****

**T.C.**

**ATATÜRK ÜNİVERSİTESİ**

**Mühendislik Fakültesi**

**Bilgisayar Mühendisliği**

**DERSİN ADI**

**BMS.302.Bilgisayar-Bilgi Güvenliği ve Yönetimi**

**ÖDEV KONUSU**

**Mail Güvenliği**

**Öğrencinin Adı**

**Fikret Öztürk**

**160757005**

**Dersin Öğretim Görevlisi**

**Prof. Dr. Abdulsamet HAŞILOĞLU**

**İÇİNDEKİLER**

1. Mail Nedir.
2. E-Posta Trafiği
3. Posta Hizmetleri Çeşitleri
4. Mail Gönderme (Send Mail)
5. Posta Tanımı
6. Mail Ağ Mimarisi:
7. Kötü E-Posta Senaryosu:
8. Protokoller
9. Çok Amaçlı İnternet Posta Uzantıları(MIME):
10. İnternet İleti Erişim Protokolü(IMAP):
11. Pop(Post Office Protokol):
12. SMTP:
13. DNS (Domain Name Sistem) Alan Adı Sistemi:
14. İnternet Metin Mesajlarının Arpa Standardında Formatı:
15. Güvenli Posta Gönderimi:
16. Kaynakça

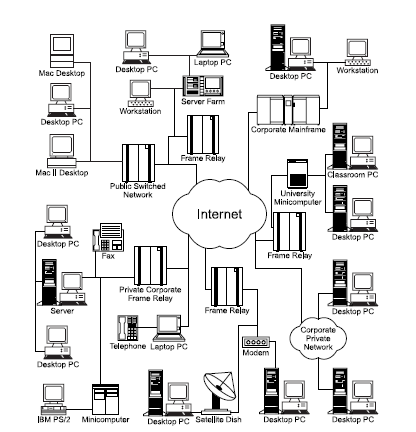
1.Mail Nedir.

Telgraf mesajı bittiğinde Elektronik haberleşme başladı Yaklaşık 50 yıl önce bir Ana bilgisayarda çalışan insanlar birinin doğrudan erişim depolama aygıtı sürücüsündeki dizinine mesaj bırakmış veya dosya yerleştirmişlerdi .Bununla Birlikte ilk elektronik mesajlaşma sistemi başlamış oldu. Bir çok insan elektronik mail veya e-mail adlandırılmasını arpa net ile başlattı Elektronik İletişimde bilgi güvenliği çalışanlar ,ticari şirketler hükümetler ve bireysel kullanıcılar için her zaman proplem olmuştur. Bilgisayar Sistemleri birbiriyle Konuşmaya başladığında ,Bilgisayar kullanıcıları arasında iletişimde gelişme çok hızlı bir şekilde arttı.

İnternet başlangıçta askeri ve üniversite kullanımı için artmıştır. Buda Güvenli tasarım ve elektronik postanın büyümesi için doğal bir alan oluşturmuştur. Bugün e-posta ,elektronik sohbet ve veri aktarımı çok hızlı bir şekilde gerçekleşmektedir. Çoklu protokol iletişimi ağları birbirine bağlama ve işletmelerin başarılı olması için zorunludur. Elektronik postanın bir noktadan diğerine gitmek için birden fazla platformdan ve bir çok ağ üzerinden geçmesi gerekir. Ağlar arası ve bağlantılardan her geçişte ele geçirilebilir değiştirilebilir kopyalanabilir veya tamamen durdurulabilir.

