelerde ve gruplarda endüstri çalışma grupları yürütür. [145]

GSMA, mobil endüstriyi hükümetler ve kurumlara karşı temsil etmektedir. Bu alandaki hedefleri, mobil telekomünikasyonların "politika ve düzenleyici çerçevelerin adil, esnek ve geleceğe yönelik olmasını" sağlamaktır. Bu spektrum "zamanında ve adil bir şekilde" mobil hizmetler için kullanılabilir hale getirildi ve gelişmekte olan pazarlarda mobil hizmetlerin kullanımı bu sayede teşvik edilmiştir. [146]

Ayrıca Sanayi Amaçlı Programının bir parçası olarak, GSMA Birleşmiş Milletlerin Sürdürülebilir Kalkınma Hedeflerini desteklemektedir. [147]. Tablo 8’de GSM güvenliği üzerine yayınlanmış GSMA standartlar listesi görülmektedir.

|  |  |
| --- | --- |
| [Specification of the 3GPP Confidentiality and Integrity Algorithms: F8 and F9 Specifications](javascript:var%20handle=window.open('http://portal.etsi.org/dvbandca/3GPPSPECIFICATIONS/3GTS35.201%20ver1.2.pdf')) |  |
| [Specification of the 3GPP Confidentiality and Integrity Algorithms: KASUMI Algorithm Specification](javascript:var%20handle=window.open('http://portal.etsi.org/dvbandca/3GPPSPECIFICATIONS/3GTS35.202.pdf')) |  |
| [Specification of the 3GPP Confidentiality and Integrity Algorithms: Implementors’ Test Data](javascript:var%20handle=window.open('http://portal.etsi.org/dvbandca/3GPPSPECIFICATIONS/3GTS35.203.pdf')) |  |
| [Specification of the 3GPP Confidentiality and Integrity Algorithms: Design Conformance Test Data](javascript:var%20handle=window.open('http://portal.etsi.org/dvbandca/3GPPSPECIFICATIONS/3GTS35.204.pdf')) |  |
| [European Communications Standards Institute: Security Algorithms & Codes](javascript:var%20handle=window.open('http://portal.etsi.org/dvbandca/home.asp')) |  |
| [TS 33.120, Security principles and objectives](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33120-300.zip) |  |
| [TS 21.133, Security threats and requirements](ftp://ftp.3gpp.org/Specs/2000-12/R1999/21_series/21133-310.zip) |  |
| [TR 33.102, 3GPP security architecture](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33102-370.zip) |  |
| [TR 33.103, Integration guidelines](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33103-340.zip) |  |
| [TR 33.105, Cryptographic algorithm requirements](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33105-360.zip) |  |
| [TR 22.022, Personalization of mobile equipment](ftp://ftp.3gpp.org/Specs/2000-12/R1999/22_series/22022-310.zip) |  |
| [TR 33.106, Lawful interception requirements](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33106-310.zip) |  |
| [TR 33.107, Lawful interception architecture and functions](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33107-310.zip) |  |
| [TR 33.900, A guide to 3G security](ftp://ftp.3gpp.org/TSG_SA/WG3_Security/_Specs/33900-120.pdf) |  |
| [TR 33.901, Criteria for cryptographic algorithm design process](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33901-300.zip) |  |
| [TR 33.902, Formal analysis of the 3G authentication protocol](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33902-310.zip) |  |
| [TR 33.908, General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms](ftp://ftp.3gpp.org/Specs/2000-12/R1999/33_series/33908-300.zip) |  |
| [ETSI SAGE Task Force for 3GPP Authentication Function Algorithms](ftp://ftp.3gpp.org/TSG_SA/WG3_Security/2000_meetings/TSGS3_16_Sophia_Antipolis/Docs/PDF/S3-000730.pdf) |  |
| [SIP (Session Initiation Protocol) Center](javascript:var%20handle=window.open('http://www.sipcenter.com/')) |  |
| [3GPP Group Security Specifications](javascript:var%20handle=window.open('http://www.3gpp.org/TB/sa/sa3/specs.htm')) |  |
| [GSM ETSI 2.81 – Line identification Supplementary Services – Stage 1](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/archive/02_series/02.81/0281-510.zip')) |  |
| [GSM ETSI 3.38 – Alphabets and language-specific information](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/archive/03_series/03.38/0338-700.zip')) |  |
| [GSM ETSI 3.40 – Technical realization of the](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/archive/03_series/03.40/0340-600.zip'))[Short Message Service (SMS)](http://www.tech-faq.com/sms-short-message-service.shtml); Point-to-Point (PP) |  |
| [GSM ETSI 3.83 – Call Waiting (CW) and Call Hold (HOLD) supplementary services – Stage 2](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/2001-06/R1996/03_series/0383-500.zip')) |  |
| [GSM ETSI 3.90 – Unstructured Supplementary Service Data (USSD) – Stage 2](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/2001-06/R1996/03_series/0390-500.zip')) |  |
| [GSM ETSI 4.85 – Closed User Group (CUG) supplementary services – Stage 3](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/2000-12/R1996/04_series/0485-500.zip')) |  |
| [GSM ETSI 7.05 – Use of Data Terminal Equipment – Data Circuit terminating; Equipment (DTE – DCE) interface for Short Message Service (SMS) and Cell Broadcast Service (CBS)](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/2001-09/R1996/07_series/0705-550.zip')) |  |
| [GSM ETSI 7.07 – AT command set for GSM Mobile Equipment (ME)](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/archive/07_series/07.07/0707-700.zip')) |  |
| [GSM ETSI 9.05 – Interworking between the Public Land Mobile Network (PLMN) and the Packet Switched Public Data Network (PSPDN) for Packet Assembly/Disassembly (PAD) facility access](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/2002-03/R1996/09_series/0905-500.zip')) |  |
| [GSM ETSI 11.11 – Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/archive/11_series/11.11/1111-620.zip')) |  |
| [GSM ETSI 11.11 – Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface](javascript:var%20handle=window.open('http://www.3gpp.org/ftp/Specs/html-info/1114.htm')) |  |

Tablo 6.8: GSM Güvenlik standartları

## 6.9. TCG (Trusted Computing Group)

Trusted Computing Group, kişisel bilgisayarlar arasında Trusted Computing kavramlarını uygulamak için AMD, Hewlett-Packard, IBM, Intel ve Microsoft tarafından oluşturulan bir gruptur. Trusted Computing Group, daha önce 1999'da kurulmuş olan Trusted Computing Platform Alliance'ın ardılı olarak 2003 yılında ilan edildi. [148] Diğer birçok şirket de, Wave Systems Corp, [149] Digital Management, Inc, [150] Cisco, Lenovo, Infineon, Juniper Networks ve Fujitsu gibi Trusted Computing Group'a katılmıştır.

