**1. Slayt - Overview**

---

- **Confidentiality** → privacy
- **Integrity** → bütünlük, guarding against improper information, modification, destruction, sızmıyor ama değiştirilmemesi gerekiyor
- Authentication → verified, trusted
- Accountability → requirement for actions, traced, log kayıtları
- **Availability** → timely and reliable access to and use of information

---

- Physical and logical placement
- asset → system resource
    - hardware, software, data, communication facilities and networks

---

- corrupted → integrity
- leaky → confidentiality
- unavailable → availability

---

- threat → if happened → attack
    - active, passive, insider, outsider

---

- countermeasures
    - prevent, detect, recover
    - may create new vulnerabilities
    - residual vulnerabilities may remain → minimize it

---

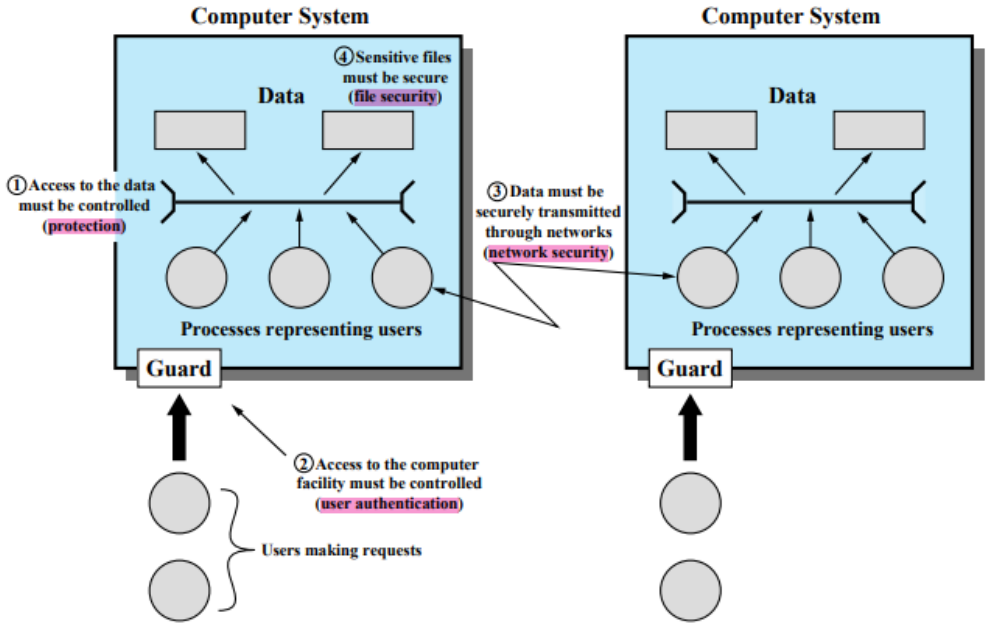
- Unauthorized Disclosure → unauthorized entity gain access to data
    - exposure → sensitive data released
    - interception → unauthorized entity access sensitive data
    - inference → threat, indirectly access sensitive data
    - intrusion → unauthorized entity gains access to sensitive data

- Deception → authorized entity receiving false data and believing it's true
    - masquerade → sahte tavır, unauthorized entity gains access and act like authorized
    - falsification → false data deceive an authorized entity
    - repudiation → entity deceives another entity by denying responsibility

- Disruption → interrupting or preventing the correct operation
    - incapacitation → disable a component
    - corruption → modify system function or data
    - obstruction → engel, prevent system operation
- Usurpation → gasp, control system services by unauthorized entity
    - misappropriation → entity assumes unauthorized logical or physical control of a system resource
    - misuse → perform a function or service that is harmful for system security

---

- protection, user authentication, network security, file security




---

- availability sorunları → direkt çalışmaya başlayamaması
- confidentiality sorunları → güvenlik ve gizlilikle alakalı sorunlar
- integrity sorunları → yanlış veya eksik çalışması

---

- passive attack → kulak misafiri, trafik analizi, mesajları okuma ve yayınlama
- active attack → sistem kaynaklarını kullanma, DoS, Masquerade, Modification of messages

---

- audit → denetim
- contingency → beklenmedik durum
- maintenance → bakım

- assessment → değerlendirme
- acquisition → kazanç

---

- attack surfaces
    - open ports, services that are inside of firewall, code that process incoming data, SQL and web forms, betrader employee
    - network attack → internet, DoS attack
    - software attack → application, OS Codes, web server in software
    - human attack → trusted insiders…

- layering arttıkça risk düşer
- attack surface genişledikçe risk artar

---

- Strategy
    - prevention
    - detection
    - response
    - recovery

    - assurance → güvence
    - evaluation → değerlendirme

---

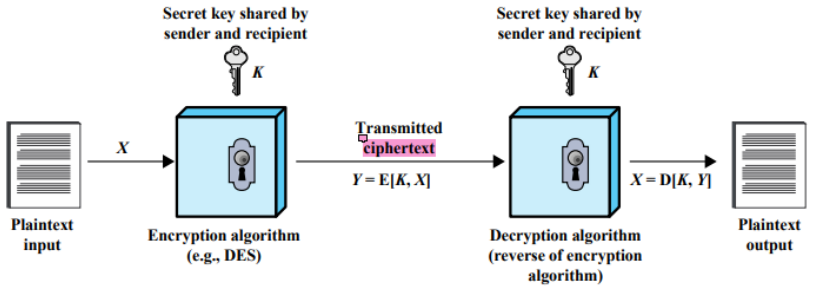
- Standards
    - NIST
    - ISOC
    - ITU-T
    - ISO

---

**2. Slayt - Cryptographic Tools**

---

- **Symmetric Encryption** (Conventional Encryption) (Single-Key Encryption)
    - sender and receiver must have copies of **secret key**




- **Attacking** symmetric encryption
  - Cryptanalytic Attacks
    - general characteristic of plain text
    - sample plain - cipher pairs
    - nature of algorithm
  - Brute-Force Attacks
    - try all

---

- **Data Encryption Standard (DES)**
  - Data Encryption Algorithm (DEA)
  - 64 bit plain - 56 bit key
  - FIPS PUB 46

- **Triple DES**
  - repeats DES
  - 2 or 3 keys
  - 168 bit key (overcome Brute-Force attacks) - 64 bit plain block
  - key uzun

- **Advanced Encryption Standard (AES)**
  - FIPS 197

| | DES | Triple DES | AES |
|---|---|---|---|
| **Plaintext block size (bits)** | 64 | 64 | 128 |
| **Ciphertext block size (bits)** | 64 | 64 | 128 |
| **Key size (bits)** | 56 | 112 or 168 | 128, 192, or 256 |

---

- **Electronic Codebook (ECB)** → multiple block encryption
  - each block using same key
  - regularities may be a problem

- **Modes of Operation** → overcomes the weakness of ECB

- Types of Symmetric Encryption
    - Block Cipher
        - output one block at a time
        - reuse keys
        - more common
    - Stream Encryption
        - continuously
        - output one element at a time
        - faster
        - use less code
        - encrypt one byte at a time
        - pseudorandom stream → unpredictable without knowledge of the input key

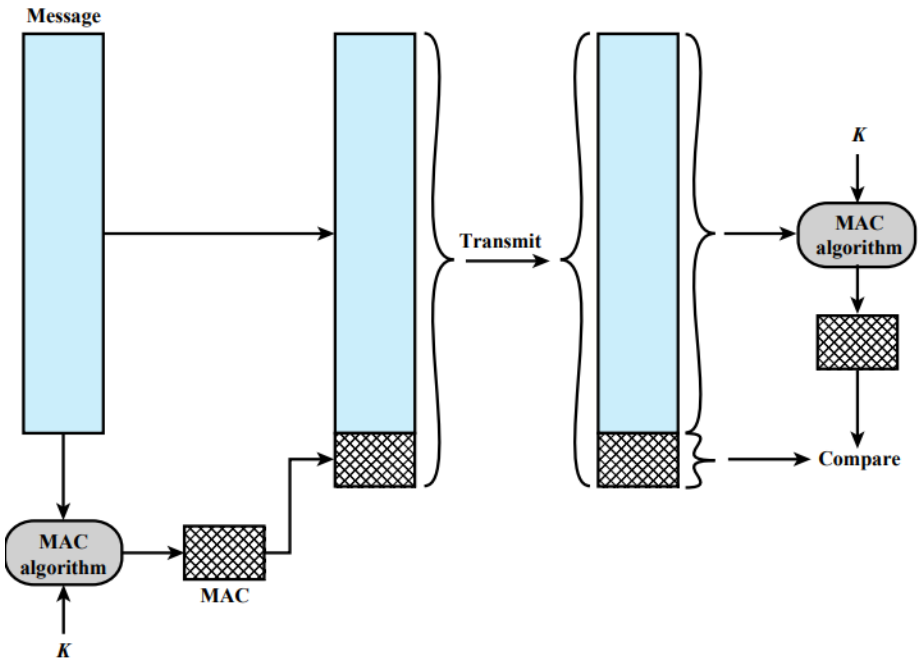
- conventional encryption → only sender and receiver share a key

---

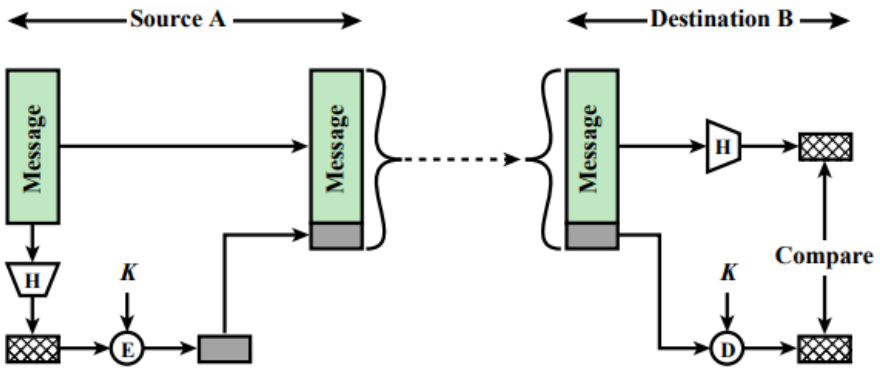
- **Message Authentication Without Confidentiality**
    - encryption is not enough for secure authentication
    - combine **authentication** and **confidentiality**
        - encrypted message + its authentication tag
    - generally message authentication separated from message encryption