İnternet Bağlantısı

Şekil-1



İnternetteki sohbet odaları internet üzerinde modifiye edilmiş e – posta siteleridir. Aynı anda e-postayı birden çok taraf okuyabilir. Bu sohbet odaları kullanıcının bir mesaj göndermesini sağlar; Bu mesajı aynı anda birkaç kişi aynı anda görebilir. Bu tarz iletişim bir risktir. Günümüzde e –postayı dünyadaki her hükümet ve kurum güvenilir bir kurumsal iletişim olarak kullanmaktadır. Dahili ağlar ile bazen çok az da olsa açık metinler taşınır fakat kimlik doğrulaması yoktur. Bu kritik iş mesajları arasında iç iletişim için kullanılan halka açık telefon hatları üzerinden taşınabilir .Bu trafik çoğu durumda orijinallik ve veri olarak sorgulanamaz ve dinlenilebilir . Mesajın orijinal yazardan geldiği bilinse de onaylayan sertifika ve imza yok. Bir çok durumda Günümüz standartlarına göre e-posta yasal olarak kabul edilen fiili güvenilir bir iletişim türü haline gelmek için yasal ve bağlayıcı olması durumunda üçüncü taraf orijinallik sertifikası içermesi gerekiyor(Bir çeşit noter tasdikli olması) Mesajdaki kimliğin nasıl değiştirileceğini hızlı bir şekilde anlayan kişi finansal bilgileri alır .Bu durum ise daha çok meseleleri karıştırır. ABD ‘de bu durum da çok dava olmuştur.

Elektronik ortamda nerede olduğunu kanıtlamak için görev sistemi yöneticilerine dava açılmış

Bilgi nereden geldi ve gitti. Aslında kim yolladı sorular sorulmuştur. Ne zaman yollandı ve nasıl kanıtlanabilir, imkansız hale geldi tüm ağları kapsayan denetim araçları bulunmadığında Uzun vadeli rapor veya denetim verilerinin saklanması. çözüm olarak sunulmuştur.

2.E-Posta Trafiği:

E posta Trafiği sesli ve görüntülü iletişim hatlarını paylaşıyor. Fiber optik kablolar iletişimde en cok kullanılan kablolardır. Bakır kablolar da problemler olabilir. Sistem yöneticileri kapasite sorunlarını ve arızalarını izlemelidir. Ne kadar trafik akışı olacağını ve ne zaman olacağını belirleyebilmeliler. Sistem yöneticisi hakkındaki tüm soruları cevapladıktan sonra kullanıcı sayısı ve her bir kullanıcıya tahsis edilecek disk alanı e –postanın depolanması için bir sistem gereksinimi bir araya getirebilir .Herhangi bir sisteme uygulanan güvenlik miktarı sistemin çalışacağı hızı ve işlevselliği etkileyebilir.

3.POSTA HİZMETLERİ ÇEŞİTLERİ:

İlk mesaj elektrik kullanan tel ile sağlanmıştır. İlk ana bilgisayar posta olarak SNA protokollerine dayanıyor sadece ASCII formattaydı. Bugün IP Tabanlı trafik var Bir çok iletişim sistemi kullanan bir çok ağ türü var.

4.MAİL GÖNDERME:(Send Mail)

Her internet e postasının bir yerlerde gittiği yol boyunca Send mail sunucusu tarafından işlenir. Send mail’in piyasaya sürülen sürümü 1997’de Eric ALLMAN ve GREG OLSON tarafından sendmaiL’İNC olarak geliştirildi. sendmail çoğu internet servis sağlayıcısı tarafından kullanılır ve gönderilir .Her internet e postasının bir yerlerde gittiği yol boyunca Sendmail sunucusu tarafından işlenir. Sendmail’in piyasaya sürülen sürümü 1997’de Eric ALLMAN ve GREG OLSON tarafından SENDMAİL’İNC olarak geliştirildi. SENDMAİL çoğu internet servis sağlayıcısı tarafından kullanılır ve gönderilir. SUN ,HP,IBM ,DEC,SGI,SCO ve diğer tüm büyük UNIX satıcılarının standart çözüm olarak sendmail kullanır. SENDMAİL uygulaması günümüz internet işlemlerinde çok önemlidir. SENDMAİL programı ARPA Net’e bağlıydı .ARPANET ,İNGRES,BERKNET SENDMAİL bağlanmak için ortak bir protokol ile bireysel e-posta programları için oluşturuldu. İlk Sendmail programı Berkeley’in 4.1c sürümüyle gönderildi. Yazılım dağıtımı veya BERKELEY UNIX’in ilk sürümü TCP/IP içeriyordu. SENDMAİL Yazarları tarafından sürekli olarak geliştirilmiştir.