TCG'nin asıl hedefi, Trusted Computing Group tarafından ileri sürülen ve güvenilir hesaplamayı etkinleştirmek için bilgisayarlara dahil edilecek olan güvenilir platform modülü spesifikasyonuna uygun bir yarıiletken fikri mülkiyet çekirdeği veya entegre devrenin bir Trusted Platform Module (TPM) şeklinin geliştirilmesidir. TCG uyumlu işlevsellik o zamandan beri belirli kitlesel pazar yonga setlerine doğrudan entegre edilmiştir. TCG ayrıca kısa bir süre önce, AAA ilkelerine dayanan, Trusted Network Connect ("TNC") protokol belirtiminin ilk sürümünü de piyasaya sunmuştur.

2009 yılında TCG, kendiliğinden şifreleyen disk sürücüleri ile iletişim protokolünü açıklayan bir dizi spesifikasyon yayımladı. TCG Depolama Alanı Çalışma Grubu (SWG) Depolama Alanı Çekirdek Mimarisi Spesifikasyonu, depolama aygıtlarındaki güven ve güvenlik hizmetlerini nasıl uygulanıp, kullanılacağını ayrıntılı olarak açıklamaktadır. Güvenlik Alt Sistem Sınıfı (SSC) Spesifikasyonları daspesifik sınıflardaki cihazların gereksinimlerini açıklar; Özellikle Enterprise SSC, Veri Merkezi ve Sunucu Sınıfı cihazlar için minimum gereksinimleri tanımlarken Opal SSC, istemci cihazlar için minimum gereksinimleri de ayrıca tanımlamaktadır. [154]

### 6.9.1 Bir TCG Standardı: TPM

TCG tarafından ortaya konan bir standart çalışma olan TPM günümüzde birçok bilgisayar üzerinde hazır gelen donanım tabanlı bir çeşit güvenlik ve kriptografi yongasıdır. Bu yonga içerisinde dijital sertifika, kriptografik anahtarlar, parolalar ve benzeri birçok gizli bilgi barındırılır. Güvenilir Platform Modülü olarak adlandırabileceğimiz TPM temel manada anakarta lehimlenmiş bir yonga ve söküp götürmenize olanak olmayan bir yapıdadır. Bilgisayarda bir şifreleme yapılmak istenildiğinde TPM yongasına ihtiyaç duyulur zira benzersiz şifre anahtarlarının tamamı veya bir kısmı bu yonga üzerine kaydedilir. Bu bakımdan anahtarlara erişim zordur ve güvenli bir şifreleme imkânı sunulur. Lehimli olduğu için sadece o anakartta geçerlidir ve söküp başka bir anakarta takılsa bile anahtarlara erişilemez.

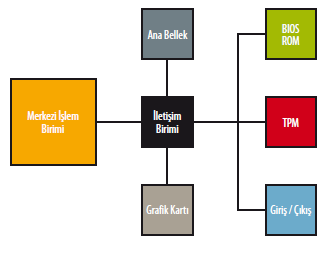
Windows tarafında sunulan BitLocker sürücü şifrelemesi, TPM yongası gerektirir. Ayrıca Windows 8.1 ve 10 ile birlikte gelen cihaz şifrelemesi özelliği de yine TPM yongasına ihtiyaç duyar. Bu şifrelemelerdeki benzersiz anahtarlar TPM üzerinde saklanır. Eğer kullanıcı şifreli sürücüyü çıkararak başka bir TPM destekli anakarta takmak isterse daha uzun kurtarma anahtarını da yanına alması gerekmektedir.

TPM yongası genelde anakartlara lehimli olarak gelmektedir ancak olmadığı durumlarda eğer anakart destekliyorsa ek bir modül olarak satın alınıp takılabilinir. Güvenli olduğu için tercih edilse de sadece yazılım olarak sürücü şifrelemesi yapılabilmektedir. Windows'ta yer alan EFS buna bir örnektir. Ayrıca Bitlocker'ın gizlenmiş olan TPM gerektirmeme özelliğini aktif hale getirilerek yine yazılım bazlı şifreleme yapılabilir. TPM modülleri günümüzde Intel, Toshiba, Atmel, Infineon gibi firmalar tarafından üretmektedir.

TPM modülleri ile ilgili ilginç bir detay ise bazı ülkelerde yasaklı olmasıdır. Benzersiz anahtarlara ulusal güvenliğin söz konusu olduğu durumlarda ulaşmak isteyen ülkeler, TPM kullanımını engelliyor. Hali hazırda Çin, Rusya, Beyaz Rusya ve Kazakistan'da TPM entegrasyonu yasak.  [151] [152] [153] [154]

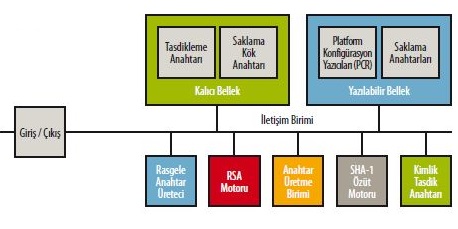
#### 6.9.1.1 TPM’nin İşlevi

TPM’in birçok işlevi vardır. Bu işlevlerden bazıları anahtar yönetimi, üzerinde çalıştığı PC’nin kimliğini doğrulama, elektronik belgeler ve e-postalar üzerinde güvenli elektronik imzalama, şifreleme, şifre çözme işlemlerini gerçekleştirmedir. Tam-sürücü şifrelemeyi yönetme, çok yönlü doğrulamada, ikinci faktör olarak görev yapma ve üzerinde bulunduğu bilgisayarın güvenliğini ve bütünlüğünü değerlendirmeye yardımcı olma diğer bazı işlevlerdendir. TPM, bilgisayarın ana kartına temel işlevi birtakım kriptografik işlemleri yerine getirmek olan ayrı bir bütünleşmiş devre konulmasını gerektirir. [156] [157] [158]



Şekil 6.9.1.1: TPM’nin işletim sistemi mimarisindeki yeri [155].

TPM, bir yardımcı işlemci olarak çalışan temel olarak kriptografik bir işlemcidir. Ana işlevi, kriptografik anahtarları korumak ve bazı kriptografik işlemlerin güvenli bir şekilde yapılmasını sağlamaktır. Bir diğer bakış açısı ile TPM, devresi yazılımın bir türlü sağlayamadığı güven kaynağı rolünü oynar. [156] [157] [158]



Şekil 6.9.1.1.a.: TPM içyapısı [155].