**Şemalar**

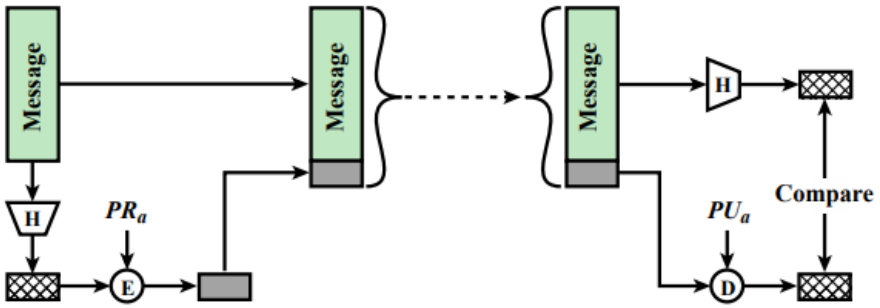
- Message Authentication Using **MAC** (Message Authentication Code)



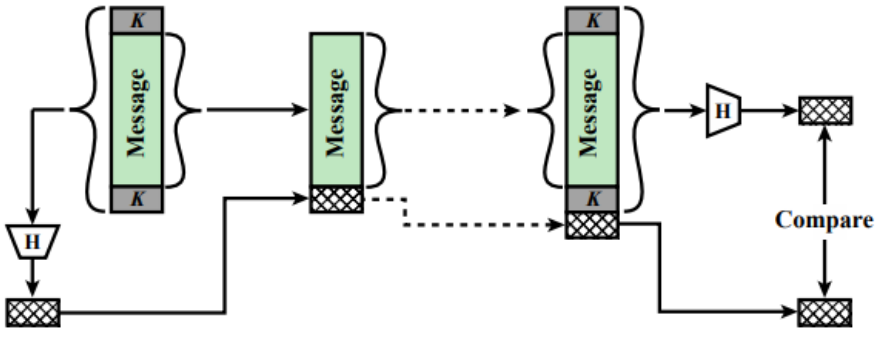
- Message Authentication Using a **One-Way Hash** Function




(a) Using symmetric encryption




(b) Using public-key encryption




(c) Using secret value

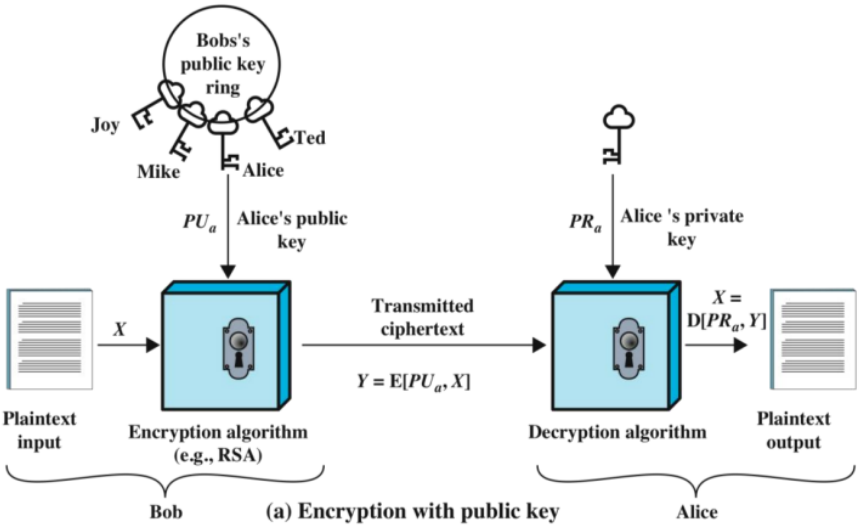
---

- hash function
  - fixed length output
  - can be applied any size of block
  - H(x) easy to compute any x

    - one way and preimage resistant → hard to invert
    - infeasible for **y != x** such that **H(y) = H(x)**
    - collision resistant any pair (x,y) such that H(x) = H(y)

- security of hash functions
    - attacking approaches
        - logical weakness
        - length of hash code

---

- **Public Key Encryption**
    - Diffie and Hellman
    - Asymmetric → two separate keys (public and private)
    - 

    - eğer bob kendi private keyi ile encrypt etseydi bob'un public key ine sahip olan herkes okuyabilirdi (public-key cryptography)

---

- Applications for Public Key Cryptosystems
    - requirements for PK
        - easy to create key pairs
        - either key can be used each role
        - easy for sender knowing public key to encrypt messages
        - easy for receiver knowing private key to decrypt cipher text
        - infeasible to determine private key to public key
        - infeasible recover original message

| Algorithm | Digital Signature | Symmetric Key Distribution | Encryption of Secret Keys |
|---|---|---|---|
| RSA | Yes | Yes | Yes |
| Diffie-Hellman | No | Yes | No |
| DSS | Yes | No | No |
| Elliptic Curve | Yes | Yes | Yes |

- Asymmetric Encryption Algorithms
  - RSA
    - most widely used
  - Diffie-Hellman
    - key exchange
    - limited exchange
    - symmetric encryption of messages
  - DSS (Digital Signature Standard)
    - cannot be used for encryption
    - cannot be used for key exchange
  - Elliptic Curve Cryptography (ECC)
    - secure like RSA but much smaller keys

---

- **Digital Signatures**
  - The result of a cryptographic transformation of data
  - Signatory non-repudiation
  - data dependent bit pattern
  - 3 digital signature algorithm:
    - DSA (Digital Sign. Alg.)
    - RSA
    - ECDSA (Elliptic Curve Boku)

---

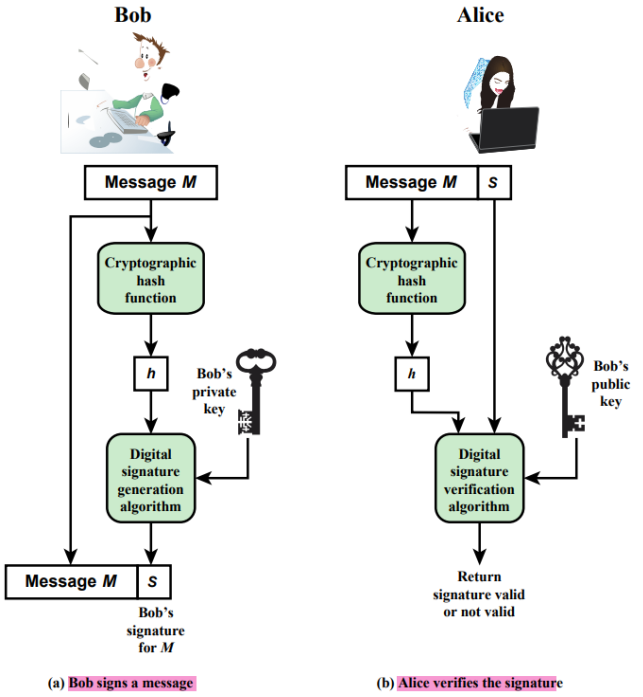



**Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process**

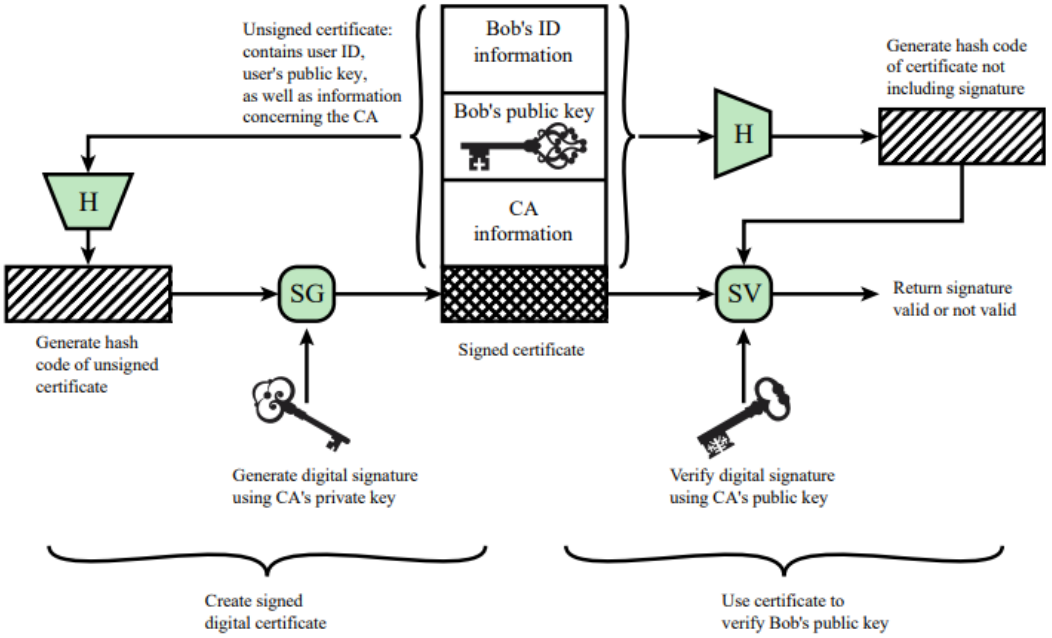



**Figure 2.8 Public-Key Certificate Use**

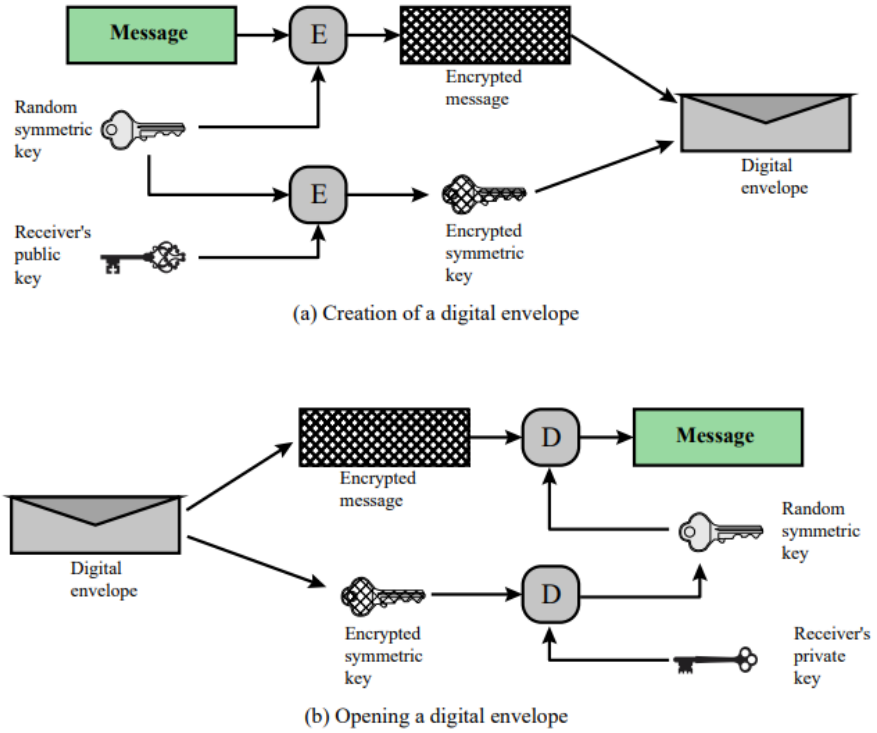



**Figure 2.9 Digital Envelopes**

---

- Random Numbers
  - keys for public key algorithms
  - stream key for symmetric stream cipher
  - symmetric key for temporary session key or digital envelope
  - **handshaking** to prevent replay attacks
  - session key