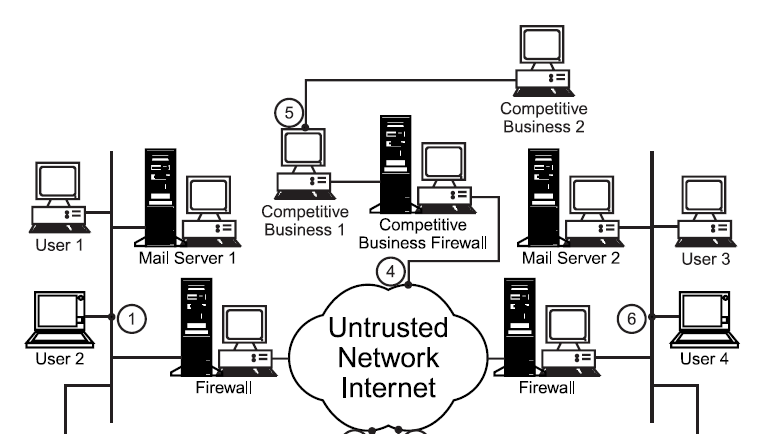
5.POSTA TANIMI:

Elektronik posta (e-posta), Internet üzerinde bilgisayarlar ve insanlar arasında bilgi alışverişini sağlayan ve en yaygın kullanılan Internet uygulamasıdır. Birinin e-posta yoluyla elektronik bir mesaj alması İnternet üzerinde TCP/IP bir parçası olan SMTP transfer protokolü kullanılmaktadır.

SMPT protokolü sayesinde farklı işletim sistemine sahip bilgisayarlar arasında e posta alışverişi gerçekleşmektedir. E-posta istemci/sunucu prensibi ile çalışmaktadır. Mail okumak ve göndermek için kullanıcılar maillerinin geldiği ve gönderildiği bilgisayara, yani sunucuya erişmelidir. istemci uygulaması kullanıcının mail okumasını, maile cevap göndermesini, maili yönlendirmesini, mail yazmasını ve mail göndermesini sağlayan arayüzdür.E –Posta Adresi Nedir-posta adresi (mektuplarda olduğu gibi) mektubun gideceği adrestir. çoğunlukla, kişinin kullanıcı adı ve kullandığı sistemin internet adresinden oluşur. Aşağıda e-posta adres örnekleri verilmiştir. [pinar@atlas.cc.itu.edu.tr](mailto:pinar@atlas.cc.itu.edu.tr) [fikretozturk2525@hotmail.com](mailto:fikretozturk2525@hotmail.com) Yukarıdaki örnek incelenirse e-posta adresi @ işareti ile ayrılmış iki kısımdan oluşmaktadır. Birinci kısım kişinin kendi sistemindeki kullanıcı adını; ikinci kısım ise, bulunduğu sistemin adresini belirtmektedir.

6.MAİL AĞ MİMARİSİ:

Kullanıcı\_1 kullanıcı\_4 bir e-posta göndermek istiyor kullanıcı \_4 ağa bağlıysa tüm mail sistemleri için e-posta kullanıcı\_1 den kullanıcı\_4 gider. Kullanıcı \_4 ağa bağlı değilse e posta daha sonra alma işlemi için kullanıcı\_4 ün posta sunucusunda saklanır. Posta sunucusu doğru çalışmıyorsa mesaj durdurulabilir. e-posta kullanıcı \_1 in posta sunucusundan geçtikten sonra güvenlik duvarı üzerinden yönlendirilir ve kullanıcı \_4 ün güvenlik duvarı üzerinden geçerek kullanıcı \_4 ‘ulaşır .Burada tüm yönlendirme ve protokollerin olduğu varsayılmaktadır



7.KÖTÜ E-POSTA SENARYOSU:

Kullanıcı \_1 kullanıcı \_4 bir mesaj yazar ve gönderir. Uygun Heder başlığı eklenir posta kutusundan posta sunucusuna iletilir. Ardından posta sunucusu Kurumsal güvenlik duvarı aracılığıyla verileri internete iletir. elektrik sinyalleri bilgisayarlardan yönlendirilenden ve router(tekrarlayıcıdan geçer) her bilgisayar adres ve paketi kontrol eder hedefine yönlendirir İnternet trafiğini dinleyen bilgisayar korsanı verileri olduğu gibi kopyalar Bu bilgileri üçüncü tarafla paylaşabilirler. Posta alıcının güvenlik duvarına varır ve posta sunucusuna gönderilir. Alıcı mesajı posta sunucundan silmeden önce yerel makinesine alır ve ve okur. Bu tür olaylarla ilgili bir çok dava olmuştur.

8.PROTOKOLLER:

Tcp/Ip beş katmanlı yapısı e –posta programı e posta belgesini taşıma katmanına gönderir. **taşıma** katmanı kendi başlığını e-postaya ekler ve ağ katmanına gönderir. Ağ katmanı veri çerçevelerini paketlere böler, pakete ek başlık bilgileri ekler ve paketleri veri bağlantı katmanına gönderir. Data-link katmanı, paketleri fiziksel katmana gönderir. fiziksel katman dosyası ağ üzerinden elektrik sinyali olarak seri olarak iletir. elektrik sinyalleri bilgisayarlardan yönlendirilenden ve router(tekrarlayıcıdan geçer) her bilgisayar adres ve paketi kontrol eder hedefine yönlendirir.fiziksel katman paketleri data link katmanına gönderir hedef bilgisayara ulaşmak için data link katmanı bilgileri ağ katmanına gönderir. Ağ katmanı fiziksel bilgileri tekrar bir araya getirir. paket ve header bilgilerini kontrol eder ve paketi taşıma katmanına gönderir. Ulaşım katmanı tüm dosyası bir araya getiri ve uygulama katmanına gönderir uygulama katmanında e-posta programı verileri kullanıcıya iletir.

9.ÇOK AMAÇLI İNTERNET POSTA UZANTILARI(MIME):

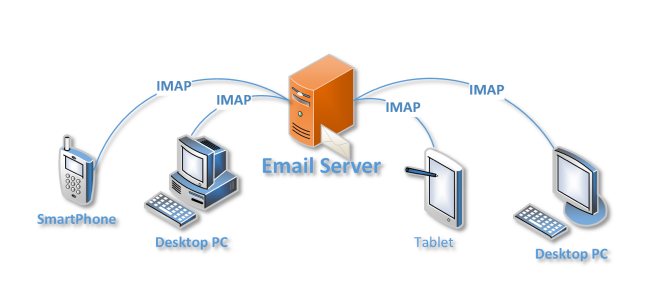
Çok Amaçlı posta uzantıları POP, veya E posta istemcileri Usenet ile birlikte kullanılabilirler. MIME internet posta biçimini genişletmiştir. e-postaların sınırlı yeteneklerini genişletmek amacıyla 1991 yılında Belli Communications tarafından önerilen bir standarttır.   
MIME, ASCII olmayan verilerin SMTP yoluyla gönderilmesine izin veren *bir ekleme veya ek protokoldür* . Kullanıcıların internette farklı türde veri dosyaları alışverişinde bulunmalarına izin verir: ses, video, görüntüler, uygulama programları. SMTP çok basit bir yapıya sahiptir. Yalnızca (SMTP) 7 bit ASCII formatındaki mesajları gönderir. FRANSIZCA ALMANCA RUSÇA ÇİNCE ve JAPONCA

7 bit ASCİİ formatını desteklemeyen diller için MIME kullanılır Video ses verileri gönderilebilir. MIME protokolü ile yollanan bir mesajda çeşitli bölümler bulunmaktadır. Bunlar şöyle sıralanabilir: Başlık bölümü (header) bu bölümde MIME sürümü (versiyon) ve içerik bilgileri yollanır. Mesajın içeriği bölümü. Bu bölüm, ilk kesmeden sonra başlar ve ikinci kesmeye kadar sürer. Basitçe postamızda yazıların bulunduğu ana bölümdür ve postanın içeriğini belirler.