Şekil 6.9.1.1.a’da görüldüğü üzere, TPM’nin temel özelliği gizli anahtarları içerisinde saklaması. Diğer bir değişle, RSA ve SHA-1 gibi şifreleme ve özgünlük denetimi işlemlerinde kullanılan standartlaştırılmış kriptografik algoritmaların güvenli bir şekilde çalıştırılmasını sağlamaktır. Kullanıcıya açık, simetrik bir şifreleme algoritması şartnamelerin zorunlu bir parçası değildir. Bunun nedeni, TPM’nin öbek şifreleme işlemlerinde, örneğin dosya şifreleme işlemlerinde, kullanılmamasıdır. Bu işlem standart bir simetrik şifreleme algoritmasıyla, yazılım olarak gerçeklenebilir. TPM’nin buradaki katkısı, simetrik şifrelemede kullanılan gizli anahtarı şifrelemek ve ancak sistem güvenilir bir durumdayken, bu anahtarı o anda çalışan yetkilendirilmiş sürecin kullanımına açmaktır. [156] [157] [158]

#### 6.9.1.2TPM’de Güvenliğin Sağlanması

Şifreleme anahtarlarının korunması, elektronik imzalama işlemlerinin yapılması gibi TPM’nin birçok işlevi vardır. Bu işlevlerin en önemlilerinden biride güvenilir önyüklemedir. Gün geçtikçe yeni çıkan teknolojilerde bilgisayarların açılma süresinin kısalması gerekirken uzadığı fark edilmiştir. Bunu sebebi, arka planda çalışmaya başlayan onlarca programdır. Normal olarak bilgisayarı ilk çalıştırdığımızda, ROM içinde bulunan BIOS bilgisayarın giriş-çıkış işlemlerini yürütmeye başlar ve diğer programları çalıştırır. [156] [157] [158]

TPM’li bir bilgisayar açılışında ise ilk olarak BIOS’un küçük bir kısmı yürütülür. BIOS’un bu kısmı ve TPM bilgisayarın güven kaynağını oluştururlar. Bunlar üreticiler tarafından gerçekleştirildiği için ve yazılım kısmı da yeterince küçük olduğundan saldırılara karşı daha dayanıklıdırlar, hata barındırma olasılıkları daha düşüktür. Kısmi BIOS yüklendikten sonra sıra BIOS programının geri kalan kısmının yüklenmesine gelir. TPM bir sorgulama ertesinde, gerekli kısmı imzalar ve sorgulayan tarafa gönderir. Böylece karşı taraf, o bilgisayara güvenip güvenemeyeceğine imza onaylama işleminin sonucuna göre karar verir. [156] [157] [158]

## 6.10. IEEE (Institute of Electrical and Electronics Engineers)

The Institute of Electrical and Electronics Engineers ya da kısaca IEEE, [elektrik](https://tr.wikipedia.org/wiki/Elektrik), [elektronik](https://tr.wikipedia.org/wiki/Elektronik), [bilgisayar](https://tr.wikipedia.org/wiki/Bilgisayar), [otomasyon](https://tr.wikipedia.org/wiki/Otomasyon), [telekomünikasyon](https://tr.wikipedia.org/wiki/Telekom%C3%BCnikasyon) ve diğer birçok alanda, [mühendislik](https://tr.wikipedia.org/wiki/M%C3%BChendislik) teori ve uygulamalarının gelişimi için çalışan, kar amacı olmayan, dünyanın önde gelen teknik standart organizasyonudur.

1884 yılında [Alexander Graham Bell](https://tr.wikipedia.org/wiki/Alexander_Graham_Bell) ve [Thomas Edison](https://tr.wikipedia.org/wiki/Thomas_Edison) gibi dönemin büyük bilim adamlarınca temelleri atılmıştır.

150 ülkede 426.000'i aşkın üyesi (71.000'i öğrenci) ile IEEE, tüm dünyaya yayılmış 10 alt bölgesi, 300'den fazla yerel bölgesi ve 1430'dan fazla öğrenci koluyla çalışmalarını sürdürmektedir. Türkiye'nin de içinde bulunduğu 8. Bölge'de (Avrupa, Ortadoğu ve Afrika) 5000'i öğrenci üye olmak üzere 26.000 üyesi vardır.

Dünyada elektrik, elektronik mühendisliği, bilgisayar ve otomasyon teknolojilerindeki yayınların %30'unu yayınlar. Bu alanlarda, 80'den fazla yayını olan 37 farklı teknik topluluk vardır ve 900'den fazla endüstri standardı geliştirilmiştir. [159]

### 6.10.1 Network and Information Security (NIS) Alanında IEEE Standart Faaliyetlerine Genel Bakış

IEEE, şebeke ve bilgi güvenliği alanında, şifreleme, sabit ve çıkarılabilir depolama ve basılı kopya cihazları alanlarında ve bu teknolojilerin akıllı şebekelerde uygulamaları dahil olmak üzere anti-malware teknolojilerinde standartlaştırma faaliyetlerine sahiptir. [160]

IEEE'nin en büyük teknik topluluğu olan IEEE Bilgisayar Topluluğu, ağ ve bilgi güvenliği çabalarında teknik uzmanlık sağlamak için çok iyi donanıma sahiptir. Bunun yanında, otuz yılı aşkın bir süredir, bilgisayar güvenliği ve gizliliğine odaklanan kaliteli bir teknik komitesi vardır. Bu komite, bilgi güvenliği endüstrisinde en üst düzey düşünürler tarafından makaleleri bulunan saygın IEEE Security & Privacy dergisini yayınlamaktadır. Ayrıca, uzun süredir, kurulmuş olan iki önde gelen teknik toplantı olan IEEE Security and Privacy Symposium ve Computer Security Foundation Workshop’u desteklemektedir. [160]

IEEE'nin Industry Connections Security (Endüstri Bağlantıları Güvenlik) Grubu, paydaşların yeni zararlı yazılım ortamına yanıt vermeleri için esnek ve çevik bir platform sağlayan başka bir önemli etkinliği olarak göze çarpmaktadır. Üç önemli etkinliği vardır: [160]

* + Bireysel güvenlik şirketlerinin ve endüstrinin çağdaş kötücül yazılım tehditlerine ve hızla değişen evrene daha etkin ve etkili bir şekilde yanıt vermelerini sağlayan bir dizi paylaşımlı destek hizmeti olan IEEE Anti-Malware Support Service (Kötü Amaçlı Yazılım Destek Hizmeti-AMSS). AMSS şu anda iki ana hizmetten oluşmaktadır: Temizlik dosyası olan Clean file Metadata eXchange (CMX) ve Taggant Sistemi.
  + Kötü amaçlı yazılım bilgilerini paylaşmanın daha iyi yollarını geliştiren, bilgisayar güvenlik endüstrisinin kötü amaçlı yazılım tehditlerine daha etkili bir şekilde cevap vermesini sağlayan The Malware Working Group.
  + Ağ trafiğini kontrol etmek için kabul edilmiş bir yol geliştirmek için şifreli ulaşım standartlarının üstünde yardımcı olan çalışma grubu The Encrypted Traffic Inspection Working Group (ETI). [160]