  - randomness
    - uniform
    - independence
  - unpredictability
    - statistically independent
    - not be able to predict future element

- algorithmic techniques numbers are not statistically random

- Pseudorandom Numbers
  - sequences that satisfy statistical randomness tests
  - likely to be predictable

- True Random Number Generator

    - nondeterministic source
    - unpredictable natural process
    - provided on modern processors

---

- Encryption on Stored Data

---

**3. Slayt - User Authentication**

---

- Identification Step
- Verification Step

- multifactor authentication for local and network access to privileged accounts
- network access to non-privileged accounts
- replay-resistant authentication mechanism for network access
- prevent reuse of identifiers
- disable identifiers after defined period ends or inactivity
- minimum password complexity and change of characters
- prevent password reuse
- kalıcı şifrede değişiklik için geçici şifreler oluştur
- sadece kriptografik olarak korunan şifreleri sakla ve ilet
- authenticating user identity:
    - individual know → password
    - individual possesses → token, smartcard
    - static biometrics → fingerprint
    - dynamic biometrics → voice pattern

- multifactor authentication

- assurance level → potential impact → areas of risk

- assurance (güven) level
    - the degree of confidence
    - four level of assurance
        - 1 → no confidence with asserted identity's validity
        - 2 → some
        - 3 → high
        - 4 → very high
- potential impact
    - low → limited adverse effect
    - moderate → serious adverse effect
    - high → severe adverse effect

| Potential Impact Categories for Authentication Errors | Assurance Level Impact Profiles | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Inconvenience, distress, or damage to standing or reputation | Low | Mod | Mod | High |
| | Low | Mod | Mod | High |
| Financial loss or organization liability | None | Low | Mod | High |
| Harm to organization programs or interests | None | Low | Mod | High |
| Unauthorized release of sensitive information | None | None | Low | Mod/ High |
| Personal safety | | | | |
| Civil or criminal violations | None | Low | Mod | High |

- **Password Based Authentication**
  - name password
  - user ID
    - authorized access
    - privileges
    - optional access control
  - vulnerabilities
    - offline dictionary attack
    - password guessing
    - popular password
    - exploiting user mistakes
    - multiple password use
    - electronic monitoring

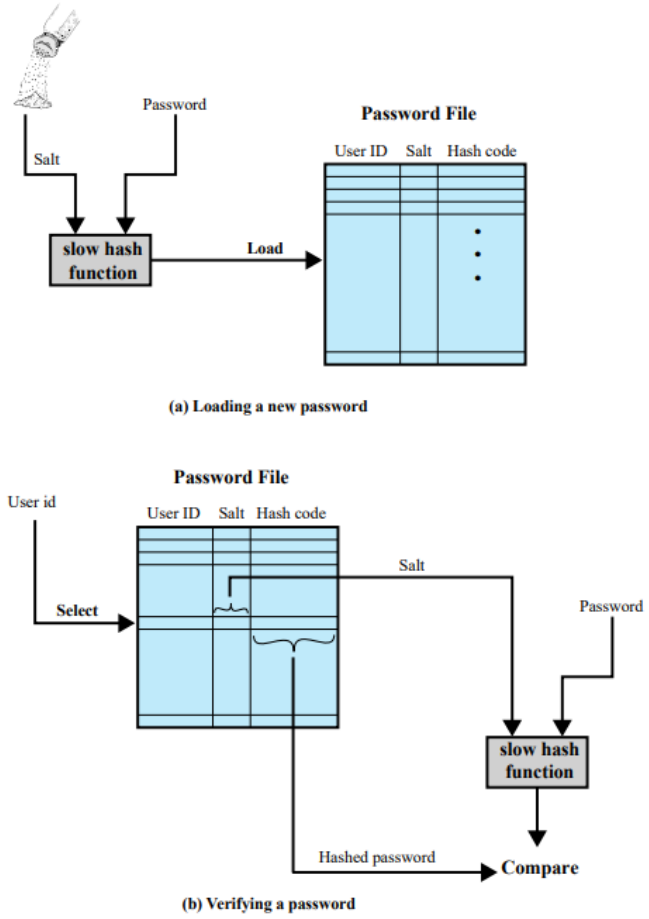



**Figure 3.3 UNIX Password Scheme**

- original scheme
  - 8 char
  - 12-bit salt, DES encryption, one-way hash
  - output translated 11 char seq

- improved implementations
  - stronger hash/salt
  - hash based on MD5 → 48 bit salt, password length unlimited, 128 bit hash
  - OpenBSD uses Blowfish block cipher based hash algorithm called **Bcrypt**
    - most secure
    - 128 bit salt, 192 bit hash
- password cracking
  - dictionary attacks
    - must be stored with hashed salt value
  - rainbow table attack
    - precompute table of hash values for all salts
    - mammoth table of hash
    - counter → large salt and large hash
  - easy passwords
  - John the Ripper
    - open source password cracker, brute force + dictionary

- modern approaches
    - complex password
    - but also crackers are improved

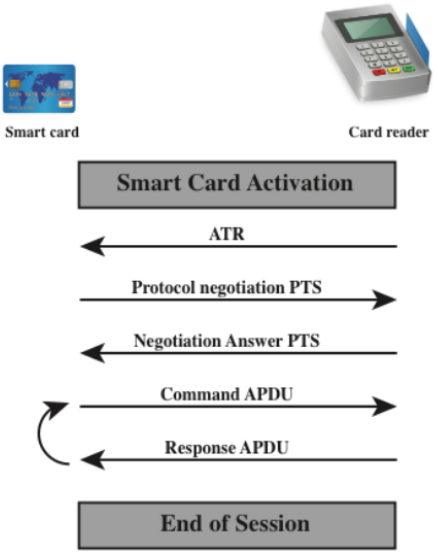
- password file access control
    - available for only privileged users
    - shadow password file
    - vulnerabilities
        - OS weakness
        - accident with permissions
        - same password user
        - backup media
        - network traffic sniffing
- reactive password checking
    - try guessable passwords periodically
- proactive password checking
    - rule enforcement
    - password checker
    - bloom filter
        - quick and memory friendly table creator for hash values
        - check desired passwords against this table

---

- types of card used as **token**
    - embossed → old credit card
    - magnetic type → bank card
    - memory → electronic memory inside
        - can store but not process
        - iş bankası kartım
        - requires special reader
        - loss of token
    - smart → electronic memory and processor
        - contact
        - contactless

- smart tokens
    - manual interfaces include a keypad or display
    - electronic interfaces, contact or contactless
    - static, dynamic password generator, challenge response

- smart cards (category of smart token)
    - credit cards
    - electronic interface
    - microprocessor, memory, IO Ports
        - memory → ROM, EEPROM, RAM

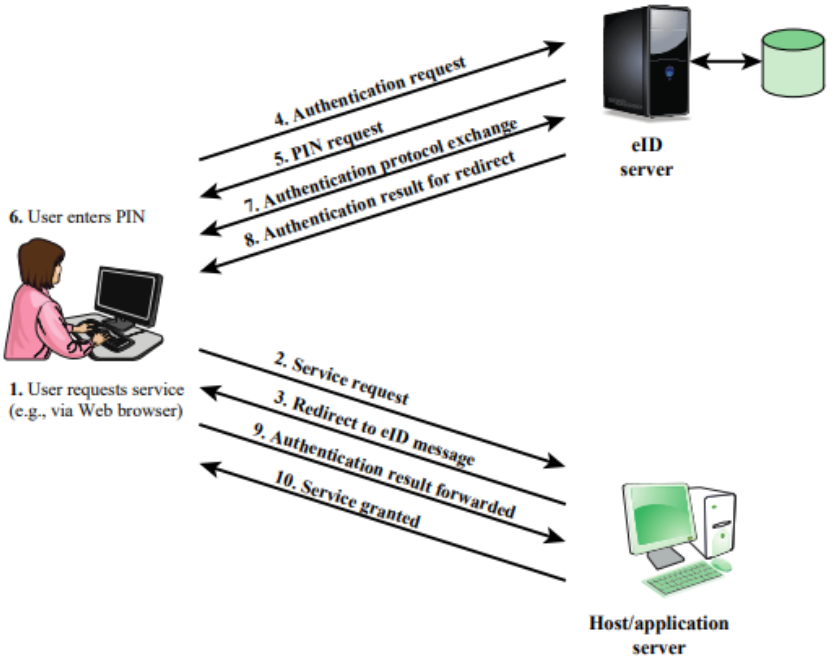



APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection

**Figure 3.6 Smart Card/Reader Exchange**

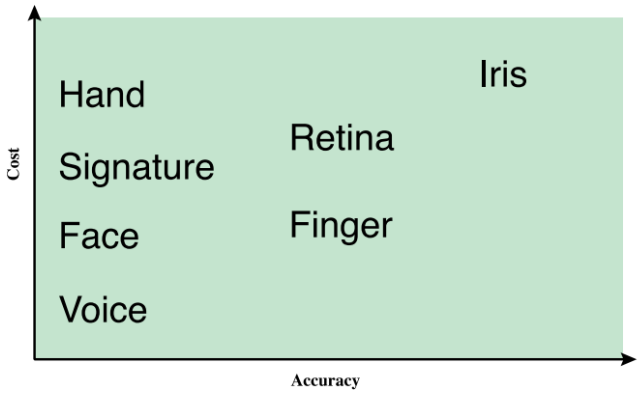
- **Electronic Identity Cards (eID)**
  - a smart card
  - national identity card ehliyet örnek
  - stronger proof of identity