Ekler bölümü. Bu bölüm 2. kesme ile başlar ve 3. kesmeye kadar devam eder. Burada postanın ekleri yer alır. Birden fazla ek varsa bu kesme sayısı arttırılarak her dosya eki için bir yeni alan açılır. Nihayet son kesme ile MIME protokolündeki posta sona erdirilir.

10.İNTERNET İLETİ ERİŞİM PROTOKOLÜ(IMAP):

IMAP Stanford Üniversitesi'nde geliştirilmiştir. IMAP4 olarak de bilinen IMAP, yerel kullanıcıların uzaktaki bir e-posta sunucusuna erişmesini sağlayan bir uygulama katmanı protokolüdür. IMAP mailleri size server üzerinden gösterir. Mailler lokal bilgisayara  indirilemez sadece server üzerinde saklanır. IMAP protokolünde maillerinizi kontrol ettiğinizde bilgisayarınızda hiç birşey saklanmaz, tüm veriler server üzerindedir. IMAP sunucusunda saklanan e-postalar masa üstünden ,evden iş yerinden seyahat ederken erişilebilir.

IMAP protokolünün çalışma şekli 

11.POP(POST OFFİCE PROTOKOL):

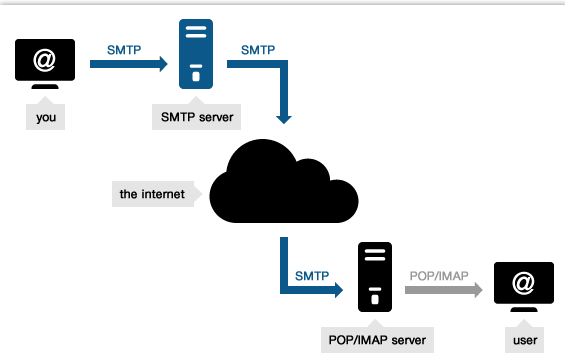
e-posta almak için kullanılır.POP3 (Post Office Protocol versiyon **3**), Outlook, Thunderbird, Windows Mail, [Mac Mail](https://www.hostinger.web.tr/rehberler/mac-mail-kurulumu) gibi yerel e mail istemcilerinin uzak e mail sunucusu ile iletişim kurmasında ve e mailleri indirmesinde kullanılır.POP3 Tek yönlü iletişi(yani veriler sunucudan alınır istemciye gönderilir).

IMAP VE POST ARASINDAKİ FARK:

IMAP VE POP Posta Protokolleri için bir sunucudur. POP Mailleri posta sunucusundan kullanıcı kendi makinesine indirerek okur. IMAP posta sunucusundan indirmeden de mailler okunabilir.

12.SMTP:

Basit Posta Aktarım Protokolü internet yardımıyla 25 numaralı [port](https://wmaraci.com/nedir/port) üzerinden [e-mail](https://wmaraci.com/nedir/e-mail) göndermeye yardımcı olan internet standardıdır. E- posta sunucuları arasında mesaj aktarma yöntemi Temelde, bir iletinin  bilgisayarınızdan alıcının bilgisayarına yolculuğu aşağıdaki gibidir



13.DNS (DOMAİN NAME SİSTEM) ALAN ADI SİSTEMİ:

Tarayıcınıza adres çubuğuna girdiğiniz site ismini IP Adresine çevirir ve yönlendirir. Örnek olarak Tarayıcınıza ‘’ GOOGLE’ in IP adresi 74.125.224.83 adresini yazmaz onun yerine [www.google](http://www.google/) .com yazarız DNS sunucusu bu adresi IP adresine yönlendirir. DNS sunucusu Site isimlerini IP adreslerine yönlendiren bir veri tabanına sahip bilgisayar sunucusudur. Bu sistem SMTP Protokolü için e-posta yönlendirmesi için genişletilmiştir.