#### 6.10.1.1 İlgili Standartlar Faaliyetleri

##### 6.10.1.1.1 Şifreleme

**Onaylı Standartlar**

* IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography
* IEEE Std 1363a-2004 IEEE Standard Specifications for Public-Key Cryptography--Amendment 1: Additional Techniques
* IEEE Std 1363.1-2008 IEEE Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices
* IEEE Std 1363.2-2008 IEEE Standard Specification for Password-Based Public Key Cryptographic Techniques
* IEEE Std 1363.3-2013 IEEE Standard for Identity-Based Cryptographic Techniques using Pairings [160]

##### 6.10.1.1.2 Sabit ve Çıkarılabilir Depolama

**Onaylı Standartlar**

* IEEE Std 1619-2007 IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
* IEEE Std 1619.1-2007 IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices
* IEEE Std 1619.2-2010 IEEE Standard for Wide-Block Encryption for Shared Storage Media
* IEEE Std 1667-2015 IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices [160]

##### 6.10.1.1.3 Yazılım Tanımlı Ağ ve Ağ İşlevleri Sanallaştırması için Güvenlik

**Geliştirilen Projeler**

* + IEEE P1915.1 Draft Standard for Software Defined Networking and Network Function Virtualization Security [160]

##### 6.10.1.1.4 Hardcopy Aygıtları için Güvenlik

**Onaylı Standartlar**

* IEEE Std 2600-2008 IEEE Standard for Information Technology: Hardcopy Device and System Security
* IEEE Std 2600.1-2009 IEEE Standard for a Protection Profile in Operational Environment A
* IEEE Std 2600.2-2009 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008 Operational Environment B
* IEEE Std 2600.3-2009 IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008 Operational Environment C
* IEEE Std 2600.4-2010 IEEE Standard Protection Profile for Hardcopy Devices in
* IEEE Std 2600-2008 Operational Environment D [160]

##### 6.10.1.1.5 Akıllı Şebeke için NIS

**Onaylı Standartlar**

* IEEE Std 1402-2000 (R2008) IEEE Guide for Electric Power Substation Physical and Electronic Security\*
* IEEE Std 1686-2013 IEEE Standard for Intelligent Electronic Devices (IED) Cyber Security Capabilities
* IEEE Std C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems

**Geliştirilen Projeler**

* IEEE P1711 Draft Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links [160]

# BÖLÜM 7: SONUÇ

Günümüzde bilişim alanındaki en büyük sorunlardan biri ağ güvenliğidir. Büyük şirketler kurmuş oldukları ağ sistemlerinin saldırılara karşı korunması için yaşamsal bir savaş vermektedirler. Bundan dolayı çok büyük yatırımlar yapmakta ve büyük paralar harcanmaktadır. Ticari anlamda firmalar büyük zarar görmektedirler. Diğer taraftan bu tür sistemleri üreten ve yazılım geliştiren firmalar büyük bir para kazanmaktadırlar. Saldırı çeşitleri arttığı sürece her gün yeni bir ağ güvenliği programı ve sistemi ortaya çıkmaktadır. Tabii olarak bu gelişme yüzünden büyük bir pazar oluşmaktadır.

Burada sadece büyük firmalar değil kişisel bazdaki kullanıcılarda bilgi saklama ve korunması için çeşitli programlar ve sistemler almaktadır. Dünya çapında büyük bir pazar haline gelen bu güvenlik sistemleri dünya ülkelerinde olduğu gibi ülkemiz ekonomisine büyük zararlar vermektedir.

Yapılan araştırmalar dünya genelinde şirkete yapılan atakların %70 ila % 90 arasında şirket çalışanları tarafından yapıldığını ortaya koymaktadır. Bu bilgi hırsızlığından tutun bilerek ya da bilmeyerek sistemlere verilen zararları kapsamaktadır. Genelde işinden kötü şekilde ayrılan şirket çalışanları sistemlere ait bilgilerini başkalarına verebilmekte ya da özellikle sistemleri sabote edebilmektedirler. Kendi bilgisayarlarına kurdukları “sniffer”(paket dinleyici)’lar sayesinde başka kişilerin maillerini ya da gizli bilgilerini elde edebilmektedirler. Ya da her türlü önleminizi dışarıdan gelebilecek saldırılara karşı almışken içeriden birisi kolaylıkla önemli sistemlere erişebilir kritik bilgileri silip değiştirebilir ya da rakip bir firmaya verebilir. Ya da meraklı bir kullanıcı yeni öğrendiği hacker araçlarını sizin firmanız üzerinden başka firmalara girmek için kullanabilirler.

Güvenlik için yapılan her yatırıma karşı bu saldırılar sürmektedir. Hatta Amerika’da dünyanın en iyi korunan, girilmesi imkânsız olan Savunma Bakanlığı bilgisayarlarına girilmiş ve bilgilere ulaşılmıştır. Amerika’da bu tür saldırılara ağır cezalar uygulanırken Türkiye’de bir yasal boşluktan dolayı yakalananlar elini kolunu sallayarak hapisten çıkmaktadır. Bundan dolayı ülkemizde en kısa sürede bu yasal boşluğun kapatılması gerekmektedir. Sonuç olarak ağ güvenliği, teknolojinin günümüz boyutlarında olduğu düşünüldüğünde artık hayati bir önem taşımaktadır ve burada bahsedilen güvenlik kavram ve önlemleri teknolojinin bu denli hızla gelişmekte olduğu bir ortamda ne yazık ki yetersiz kalmaktadır. Bu çalışmada görülen vizyon, aslında hiçbir sistemin, hiçbir zaman yüzde yüz güvenli olamayacağıdır. Saldırılar, türleri ve algoritmaları bugün teknolojik anlamda diğer tüm sistemlerden daha hızlı gelişmektedir. Bu çalışmayı, bundan sonra referans alacak olan kurum ve ya kişiler, bugünün teknolojisinden sonra ortaya çıkacak yeni teknolojilere dair güvenlik kavramları üzerinde çalışarak bu kaynağı ilerletebilir, geleceğe uyumlu hale getirebilirler.

**KAYNAKLAR**

[1]Dr. ÇÖLKESEN Rifat, Prof.Dr. Bülent ÖRENCİK, Bilgisayar Haberleşmesi ve Ağ Teknolojileri, İstanbul, [Mayıs 2008].

[2]Dr. ÇÖLKESEN Rifat, Yasin KAPLAN, Yüksek Hızlı Kablosuz Hücresel Ağ

Erişimi.[2012]

[3]ÖZTÜRK Emin, WLAN Kablosuz Yerel Alan Ağları Teknolojisinin İncelenmesi, Mevcut Düzenlemelerin Değerlendirilmesi ve Ülkemize Yönelik Düzenleme Önerisi, Uzmanlık Tezi, Ankara, 2004.