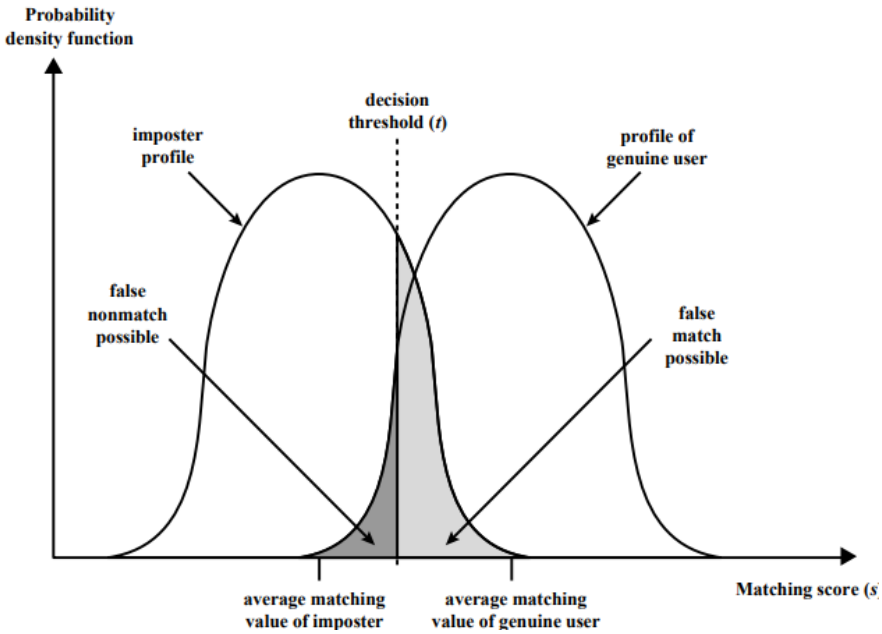
- ePass, eID, eSign tablosu




- **Figure 3.7 User Authentication with eID**

- **Password Authenticated Connection Establishment (PACE)**
  - ensure RF chip cannot read without explicit access control
  - PIN check
  - for offline, MRZ printed on the back or CAN on the front is used
    - CAN = card access number
    - MRZ = machine readable zone

- Biometric Authentication
  - physical characteristic
  - pattern recognition
  - 

  - verification → bilinenle karşılaştırma
  - identification → tanıma (bütün templateler ile karşılaştır)
  - 

  - bunun gibi iki üç tane daha grafik var…

- Remote User Authentication
  - over network
  - extra risks
  - rely on challenge-response protocol
  - protocol schemes

| Attacks | Authenticators | Examples | Typical defenses |
|---|---|---|---|
| **Client attack** | Password | Guessing, exhaustive search | Large entropy; limited attempts |
| | Token | Exhaustive search | Large entropy; limited attempts, theft of object requires presence |
| | Biometric | False match | Large entropy; limited attempts |
| **Host attack** | Password | Plaintext theft, dictionary/exhaustive search | Hashing; large entropy; protection of password database |
| | Token | Passcode theft | Same as password; 1-time passcode |
| | Biometric | Template theft | Capture device authentication; challenge response |
| **Eavesdropping, theft, and copying** | Password | "Shoulder surfing" | User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication |
| | Token | Theft, counterfeiting hardware | Multifactor authentication; tamper resistant/evident token |
| | Biometric | Copying (spoofing) biometric | Copy detection at capture device and capture device authentication |
| **Replay** | Password | Replay stolen password response | Challenge-response protocol |
| | Token | Replay stolen passcode response | Challenge-response protocol; 1-time passcode |
| | Biometric | Replay stolen biometric template response | Copy detection at capture device and capture device authentication via challenge-response protocol |
| **Trojan horse** | Password, token, biometric | Installation of rogue client or capture device | Authentication of client or capture device within trusted security perimeter |
| **Denial of service** | Password, token, biometric | Lockout by multiple failed authentications | Multifactor with token |

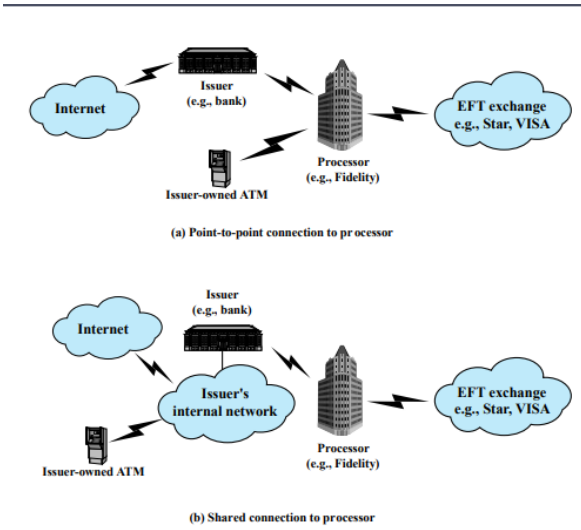



Figure 3.15 ATM Architectures. Most small to mid-sized issuers of debit cards contract processors to provide core data processing and electronic funds transfer (EFT) services. The bank's ATM machine may link directly to the processor or to the bank.

# Case Study: ATM Security Problems

- eavesdropping → adversary attempts to learn password
- host attacks → host → storage
- replay → repeats a previous captured user response
- client attacks → iletişimde araya girerek authentication kazanmaya çalışmak
- trojan horse → application or physical device that purposes capturing a user password
- DoS → bir sürü askerle saldırıp sistemi kilitlemek

---

## 4. Slayt - Access Control

---

- enter specific physical facilities

- limit information for unauthorized user or applications or transactions or functions
- separate the duties of individuals
- least privilege
- limit unsuccessful login attempts
- use session lock
- terminate automatically a user session after defined condition
- monitor and control access?? sadece yap, LATTE!
- remote access session için kriptoloji ile kontrol sağla
- remote access olanları kontrol edilen noktalardan (router) geçir
- wireless access yaparken de kriptoloji
- mobil cihazları kontrol et
    - bilgileri enkript et
- use of external information ı kısıtla, kontrol ve verify et
- portable storage kullanımını limitle
- public datayı kontrol et

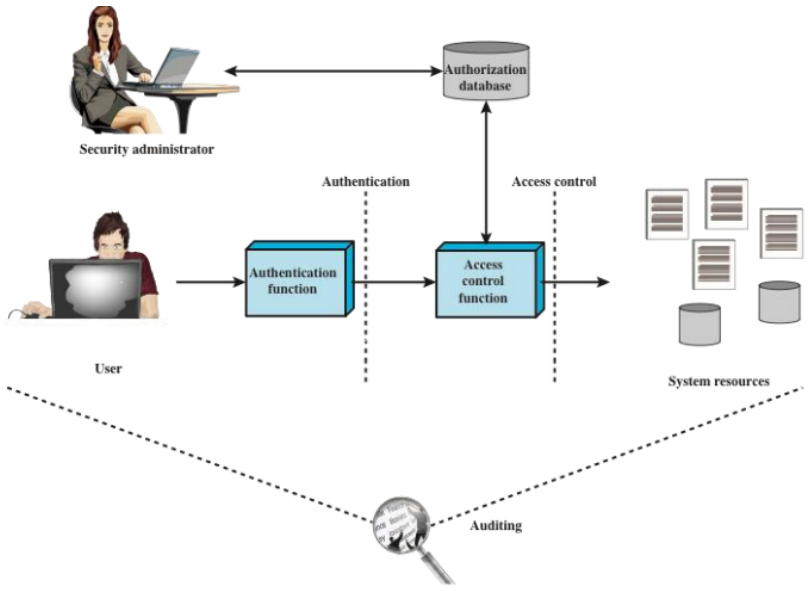
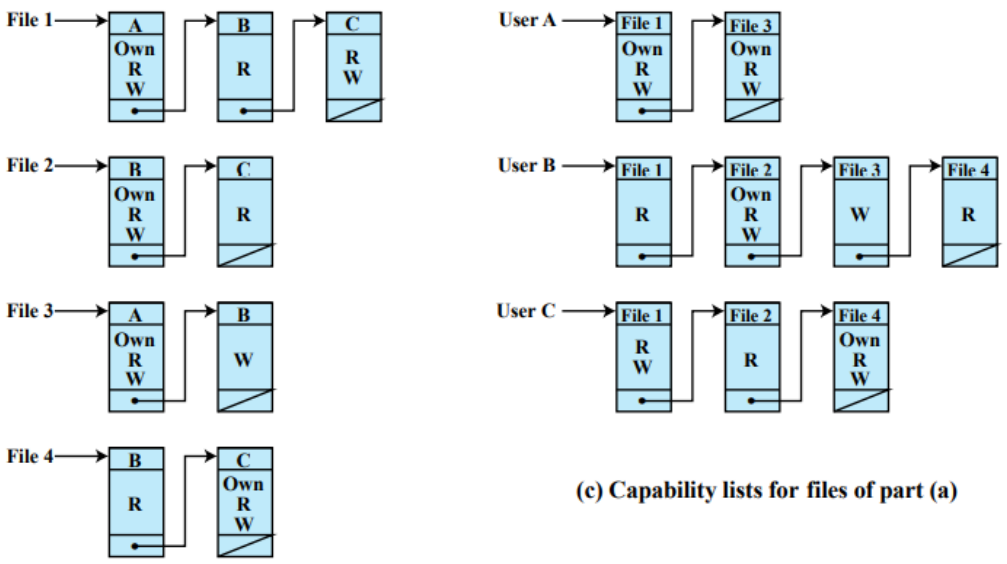



Figure 4.1 Relationship Among Access Control and Other Security Functions

- **Access Control Policies**
  - DAC Discretionary (isteğe bağlı) Access Control
    - control access based on identity, access rules
    - bir entity diğerine access izni verebilir
    - using an access matrix
  - Role-based access control (RBAC)
    - based on roles
  - Attribute-based access control (ABAC)
    - based on attributes of user
  - Mandatory Access Control (MAC)
    - comparing security labels with security clearances
    - bir entity diğerine access izni verebilir

- Subjects
  - an entity
  - owner, group, world
- Objects
  - a resource
  - entity used to contain or receive information
- Access Rights
  - subject object access control
  - read, write, execute, delete, create, search



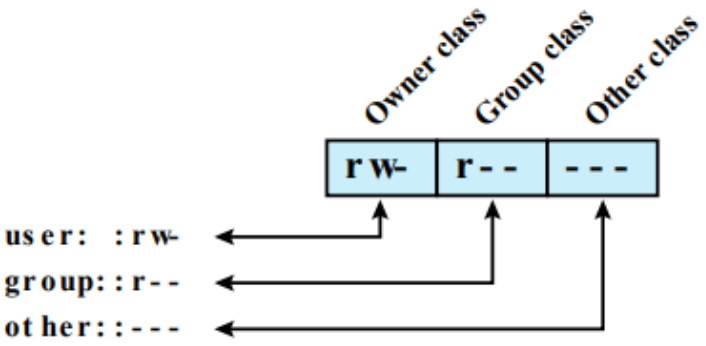

b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)