14.İNTERNET METİN MESAJLARININ ARPA STANDARTINDA FORMATI:

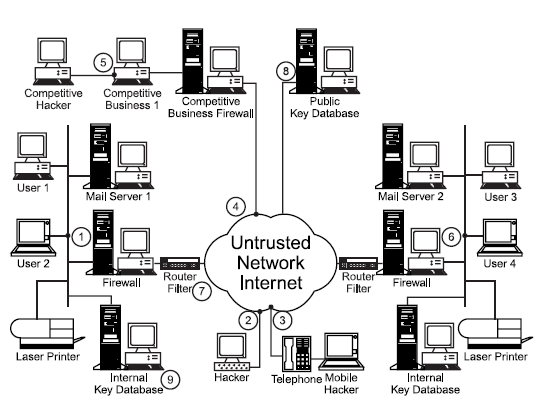
Başlangıçta RFC -822 diğer RFC tarafından genişletilmiş ve değiştirilmiştir. Bu standart değiştirilecek mesajların biçimin belirler. Metin bilgisi içermeyen Çok parçalı mesaj gövdelerini kodlamak için standart bir yöntemdir.

GÜVENLİ POSTA GÖNDERİMİ:

Mesaj Göndermeden Özel ağından özel bir şifreleme anahtarı alır. Yazar Mesajı gönderen Ağlara iki ortak anahtar yerleştirir. Birincisi İç anahtar halkasına yerleştirilmiş İkincisi ise genel anahtardır.(Burada amaç İç postaları gizli tutmaktır. Mesajı yazan genel özel anahtar şifrelemesini kullanabilir. E-posta gönderen Kişisel network unda oturum açar posta sunucusu tarafından şifre kullanılarak mesaj gönderilmeye hazır hale gelir. Kişisel posta yardımcı programını kullanarak mesajı oluşturur. Mesajların Güvenliği için tüm mesajlar dijital imza ile gönderilecek tüm mesajlarda alındı bilgisi olacak özel anahtar şifreleme otomatik olarak kullanılacaktır. Yazar Dokumanı imzalar(mesajı) ve güvenli bir sunucuya gönderir. Mesaj şifrelenir ve dijital olarak imzalanır. Yazarın Posta sunucusu donanım düzeyinde dahili iletişimi korumak için yönlendiriciler(Routerler) şifrelenir.

Posta sunucusu trafiğin dahili mi yoksa harici mi olduğunu belirler mesajı uygun şekilde güvenlik duvarına iletir. Routerler tarafından internete iletilir. Alıcının Güvenlik duvarının önündeki ROUTER Bu katmandaki trafiğin şifresini çözer ancak ancak şifreli bırakır.. Mesaj daha sonra alıcının güvenlik duvarı tarafından alınır ve mesaj adreslemesini esas alarak mesaja izin verilir. Güvenlik duvarı mesajı virüslere karşı tarar ve posta sunucusuna iletir. Mesaj alıcı oturum açana kadar posta sunucunda saklanır. Posta sunucusu şifre korumalıdır ve burada bulunan tüm veriler ayrıca şifrelenir.

Posta sunucusu daha sonra mesajı bireysel kullanıcıya iletir. sonra mesajı açar imza temelli eşleşen mesaj özetlerini doğrular. Alındı bildirimi otomatik olarak oluşturulur ve geri iletilir.



Kaynakça

1. NIPC Advisory 02*-*001: Internet Content Advisory: Considering the Unintended Audience, National

Infrastructure Protection Center, January 17, 2002.

2. *Service Member’s Personal Protection Guide: A Self-Help Handbook to Combating Terrorism*, U.S. Joint

Chiefs of Staff, Joint Staff Guide 5260, July 1996.

3. *Joint Tactics, Techniques and Procedures for Antiterrorism*, U.S. Joint Chiefs of Staff, Joint Pub 3*-*07.2, 17

March 1998, Appendix.

4. *ATF Bomb Threat Checklist*, ATF-F 1613.1, Bureau of Alcohol, Tobacco and Firearms, June 1997.

5. Merrill Lynch Resumes Critical Business Functions within Minutes of Attack, Janette Ballman, *Disaster*

*Recovery Journal*, 14, 4, p. 26, Fall 2001.