[4]A-Z’ ye Kablosuz Ağ Hakkında Herşey, Chip Dergisi Eki, Kasım 2009

[5]Schenk, Rob. Garcia, Andrew. Iwanchuk, Russ. “Wireless LAN Deployment and Security Basics.” ExtremeTech.com. URL: http://www.extremetech.com/article2/0,3973,1073,00.asp (7 Nov. 2003)

[6]http://www.radio-electronics.com/info/antennas/mimo/multiple-input-multiple-output-technology-tutorial.php[Site Güncelleme: Undefined, Ziyaret Tarihi:24.11.2016]

[7]<http://www.jhuapl.edu/techdigest/TD/td3002/Hampton.pdf> [Site Güncelleme: Undefined, Ziyaret Tarihi:24.11.2016]

[8]TÜBİTAK-BİLTEN, Elektromanyetik Dalgalar ve İnsan Sağlığı - Sıkça Sorulan Sorular ve Yanıtları, Ankara, 2001.

[9]KOÇAK Yılmaz, M.Akif SABAH, Necmi TAŞPINAR, Genel Paket Radyo Servisi (Gprs)Yapısı, Protokolleri ve Kaynak Yönetimi, Erciyes Üniversitesi Fen Bilimleri Ensitüsü Dergisi, Kayseri, 2002.

[10] [Next Generation Wireless LANs: 802.11n and 802.11ac](http://amzn.to/2bh3gRR)by Eldad Perahia, Robert Stacey (2013)

[11][Wireless Networks](http://amzn.to/1NXcBQK) by Clint Smith and Daniel Collins (2014)

[12][802.11 Wireless Networks: The Definitive Guide, Second Edition](http://amzn.to/1NXcKDx) by Matthew S. Gast (2005)

[13] [Designing and Deploying 802.11ac Wireless Networks](http://amzn.to/1Nkavu6) by Jim Geier (2010)

[14][Wireless Networking Absolute Beginner’s Guide](http://amzn.to/1VKuF2U) **by Michael Miller** (2013)

[15][CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106](http://amzn.to/1T2dV6Z) by David D. Coleman and David A. Westcott (2014)

[16][Wireless Network Security A Beginner’s Guide](http://amzn.to/1VKvcCc) by Tyler Wrightson (2012)

[17][Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications (2nd Edition)](http://amzn.to/1NkaW7C) by Jim Geier (2015)

[18][Network Warrior](http://amzn.to/1T2e2PZ) by Gary A. Donahue Sayfa:323-391 June 2007

[19][Energy and Spectrum Efficient Wireless Network Design](http://amzn.to/1OeGt5L) by Guowang Miao and Guocong Song (2014) Sayfa: 14-258

[20]CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide by [Darril Gibson](https://www.amazon.com/Darril-Gibson/e/B001IOH64U/ref=dp_byline_cont_book_1)  (2014) Sayfa:29-155

[21]“Data Communications Technology.” Understanding Networking Technologies. Course Manual.Chapter5.AtriumTechnical,Inc.URL: http://www.netguru.net/courses/ntc/NTCC5.htm (7 Nov. 2003)

[22]“Wireless Technologies.” Internetworking Technologies Handbook. Chapter 20. Cisco Systems, Inc. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\_doc/wireless.pdf (7 Nov. 2003) “Wireless Tech

[23] Understanding TCP/IP, chapter-10, by Libor Dostálek, Alena Kabelová Publisher: Packt Publishing [May 2006]

[24]“802.11a Technology Overview.” Stanford University Communication and Networking Services. URL: http://www.stanford.edu/group/networking/NetConsult/wireless/80211a.html (7 Nov. 2003)

[25]https://pdfs.semanticscholar.org/aeaa/7a8b4ef97bbf2b0ea2ad2ee88b13fcb2b797.pdf[Site Güncelleme: Undefined, Ziyaret Tarihi:29.11.2016]

[26]http://searchnetworking.techtarget.com/info/problemsolve/LANs-Local-Area-Networks[Site Güncelleme: Undefined, Ziyaret Tarihi:29.11.2016]

[27]Wireless LAN Systems (Artech House Telecommunications Library) by [Asuncion Santamarie](https://www.amazon.com/s/ref=dp_byline_sr_book_1?ie=UTF8&text=Asuncion+Santamarie&search-alias=books&field-author=Asuncion+Santamarie&sort=relevancerank) (Editor), [F. J. Lopez-Hernandez](https://www.amazon.com/s/ref=dp_byline_sr_book_2?ie=UTF8&text=F.+J.+Lopez-Hernandez&search-alias=books&field-author=F.+J.+Lopez-Hernandez&sort=relevancerank) (Editor)( 1 Dec 1994 by Artech House)

[28]“Principles of 802.1x Security.” ORiNOCO Technical Bulletin 048/B. Agere Systems Inc. April 2002.

[29]“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.” ANSI/IEEE Std. 802.11. 1999 Edition.

[30]http://support.usr.com/download/whitepapers/wireless-wp.pdf[SonGüncelleme Tarihi:Undefined, Ziyaret Tarihi:09/12/2016]

[31]Cable Networks, Services, and Management by Mehmet Toy(IEEE Press Series on Networks and Services Management) 1st Edition[2015]

[32]Cable and Wireless Networks: Theory and Practice by Mário Marques da Silva(January 19, 2016 by CRC Press ) Sayfa:495-564,

[33]Telecommunication Networks by Eugenio Iannone(December 14, 2011 by CRC Press ) Sayfa:219-323

[34]The Future of Wireless Networks: Architectures, Protocols, and Services by Mohesen Guizani, Hsiao-Hwa Chen, Chonggang Wang(September 22, 2015 by CRC Press ) Sayfa:23-137, 175-300, 361-430

[35]Wireless Quality of Service: Techniques, Standards, and Applications by Maode Ma, Mieso, K. Denko(September 9, 2008 by Auerbach Publications ) Sayfa:3-38

[36]The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition by [Dafydd Stuttard](https://www.amazon.com/Dafydd-Stuttard/e/B001JS8ORI/ref=dp_byline_cont_book_1)  , [Marcus Pinto](https://www.amazon.com/s/ref=dp_byline_sr_book_2?ie=UTF8&text=Marcus+Pinto&search-alias=books&field-author=Marcus+Pinto&sort=relevancerank) Sayfa:1-117,159-571,701-853[2011]

[37]DİRİCAN Okan Can, TCP/IP ve Ağ Güvenliği, Açık Akademi Yayınları, İstanbul, 2005.

[38]ÖZBİLEN Alper, Bilgisayar Ağları ve Güvenliği, Pusula Yayıncılık, Ankara, 2005.

[39]ŞEN Ömer Faruk, Özgür ÖZDEMİRCİLİ, Ağ Güvenliği İpuçları, Açık Akademi Yayınları, İstanbul, 2006.

[40]UÇAN N. Osman, OSMAN Onur, Bilgisayar Ağları ve Ağ Güvenliği, Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti, Ankara, 2007.