- **Figure 4.2 Example of Access Control Structures**

- **Protection Domains**
  - toplu izinler verme gibi bir olay sanırım
  - can be static or dynamic
  - certain memory areas and instructions are forbidden for user mode
  - kernel mode → everything is alright

- **UNIX File Access Control**
  - UNIX files are administered using inodes (index nodes)
  - several files may be associated with a single inode
  - active inode → exactly one file
  - file attributes, permissions, control info → sorted in inode
  - inode table
    - on the disk
    - inodes of all files
  - directories are structured in a hierarchical tree
    - file names + pointers in inodes
  - user ID, group ID
  - 12 protection bits
  - The owner ID, group ID, and protection bits are part of the files' inode




(a) Traditional UNIX approach (minimal access control list)

**Figure 4.5 UNIX File Access Control**

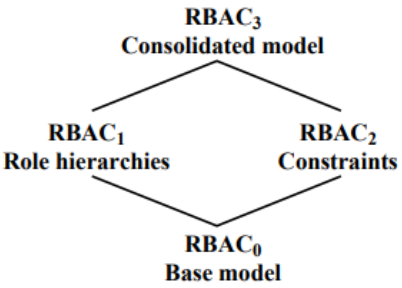
  -

- Traditional UNIX File Access
  - Set user ID
  - Set group ID
  - Sticky bit
    - only owner rename move or delete
  - SUper user
    - isterse ananı bile

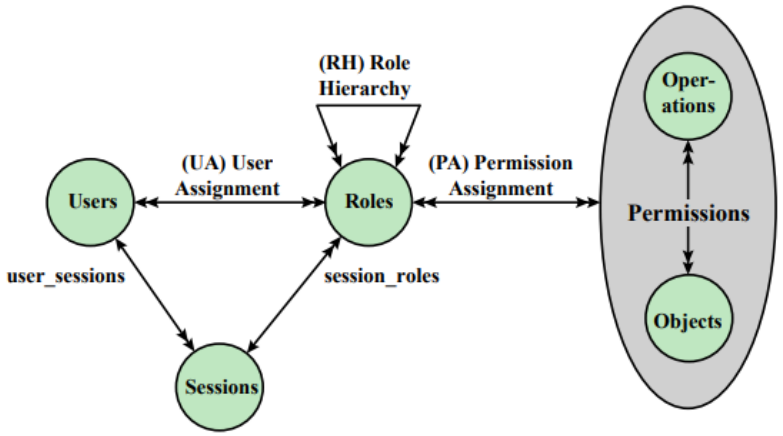
- Access Control Lists (ACL) in UNIX
  - FreeBSD (Free BDSM)
  - Setfacl command assigns a list of UNIX user IDs and group
  - read write execute protection bits
  - file does not need to have an ACL
  - protection bit → the file has or has not extended ACL

- request anında

    - select ACL
    - check permissions
- RBAC (role)
    - scope → 0,1,2,3




(a) Relationship among RBAC models




(b) RBAC models

**Figure 4.8 A Family of Role-Based Access Control Models.**

    - 
    - constraints
        - Mutually exclusive roles
            - one user - one role in the set
            - any permission can be granted to only one role in the set
        - Cardinality
            - Setting a maximum number with respect to roles
        - Prerequisite roles
            - şartlı rollendirme
            - bir rolü varsa diğerini ona göre vermek gibi

- ABAC (attribute)
    - flexible and powerful
    - concern about performance → her access olduğunda subject ve object attribute kontrolü
    - XAMCL (eXtensible Access Control Markup Language)

    - subject attributes
        - active entity

        - define the identity and characteristic of the subject
        - role is also attribute
    - object attributes
        - passive information
        - can have privilege make access control decisions
    - environment attributes
        - operational, technical, situational env.
        - context which is created when information access occurs
        - ignored most access control policies

    - Distinguishable because it controls access to objects by evaluating rules against the attributes of entities
    - Systems are capable of enforcing DAC, RBAC, and MAC concepts
    - unlimited number of attributes to be combined

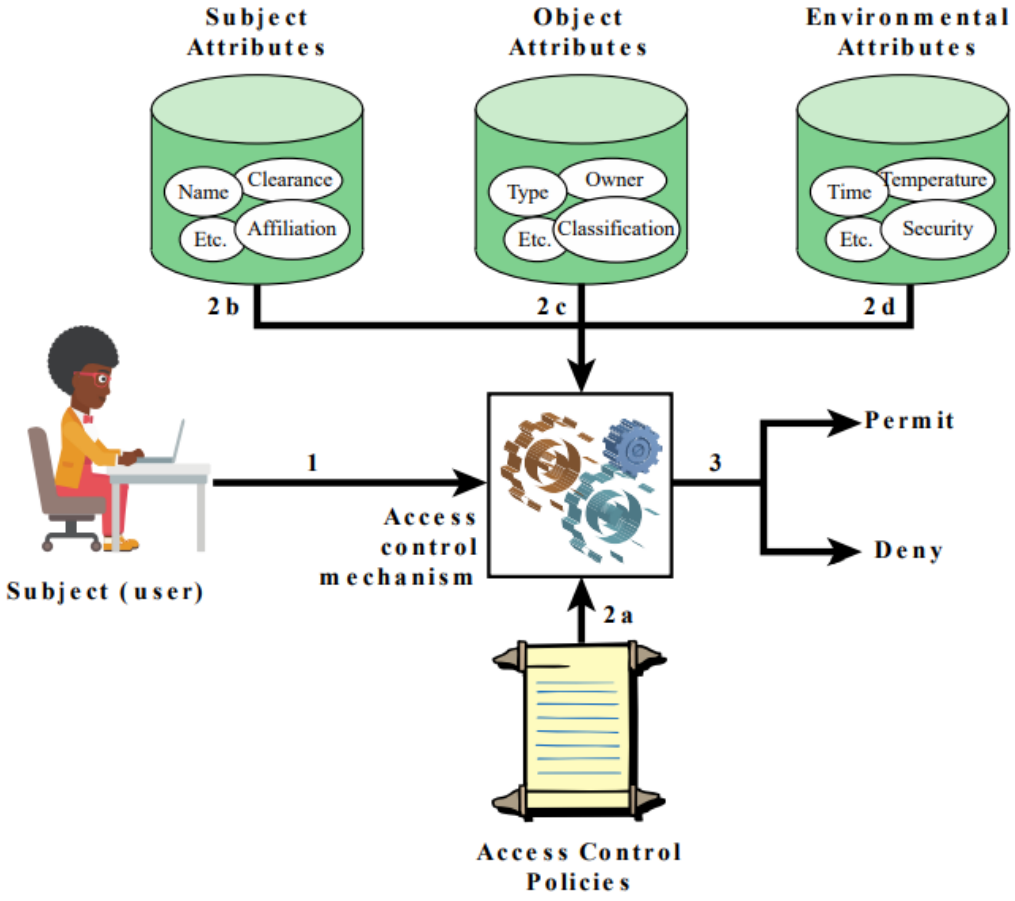
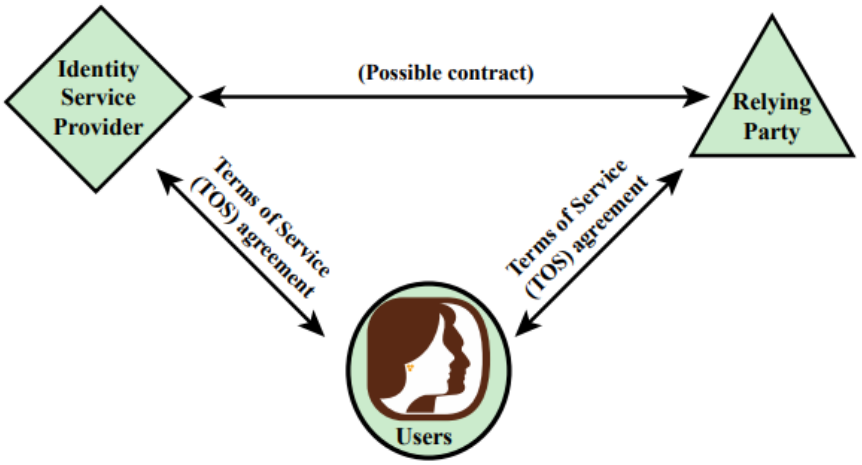



Figure 4.10 ABAC Scenario

    - ABAC Policies
        - ...
    - Other terms commonly used instead of privileges are: rights, authorizations, and entitlements

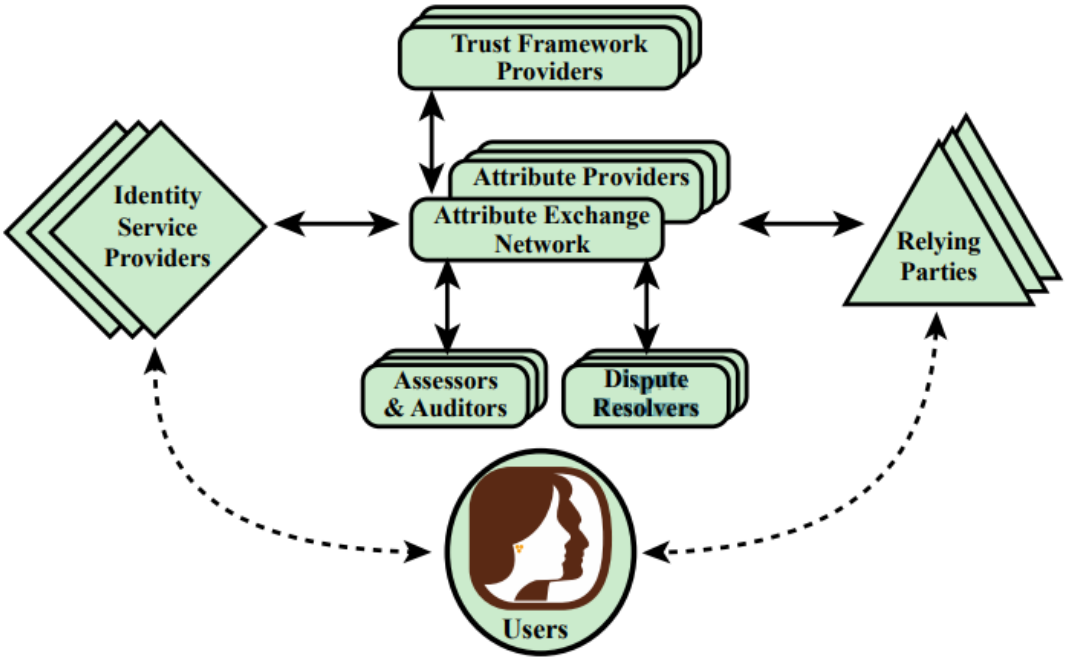
- Identity, Credential, and Access Management (ICAM)
  - Developed by the U.S. government
  - create digital identity representations for users
  - Identity Federation
    - …




**(a) Traditional triangle of parties involved in an exchange of identity information**

  -

- Open Identity Trust Framework
  - OpenID
    - open standard that allows users to be authenticated by certain cooperating sites using a third party service
  - OIDF
    - international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies
  - ICF Information Card Foundation
    - nonprofit community of companies and individuals working together to evolve the Information Card ecosystem
  - OITF
    - Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF
  - OIX
    - Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the OITF model
  - AXN
    - Attribute Exchange Network is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs




(B) Identity attribute exchange elements

**Figure 4.13 Identity Information Exchange Approaches**

---

**5. Slayt - Malicious Software**

---

- malware → kötü amaçlı yazılım
- Advanced persistent (kalıcı) threat → Cybercrime directed at business and political targets,
- Adware (reklam yazılımı) → pop-up, redirection, commercial
- Attack kit → generating new malware automatically
- Auto-rooter → hacker tool for breaking into new machines
- Backdoor (trapdoor) → normal güvenlik kontrolünü geçebilen mekanizma
- Downloaders → code that install other items under attack
- Drive-by download → exploit a browser vulnerability to attack when the site is viewed
- Exploits → code, specific to a single or set of vulnerability
- Flooders (DoS client) → large volume data ile saldırma, DoS benzeri bir atak
- Keyloggers → basılan tuşlar üzerinden hack
- Logic bomb → inserted into malware, trigger alınca açığa çıkar
- Macro Virus → embedded in a document, triggered when the document is viewed, run and replicate itself to other documents
- Mobile Code → software, execute with identical semantics
- rootkit → hacker tool, used after breaking into to access root-level
- spammer programs → large volumes of unwanted e-mail
- spyware → bilgisayardan bilgi toplayıp başka sisteme aktaran yazılım
- neye göre sınıflandırılıyor

    - how to spread
    - actions or payloads
    - needed host program (virus) or independent (worms, trojans, bots)
    - does not replicate (trojan, spam mail) - replicate (viruses and worms)

- infection and subsequently spread → viruses
- exploit vulnerabilities → worms, drive-by-downloads, replicate
- social engineering → respond phishing attacks, convince user

- corruption of system or data files
- theft of service → zombie agent → part of botnet
- theft of info from system → keylogging
- sistemde varlığını gizleme

- Attack Kits
    - toolkits → crimeware → Zeus • Angler • Blackhole • Sakura • Phoenix
- Attack sources
    - politically motivated
    - criminals
    - organized crime
    - hizmet satan organizasyonlar
    - ulusal devlet destekli ajanslar

- Advanced Persistent Threats (APTs)
    - usually business or political
    - devlet destekli veya suç girişimleri
    - **kesin target seçimi** yapılır
    - ADVANCED
        - yüksek teknoloji uygulamalar ve elle baştan kodlamalar içerir
        - seçili hedefe uygun tool seçimi
    - PERSISTENT
        - uzun süreli saldırı veya saldırı planı, başarı oranını artırır
    - THREATS
        - işin içine aktif insan katılımı olunca ataklar daha başarılı oluyor

- APT Attacks
    - Aim → altyapıda bulunan veriye veya altyapının fiziksel olarak kesilmesine yönelik
    - Techniques used → social eng., spear-phishing email, drive-by-downloads from websites (hedef şirketten biri siteye girerse diye :D )
    - Intent → hedefi çok yönlü olarak etkilemek (payloadlar ile vs.), bir kere sisteme girerlerse daha da güçlenirler

- Viruses
    - replicate
    - easily spread
    - host program çalışırken gizlice çalışabilir

    - bir programa bağlandıktan sonra her şeyi yapabilir
    - sistem donanımı ve işletim sistemi zayıflıklarından faydalanır

- Virus Components
    - infection mechanism → spread and propagate
    - trigger → logic bomb
    - payload → what virus does

- Virus Phases
    - dormant → uykuda, idle mode, bütün virüslerde bu evre yok
    - triggering → activated, because of an event
    - propagation → replicate itself
    - execution → function is performed, harmless or damaging
- Macro and Scripting Virus
    - macro → attaches itself to a document, macro programming capabilities
        - infect scripting code
        - platform independent
        - not executable part, infect documents
        - easily spread
        - they infect user documents rather than system programs
        - traditional file system access controls are of limited use in preventing their spread
        - easier to write and modify than traditional executable viruses

- Virus Classifications
    - by target
        - boot sector infector → infects master boot record and spread when the system booted
        - file infector
        - macro virus → infect files with macro or scripting code
        - multipartite virus → infect files in multiple ways sağ ol bilgi için aq

    - by concealment strategy (gizleme stratejisi)
        - encrypted virus
        - stealth virus → hide
        - Polymorphic virus → mutate every infection
        - Metamorphic virus → mutate and rewrites itself completely each iteration

- **Worms**
    - aktif olarak saldıran ve her bulaştığı makineyi bir sonrakine saldırmak için üs olarak kullanan program
    - exploit software vulnerabilities in client or server programs
    - can use network connections
    - spread through shared media
    - spread in macro or script code included in attachments

- Worm Replication

    - email → send itself as an attachment
    - file sharing
    - remote execution
    - remote file access
    - remote login capability

- Target Discovery
    - scanning → (fingerprinting) search for other systems
    - random → different seeds of IPs, causes internet traffic
    - hit-list → potential vulnerable machines → Each infected machine is provided with a portion of the list to scan
    - topological → etkilediği üzerinden yeni kurban buluyor
    - local subnet → kendi ağındaki sistemlere yayılır
- Morris Worm
    - spread on UNIX systems
    - crack local passwords
    - Sent interpreter a bootstrap program to copy worm over

- Worm Tec
    - multiplatform
    - multi-exploit
    - ultrafast spreading
    - polymorphic
    - metamorphic
- Mobile Code
    - “programs that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics”
    - remote system to local system then execute
    - often acts as a mechanism for a virus, worm or trojan

    - Cross-site scripting
    - Interactive and dynamic Web sites
    - E-mail attachments
    - Downloads from untrusted sites or of untrusted software

- Mobile Phone Worms → target smartphone, delete everything and disable phone force to send messages that cost a lot
    - CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages

- Drive-by-Downloads
    - browser vulnerabilities
    - plugin vulnerabilities
    - user views a web page
    - In most cases the malware does not actively propagate as a worm does

- Watering-Hole Attacks
    - variant of drive-by-download
    - hedefin ziyaret ettiği siteleri bulur ve açığını arar
    - sonra hedefi bekler
    - sadece hedefi etkileyen yazılımlar olabilir
    - undetected kalma ihtimalini artırır

- Malvertising
    - web sitelerine malware koy ama riske atmadan
    - attacker reklam için para öder ve reklamın içine yerleştirir
    - tıklayanlara bulaşır
    - spesifik sistemleri etkilemesi ve dinamik olması sebebiyle zor yakalanır

- Clickjacking
    - UI redressing
    - similar to keystrokes (they also hijacking)
    - invisible frame

- Social Engineering
    - spam → phishing
    - trojan → hidden code
    - mobile phone trojan

- Payload System Corruption
    - chernobyl virus
    - klez
    - ransomware → wannacry
    - real world damage → rewrites BIOS code
    - logic bomb → explode command

- Payload – Attack Agents Bots
    - başka bir bilgisayarı ele geçirip onu saldırıları yönetmek için kullanır
    - botnet → bot toplayarak koordine şekilde hareket ettirmek
        - DDoS
        - spamming
        - sniffing traffic
        - keylogging
        - spreading
        - manipulate games
        - ...

- Remote Control Facility
    - botu wormdan ayıran şeydir
    - worm kendini aktive edip yayar
    - bot kontrol edilir

    - bot serverdaki özel bi kanala katılır
        - http protokolü kullanılabilir
    - kontrol mekanizmaları peer-to-peer protokoller kullanır

- Keyloggers and Spyware
    - keylogger → password username
    - spyware → allow monitoring the activity, history, browsing activity, fake site requests
- Phishing
    - social engineering
    - spear-phishing → daha özenli phishing

- Payload – Stealthing
    - Backdoor
        - trapdoor
        - secret entry point
        - pass the security
        - Maintenance hook → a backdoor used by Programmers to debug and test programs
    - rootkit
        - Set of hidden programs installed on a system
        - gives admin privilege
        - classification
            - persistent
            - memory based
            - user mode
            - kernel mode
            - virtual machine based
            - external mode

- **Malware Countermeasure Approaches**
    - ideal solution prevent
    - policy - awareness - vulnerability mitigation (azaltma) - threat mitigation
    - if occurs → detection - identification - removal

- Anti-Virus Software
    - first generation → simple scanners
    - second → heuristic scanners, integrity checking
    - third → activity traps, identify malware by its actions rather than its structure in an infected program
    - fourth → full-featured protection

- Sandbox analysis
    - simulasyon malicious attack in an emulated sandbox or an a virtual machine
    - real sistemi tehlikeye atmadan deneme yapmak
    - difficult side → how long to run each interpretation

- host based behaviour-blocking software
    - malicious atak karşısında host bilgisayarın tepkisini ölçer
    - block malicious actions
    - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics
    - tamamen tespit edilemeden zarar verebilir

- Perimeter (çevre) Scanning Approaches
    - Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall and IDS
    - intrusion prevention measures → blocking the flow of any suspicious traffic
    - the traffic analysis component of an IDS
    - limited to scanning malware

    - two types of monitoring software:
    - ingress (giriş) monitors
        - located at enterprise network and the Internet
        - look for incoming traffic
    - egress (çıkış) monitors
        - Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet
        - outgoing traffic for signs of scanning