[41]Bilgi Güvenliği Farkındalık Eğitim Örneği, E.Şahinaslan, A.Kantürk, Ö.Şahinaslan, E.Borandağ, Ab2009 Akademik Bilişim Konferansı, , Şubat 2009

[42]Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, E.Şahinaslan, R.Kandemir, Ö.Şahinaslan, Ab2009 Akademik Bilişim Konferansı, Şubat 2009

[43]TBD Kamu BİB VIII, Bilişim Teknolojilerinde Risk Yönetimi – II. Çalışma Grubu, S.4.[2011]

[44]ÇÖLKESEN, R.[OCAK 2012], *Network TCP/IP unix el kitabı,* Papatya Yayınları, İstanbul, 975–6797–02–9.

[45]<http://www.bmtrada.com.tr/27001BrosurA4.pdf> [Ziyaret Tarihi:12 ARALIK]

[46]<https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html> 12.13.2016

[47]Karaarslan Enis, Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar, Akademik Bilişim 2003

[48] Karaarslan Enis, “Network Cihazlarının ve Sistemlerinin Güvenliği”, inet-tr 2002 Konferansı

[49]PUSULA NET KURUMSAL HİZMETLER, *Yerel alan a*ğ *hizmetleri*, <http://www.pusula.net.tr/yerelag.htm> [Son Güncelleme Tarihi:Undefined, Ziyaret Tarihi:15.12.2016]

[50]KAPLAN Y. , 2000, *Veri haberle*ş*mesi temelleri*, Papatya Yayınları, İstanbul, 975– 6797–15–0.

[51]KARACI, A., İnternetle ilgili bazı temel kavramlar, Gazi Üniversitesi, http://w3.gazi.edu.tr/web/akaraci/ders/internet.htm [Ziyaret Tarihi: Şubat 2007].

[52]<http://searchnetworking.techtarget.com/definition/OSI> [Son Güncelleme Tarihi: Undefined, Ziyaret Tarihi:14.12.2016]

[53]<http://www.clib.dauniv.ac.in/E-Lecture/Osi.pdf> [Son Güncelleme Tarihi: Undefined, Ziyaret Tarihi:14.12.2016]

[54]<http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf> [Son Güncelleme Tarihi: Undefined, Ziyaret Tarihi:14.12.2016]

[55]ODOM, W. , 2003, Cisco CCNA 640–647 sınavı sertifikasyon rehberi, Sistem Yayıncılık, İstanbul, 975–322–301–3.

[56] 802.11 Wireless Networks: The Definitive Guide, 2nd Edition by Matthew Gast Publisher: O'Reilly Media, Inc. April 2005

[57]<https://www.safaribooksonline.com/library/view/ethernet-the-definitive/1565926609/ch01.html> [Son Güncelleme Tarihi: Undefined, Ziyaret Tarihi:14.12.2016]

[58]https://www.ccontrols.com/pdf/ExtV1N3.pdf[Son Güncelleme Tarihi: Undefined, Ziyaret Tarihi:14.12.2016]

[59] Ethernet: The Definitive Guide: Designing and Managing Local Area Networks 2nd Edition by Charles E. Spurgeon (Author), Joann Zimmerman (Author)[2014]

[60] Ethernet Switches by Joann Zimmerman, Charles E. Spurgeon Publisher: O'Reilly Media, Inc. Release Date: April 2013

[61]TECHFEST, Ethernet technical summary - Chapter 2 (31 Eki 2007 )

URL:<http://scp.s-scptuj.mb.edus.si/~murkos/Teorija%20in%20vaje/ROM/Racunalniske%20mreze/Kontrolna%20naloga/Literatura%20za%20KN/Ethernet%20FRAME/ethernet%20FRAME.htm>

[62]Computer Networks 5th By Andrew S. Tanenbaum (International Economy Edition) (January 9, 2010)

[63]TCP/IP Tutorial and Technical Overview by Lydia Parzial, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews, Nicolas Rosselot (December 2006)

[64]<https://www.netlab.tkk.fi/opetus/s38130/s98/tcpapp/TCP_appl.pdf> [Son Güncelleme Tarihi: Undefined, Ziyaret Tarihi:15.12.2016]

[65] Exploring Transmission Control Protocol (TCP) (Exploring RFC Series Book 1) Kindle Edition by Phil Smith (Author)[2014]

[66]Harris, S. (2013). Physical and Environmental Security. In CISSP Exam Guide (6th ed., pp. 427-502). USA McGraw-Hill;

[67] THE TCP/IP GUIDE A Comprehensive, Illustrated Internet Protocols Reference by Charles M. Kozierok

[68]INDEX of VERİ İLETİŞİM MODELLERİ, 2005, *ICMP*, Hacettepe Üniversitesi, <http://yunus.hacettepe.edu.tr/~b0045188/veri_iletisim_modelleri/>

[69]AYAV, T. , YILMAZ, S. , 2003, Bir ağ yönetim sistemi: Guardilan, *TBD 20th Bilisim Kurultayi Bildiriler Kitabi*, Eylül 2003, İstanbul, 1–1.

[70]ÇAY, K. , 2006, *TCP / IP* protokolgrubutarihçesi*,* <http://www.turkcenet.org/danlar-mainmenu-55/i-makaleler-mainmenu-56/256-tcp--ip-protokol-grubu-tarihi-.html(10.09.2006)>

[71]Computer Network Security 2005th Edition by [Joseph Migga Kizza](https://www.amazon.com/Joseph-Migga-Kizza/e/B001H6IYEU/ref=dp_byline_cont_book_1) (2005)

[72]Network Security: A Beginner's Guide, Second Edition (Beginner's Guide) 2nd Edition

by [Eric Maiwald](https://www.amazon.com/Eric-Maiwald/e/B001IU0LAU/ref=dp_byline_cont_book_1)(2003)

[73]Bejtlich R., The Tao of Network Security Monitoring: Beyond Intrusion Detection, Lesson Notes, (Addison-Wesley, 2005;

[74] Information Security and Ethics: Concepts, Methodologies, Tools and Applications (Contemporary Research in Information Science and Technology) 1st Edition by Hamid Nemati (Author, Editor

[75]Özgit, A., ʺBilişim Güvenliğinden Ne Anlıyoruz?ʺ, TBD BIMY-10 Bildiriler Kitabi, Nisan 2003.