---

**6. Slayt - Denial-of-Service Attacks (DoS)**

---

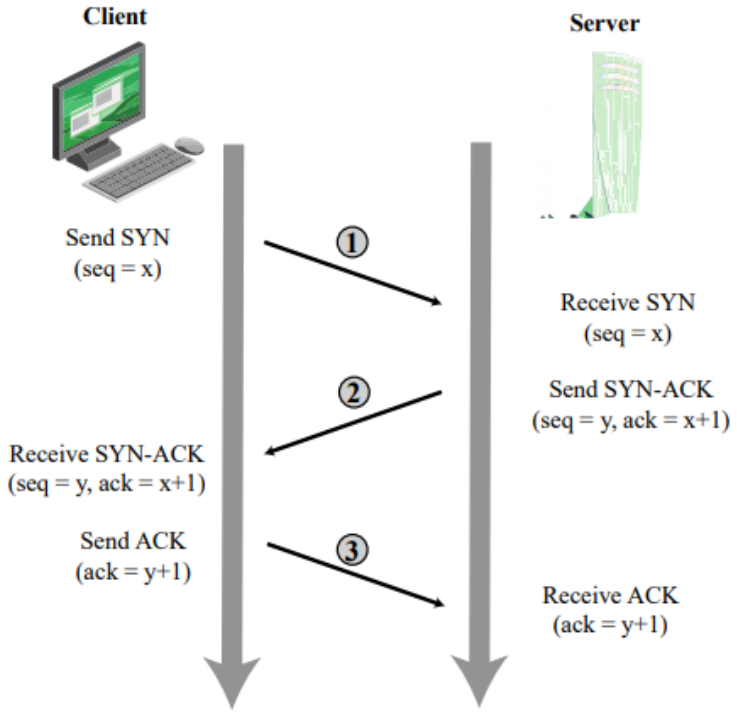
- exhausting resources
- attack to availability service
    - network bandwidth → fill capacity of the network links
    - system resources → network handling software
    - application resources → limit the server to respond to requests

- Classic DoS Attacks
    - flooding ping command
        - overwhelm the capacity of the network connection
        - source of the attack clearly identified (except spoofed address (sahte))

- Source Address Spoofing
    - raw socket interface on operating systems can be used
    - hard to identify

    - congestion → tıkanıklık
    - backscatter traffic → advertise routes to unused IP addresses to monitor attack traffic

- SYN Spoofing
    - Common DoS attack
    - overflowing the tables used to manage responds




    -

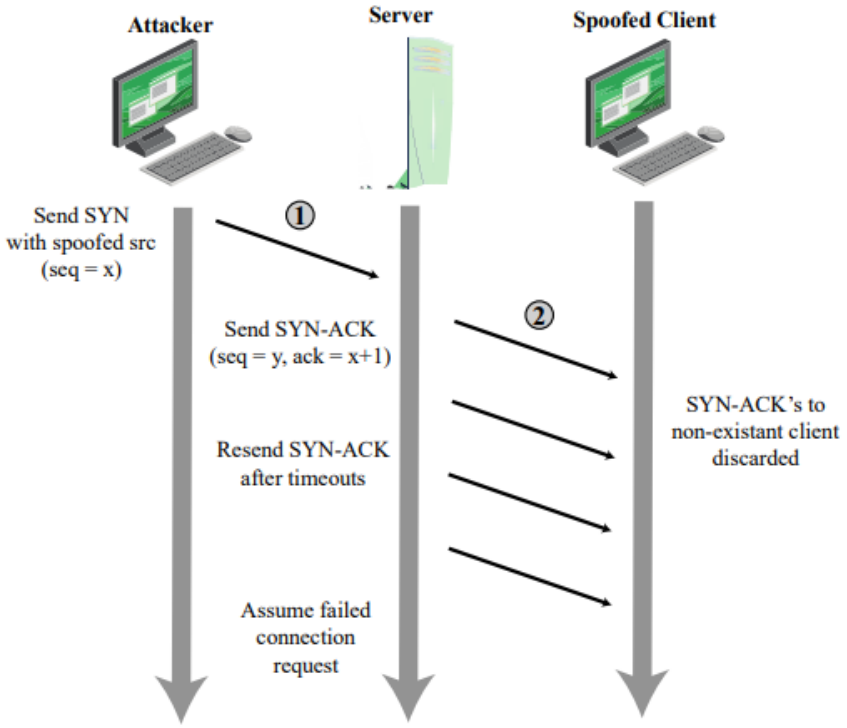



**Figure7.3 TCP SYN Spoofing Attack**

- Flooding Attacks
  - categorize them based on network protocol
  - **ICMP** flood, **UDP** flood → directed to some number port on the system, TCP **SYN** flood → sends TCP packages, total volume of the attack

- Distributed DoS
  - use multiple systems
  - zombie kavramı (install a program)
  - handler zombies - agent zombies
  - botnet can be created

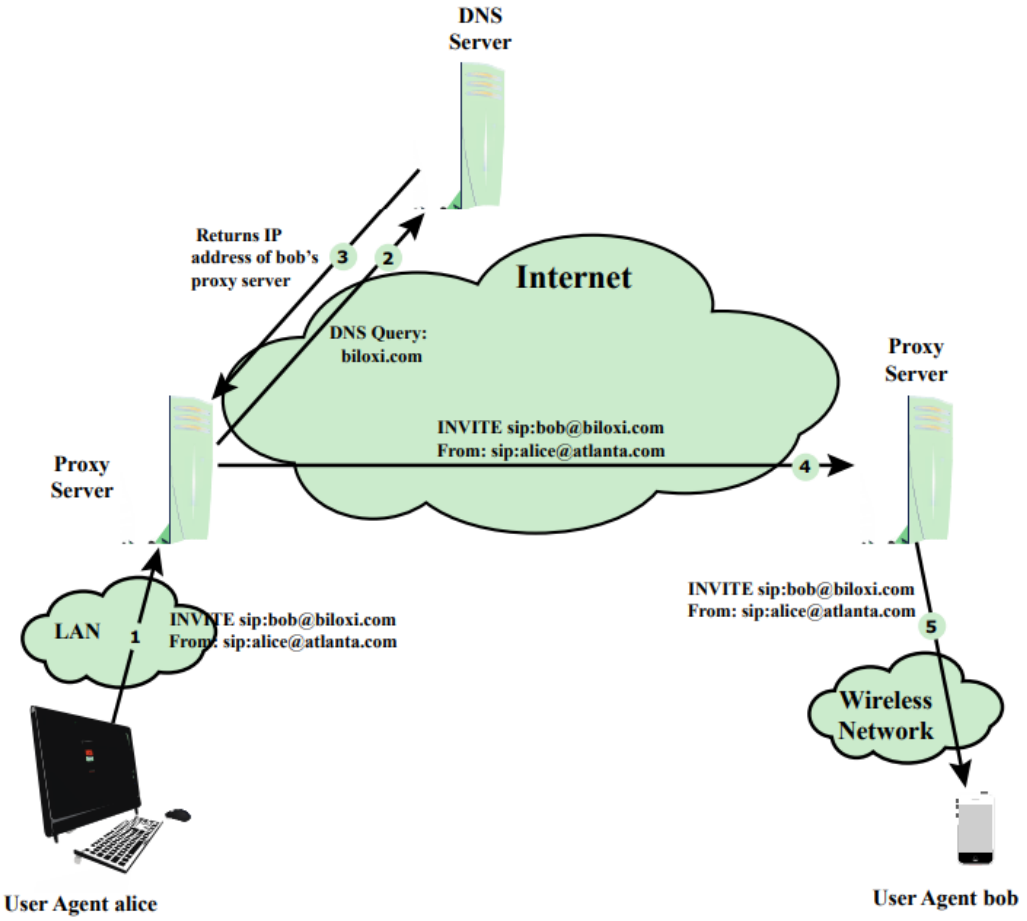
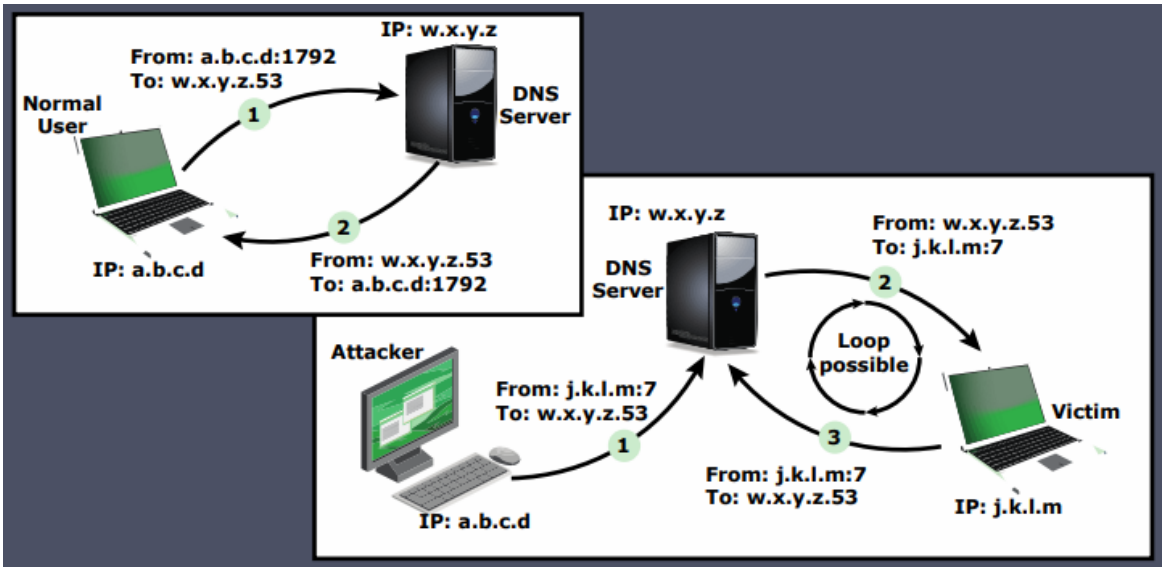



**Figure 7.5 SIP INVITE Scenario**

---

- Hypertext Transfer Protocol (HTTP) Based Attacks
  - HTTP Flood:
    - bombard the web server with http requests
    - spidering
      - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way
  - Slowloris
    - http requests that never complete
    - detect attacks will generally not recognize Slowloris

- Reflection Attack
  - attacker send packets to a known service on the intermediary (aracı) with a spoofed source address
  - reflects the attack off the intermediary (reflektör)
  - without alerting the intermediary
  - blocking spoofed-source packets

- 


- Amplification Attack
  - legitimate DNS Server as the intermediary system
  - exploit DNS behavior to convert a small request to a much larger response (amplification)
  - target is flooded with responses
  - defense
    - prevent the use of spoofed source addresses

- DoS Attack Defenses
  - cannot be prevent entirely
  - attack prevention and preemption (önce) → attack detection and filtering (sırasında) → attack source traceback and identification (sırasında ve sonrasında) → attack reaction (sonrasında)

- DoS Attack Prevention
  - Block spoofed source addresses → on routers as close to source as possible
  - filters may be used to ensure path back to the claimed source address
    - must be applied to traffic before it leaves the ISP or at the point of entry to their network
  - modified TCP connection hanfling code
    - encode critical information in a cookie
      - legal clients responds ACK
    - **drop** an entry for an **incomplete** connection from the TCP connections table when it overflows
  - block IP directed broadcasts
  - block suspicious services and combinations
  - captcha ile engelle
  - security açısından genel olarak iyi bir sistem geliştir??? sadece yap, LATTE!
  - use mirrored and replicated servers → high performance and reliability gerektiğinde