[76]BGA, "Günümüz Internet Dünyası nda IP Spoofi ng", <http:/ /blog.bga. com.tr / network-securit y/ gunumuz-internet -dunyasinda-ip-spoofi ng>, 03.05.2012

[77]DOS/DDOS Saldırıları,Savunma Yolları ve Çöüzm Önerileri, Huzeyfe Önal,Bilgi Güvenliği Akademisi,2012

[78]White Paper: Type of Attacks, Author: Mr. Mayank Lau, Consultant Security-Practices,<https://www.dsci.in/sites/default/files/Type%20of%20Attacks_DSCI_White%20Paper_1.pdf> [Ziyaret Tarihi:23.12.2016]

[79]Today’s Impact on Communication System by IP Spoofing: Some great methods for detecting and preventing IP Spoofing Paperback – January 18, 2012by [Sharmin Rashid Linta](https://www.amazon.com/s/ref=dp_byline_sr_book_1?ie=UTF8&text=Sharmin+Rashid+Linta&search-alias=books&field-author=Sharmin+Rashid+Linta&sort=relevancerank) (Author), [Md. Ridgewan Khan Neuton](https://www.amazon.com/s/ref=dp_byline_sr_book_2?ie=UTF8&text=Md.Ridgewan+Khan+Neuton&search-alias=books&field-author=Md.Ridgewan+Khan+Neuton&sort=relevancerank) (Author)

[80] James Graham and Richard Howard, et all, Cyber Security Essentials, Boca Raton, Auerbach Publications, 2010, pp. 198, 199

[81]Richard Kissel (Ed.), Glossary of Key Information Security Terms, National Institute of Standards and Technology, 2011, <http://csrc.nist.gov/publications/nistir/ir7298rev1/nistir-7298-revision1.pdf>, 08.03.2012, p. 196

[82][http://80.251.40.59/science.ankara.edu.tr/ozbek/kripto1.htm(Ziyaret](http://80.251.40.59/science.ankara.edu.tr/ozbek/kripto1.htm%20(Ziyaret)Tarihi:23.12.2016,Güncelleme:Undefined)

[83]<http://dokumanistan.blogspot.com.tr/2012/07/internet-protocol-security.html(Ziyaret> Tarihi: 23.12.2016,Güncelleme:Undefined)

[84]Khaleel Ahmad, Jayant Shektar, K.P. Yadav, “Classification of SQL Injection Attacks”, VSRD-TNTJ, Vol. I(4), 2010, 235-242

[85]<http://www.cse.usf.edu/~ligatti/papers/code-inj.pdf> (Ziyaret Tarihi:24.12.2016)

[86]http://admin.utep.edu/Default.aspx?tabid=54090(Ziyaret Tarihi:24.12.2016, Güncelleme:Undefined)

[87]http://www.cyber-warrior.org/Dokuman/Default.Asp?Data\_id=4670(Ziyaret Tarihi:24.12.2016, Güncelleme:Undefined)

[88]https://telekom.com.tr/index.php/blog/arka-kapilar-backdoors(Ziyaret Tarihi:24.12.2016, Güncelleme:Undefined)

[89]https://www.olympos.net/belgeler/turkiyede-phishing-126266.html(Ziyaret Tarihi:24.12.2016, Güncelleme:Undefined)

[90]SRIVASTAVA Tushar. “Phishing and Pharming – The Deadly Duo”. 2007. SANS Institute.

[91]https://www.cs.ucsb.edu/~chris/research/doc/cj06\_phish.pdf(Ziyaret Tarihi:24.12.2016)

[92]http://www.langturk.com/rootkit-nedir/(ZiyaretTarihi:24.12.2016, Güncelleme:Undefined)

[93]IT Governance: An International Guide to Data Security and ISO27001/ISO27002 Yazar: Alan Calder,Steve Watkins(03.09.2015)

[94]SearchSecurity İnternet Sitesi, Botnet (Zombie Army), <http://searchsecurity.techtarget.com/definition/botnet>, 17.04.2012.

[95]Information Security: The Complete Reference, Second Edition 2nd Edition by Mark Rhodes-Ousley (Author)(01.01.2013)

[96]https://notlaricin.files.wordpress.com/2016/03/5-bilgi-gc3bcvenlic49fi.pdf(Ziyaret Tarihi:24.12.2016)

[97][http://whatis.techtarget.com/definition/S-MIME-Secure-Multi-Purpose-Internet-Mail-Extensions (Site](http://whatis.techtarget.com/definition/S-MIME-Secure-Multi-Purpose-Internet-Mail-Extensions%20(Site) Güncelleme Tarihi: Ekim 2008,Ziyaret Tarihi: 24.12.2016 )

[98] PGP & GPG: Email for the Practical Paranoid Paperback – (April 1, 2006) by Michael W Lucas (Author)

[99]<http://searchsoftwarequality.techtarget.com/definition/S-HTTP> (Güncelleme:[January 2006](http://searchsoftwarequality.techtarget.com/archive/2006/1))

[100][http://searchsoftwarequality.techtarget.com/definition/HTTPS (Güncelleme:August](http://searchsoftwarequality.techtarget.com/definition/HTTPS%20(August) [2008](http://searchsoftwarequality.techtarget.com/archive/2006/1))

[101]http://searchfinancialsecurity.techtarget.com/definition/Secure-Electronic-Transaction(Güncelleme:[January 2008](http://searchfinancialsecurity.techtarget.com/archive/2008/1))

[102]http://searchsecurity.techtarget.com/definition/Kerberos(Güncelleme:[August](http://searchfinancialsecurity.techtarget.com/archive/2008/1) 2016)

[103][http://searchsecurity.techtarget.com/definition/SSL-VPN (Güncelleme:January](http://searchsecurity.techtarget.com/definition/SSL-VPN%20(January) 2009)

[104]http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS(Güncelleme:May 2016)

[105]https://technet.microsoft.com/en-us/library/cc959507.aspx(24.12.2016)

[106]<http://searchmidmarketsecurity.techtarget.com/definition/IPsec(Güncelleme:November> 2010)

[107][https://technet.microsoft.com/en-us/library/cc959510.aspx (Güncelleme:24.12.2016)](https://technet.microsoft.com/en-us/library/cc959510.aspx%20(Güncelleme:24.12.2016))

[108]<http://searchenterprisewan.techtarget.com/definition/virtual-private-network(Güncelleme:July> 2016)

[109][http://searchnetworking.techtarget.com/definition/PPP (Güncelleme:September](http://searchnetworking.techtarget.com/definition/PPP%20(Güncelleme:September) 2016)

[110]<http://searchsecurity.techtarget.com/definition/RADIUS(Güncelleme:June> 2007)

[111]http://searchsecurity.techtarget.com/definition/TACACS[(Güncelleme:June](http://searchsecurity.techtarget.com/definition/RADIUS(Güncelleme:June) 2007)

[112]<http://searchsecurity.techtarget.com/definition/CHAP-Challenge-Handshake-Authentication-Protocol(Güncelleme>: June 2005)

[113]<http://searchsecurity.techtarget.com/definition/Extensible-Authentication-Protocol-EAP(Güncelleme:September> 2005)

[114]<https://www.techopedia.com/definition/4043/password-authentication-protocol-pap> (Güncelleme:24.12.2016)

[115]<http://www.certiology.com/tech-terms/network/shiva-password-authentication-protocol-spap.html> (Güncelleme: 24.12.2016 )

[116]<http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard(Güncelleme>: [November 2014](http://searchsecurity.techtarget.com/archive/2014/11))

[117]<http://www.webopedia.com/TERM/S/S_key.html(Güncelleme>: 24.12.2016)

[118]<https://technet.microsoft.com/en-us/library/cc957985.aspx> (Güncelleme: 25.12.2016)

[119]Krishna Shankar, et al, "Cisco Wireless LAN Security," Cisco Press, 2005, 420 pp, ISBN:1587051540

[120]J. Edney and W.A. Arbaugh, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i,” AddisonWesley, 2004, 481 pp., ISBN:0321156209

[121]<https://www.juniper.net/techpubs/en_US/release-independent/wireless/information-products/topic-collections/wireless-lan/software/9.0/mss_config_90.pdf> (Basım:2013)

[122]KABLOSUZ YEREL ALAN AĞI GÜVENLİĞİ KILAVUZU, Battal Özdemir, (3 mart 2008)

[123]<http://www.iso.org/> (Tarihi:25.12.2016)

[124]<https://share.ansi.org/shared%20documents/News%20and%20Publications/Brochures/WhatIsANSI_brochure.pdf> (Ziyaret: 25.12.2016)

[125]<http://searchsoftwarequality.techtarget.com/definition/NIST> (January 2006)

[126]<https://www.nist.gov/director/pao/nist-general-information> (Ziyaret: 25.12.2016)

[127]<http://csrc.nist.gov/publications/PubsSPs.html> (Ziyaret: 25.12.2016)

[128]Ben-Tovim, Erez (February 2014). "12". In Berger, Lars T. ; Schwager, Andreas; Pagani, Pascal; Schneider, Daniel M. [*{ITU} {G.hn} - {B}roadband Home Networking*](http://www.crcpress.com/product/isbn/9781466557529). Devices, Circuits, and Systems. CRC Press. [doi](https://en.wikipedia.org/wiki/Digital_object_identifier):[10.1201/b16540-14](https://dx.doi.org/10.1201%2Fb16540-14). [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [9781466557529](https://en.wikipedia.org/wiki/Special:BookSources/9781466557529).

[129]X.805: Security architecture for systems providing end-to-end communications <http://www.itu.int/rec/T-REC-X.805-200310-I/en> (Ziyaret : 25.12.2016)

[130]["Internet Engineering Task Force (IETF)"](https://www.ripe.net/internet-coordination/internet-governance/internet-technical-community/ietf). RIPE NCC. 10 August 2012. Retrieved 13 October 2012.

[131]<https://www.iab.org/about/> (Güncelleme: 23.05.2016)

[132]https://www.iab.org/(Güncelleme: 23.05.2016)

[132]<https://www.iab.org/> (Güncelleme: 25.12.2016)

[133]https://www.ietf.org/iesg/ (Güncelleme: 17.11.2016)

[134]<https://irtf.org/> (Ziyaret Tarih: 25.12.2016)

[135]["RFC's, Internet Request For Comments"](http://www.livinginternet.com/i/ia_rfc.htm). http://www.livinginternet.com/i/ia\_rfc.htm. Retrieved 2012-04-03

[136]http://www.etsi.org/standards/different-types-of-etsi-standards.ETSI.(Güncelleme:1 February 2014)

[137]<http://www.etsi.org/about/who-we-are> (Ziyaret: 25.12.2016)

[138]<http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpadvancedtrustedenvironmentomtptr1v11.pdf> (Ziyaret: 25.12.2016)

[139]<http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpsecuritythreatsonembeddedconsumerdevicesv11.pdf>(Ziyaret:25.12.2016)

[140]<http://telecoms.com/9012/crime-fighters-welcome-mobile-security-requirements/>(Ziyaret:25.12.2016)

[141]<http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpuiccusimv20.pdf> (Ziyaret: 25.12.2016)

[142]<http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtplocaldataconnectivityv10.pdf> (Ziyaret: 25.12.2016)

[143]http://www.theregister.co.uk/2015/08/25/mats\_granryd\_is\_the\_new\_gsma\_director\_general/ ,The Register,Retrieved 25 August 2015.

[144]<http://www.zdnet.com/article/happy-20th-birthday-gsm/> ,ZDNet,Retrieved

(7 September 2007)

[145]<http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups> (Ziyaret: 25.12.2016)

[146]<http://www.gsma.com/aboutus/annualreport> (Ziyaret: 25.12.2016)

[147]<http://www.un.org/sustainabledevelopment/blog/2016/09/new-mobile-app-launches-to-drive-action-on-sustainable-development-goals/> ,United Nations, Retrieved 18 September 2016.

[148]Rick Merritt (April 8, 2003). ["New group aims to secure PCs, PDAs, cell phones"](http://www.eetimes.com/document.asp?doc_id=1202119). Retrieved 2014-11-17. <http://www.eetimes.com/document.asp?doc_id=1202119>

[149]<https://www.trustedcomputinggroup.org/members/wave_systems_corp>(ZiyaretTarihi:26.12.2016)

[150]<https://www.trustedcomputinggroup.org/dmi/> (Ziyaret Tarihi: 26.12.2016)

[151]<https://www.trustedcomputinggroup.org/faq/TPMFAQ/> (Ziyaret Tarihi: 26.12.2016)

[152]<http://www.theverge.com/microsoft/2012/2/1/2763980/windows-8-arm-desktop-app-restriction-certificates> (Ziyaret Tarihi: 26.12.2016)

[153]http://www.softwarefreedom.org/blog/2012/jan/12/microsoft-confirms-UEFI-fears-locks-down-ARM/ (Ziyaret Tarihi: 26.12.2016)

[154]Huanguo, Z, Yi, M. "Trusted computing and information security", **Communications**, 9-10, (2013) .

[155]Cabiddu, G. Cesena, E, Sassu, R., Vernizzi, D., Ramunno, G., Lioy, A., "The Trusted Platform Agent", **IEEE Software**, XXVIII: 35-41, (2011).

[156]Fournaris, A. P, "Toward Flexible Security and Trust Hardware Structures for Mobile-Portable Systems", **IEEE Latin America Transactions**, 1719-1722, (2012).

[157]Metke, A. R, Ekl, R. L., “Security Technology for Smart Grid Networks”, **IEEE Transactions on Smart Grid**, 99-107, (2010).

[158]Mooseop, K. Hongil, J., Youngsae, K., Jiman, P., Youngsoo, P., “Design and implementation of mobile trusted module for trusted mobile computing”, **IEEE Transactions on Consumer Electronics**, 134-140, (2010).

[159]<http://www.ieee.org/membership_services/membership/statistics/annual_report_of_the_secretary.html(Ziyaret> Tarih:23.12.2016)

[160]<http://standards.ieee.org/develop/msp/nis.pdf> (Güncelleme: 23.09.2016)

[161]<http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/veri-ba%C4%9Flant%C4%B1-(data-link)-katman%C4%B1> (Güncelleme: 7 Eylül 2013)