- Responding DoS Attacks
    - contact with ISP teknik elemanı
    - traffic filtering upstream empoze et
    - Antispoofing
    - directed broadcast
    - rate limiting filters
    - network monitors to detect anormal traffic patterns

    - identify the type of attack
    - Have ISP trace packet flow back to source → difficult and time consuming
    - contingency planning → alternate backup servers
    - hatadan ders al response planı güncelle

**UYGULAMA NOTLARI**

---

**SQL injection (LOW)**

- 1' and '0'='0' union select database(),version() # → **mysql versiyonu ve ubuntu bilgisi**
- 1' and '0'='0' union select null,table_name from information_schema.tables where table_schema = 'dvwa' # → **tablo isimlerini öğrenme**
- 1' and '0'='0' union select null,column_name from information_schema.columns where table_name = 'users' # → **istenilen tablonun kolon isimlerini öğrenme**
- 1' and '0' = '0' union select user_id, password from users # → **şifreleri elde etme**

**SQL injection (MEDIUM)**

- **Burp Suite:** bir tool, proxy sunucusu olarak kullanılabilir, **request interception** yapılabilir → combobox kullansa bile bu uygulama ile injection yapılabilir

**Şifre Kırma Yöntemleri**

- Brute Force
- Dictionary Attack
- Rainbow Tables → precomputed table

**Şifre Kırma Araçları**

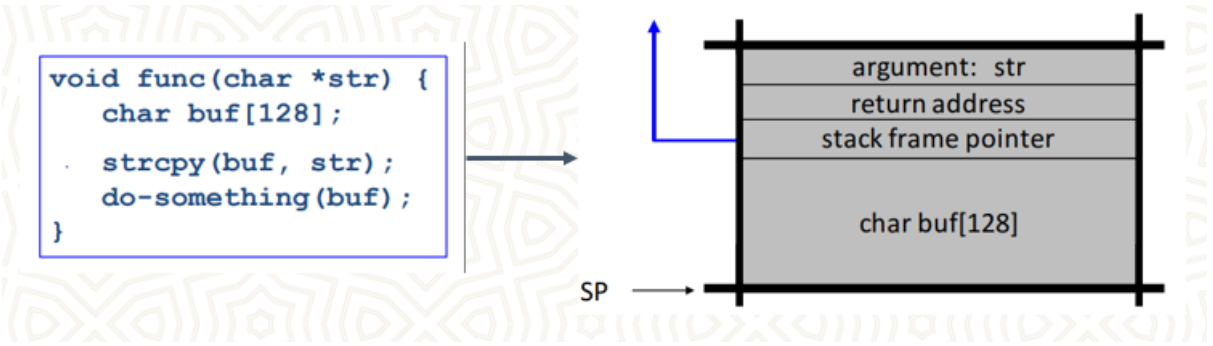
- John the Ripper (JtR) (Brute Force and Dictionary)
- HashCat
- Cain and Abel
- Hydra
- Rainbow Crack
- Brutus

- Medusa
- OphCrack
- sudo john hash.txt
  sudo john --show hash.txt

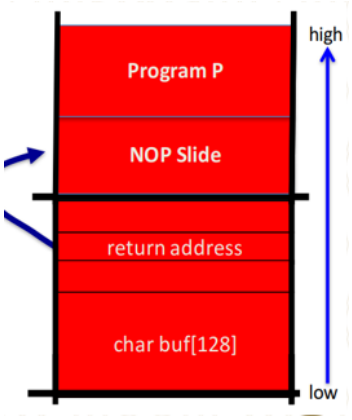
**Buffer Overflow Attack**

- **Buffer Overflow – attacks**
- Integer Overflow – attacks
- Format String – vulnerabilities

- C C++
- C fonksiyonları, heap ve stack memory bilgisi **gerekiyor**
- sistem çağrıları bilgisi ( exec() gibi)
- hangi işlemci ve hangi işletim sistemi olduğunu bilmesi
- little/big endian or unix/windows farkediyor



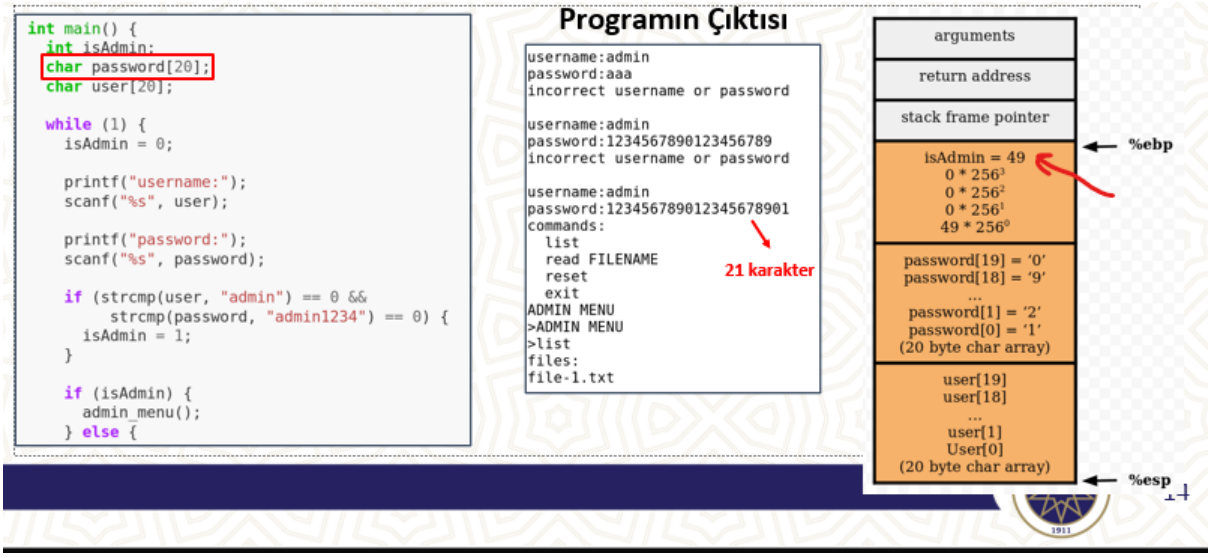

- strcpy **string uzunluğunu** kontrol etmez
- Stack açığından faydalanma
  - string boyutunu öyle bir ayarlıyoruz ki bizim yazdığımız programı gösteriyor artık
- Dönüş adresini nasıl buluruz → **NOP slide**

- **Yazdığımız Program** → (Hijack uygulaması, yani Shell komutunu çalıştıran uygulama), çalıştırılmadan önce çok sayıda NOP komutu girerek, dönüş adresini ezmek mümkün
  - 

- strcpy strcat gets scanf → açığı bulunan fonksiyonlar

**Buffer overflow ile fonksiyondaki değişkenlerin değerinin değiştirilmesi**

Değişkenin kapasitesini aşınca başka bir değişkenin değerini değiştirebiliyoruz



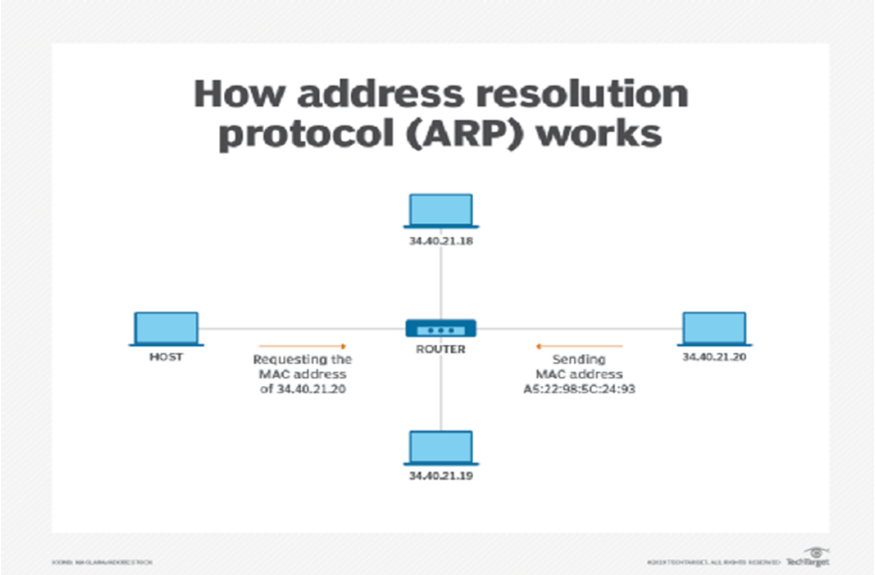

**Buffer overflow ile exec sistem çağrısını kullanarak shell çalıştırılması**

TAM ANLAMADIM BU KISMI
shell komutu çalıştırma

**Alınabilecek Önlemler**

- address space layout randomization
- non executable stack
- guard variable (canary)
- strcpy yerine strncpy
- gets yerine fgets
- guard pages

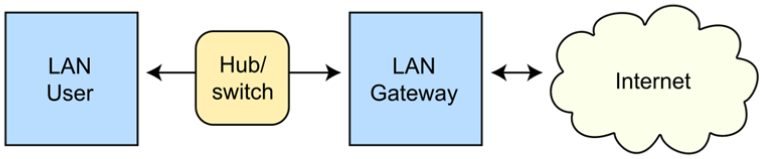
**ARP Poisoning**
**( Address Resolution Protocol (ARP) )**



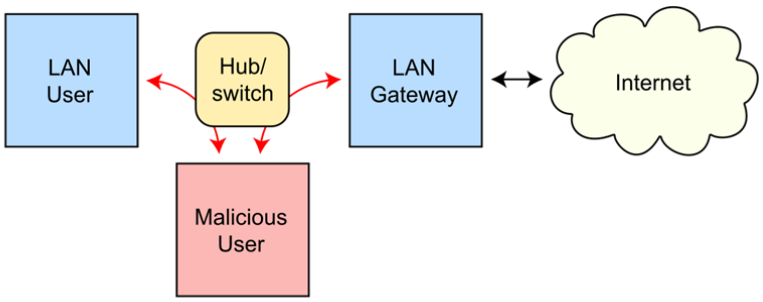

- ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa
- devices use ARP to contact the router or gateway that enables them to connect to the Internet
- network üzerindeki başka bir cihaza bağlanmak için router dan o cihazın MAC adresini istemek gibi işlerde kullanılır

- ARP ilk çıktığında güvenlik bu kadar önemli değildi
    - For example, if Computer A “asks” for the MAC address of Computer B, an attacker at Computer C can respond and Computer A would accept this response as authentic

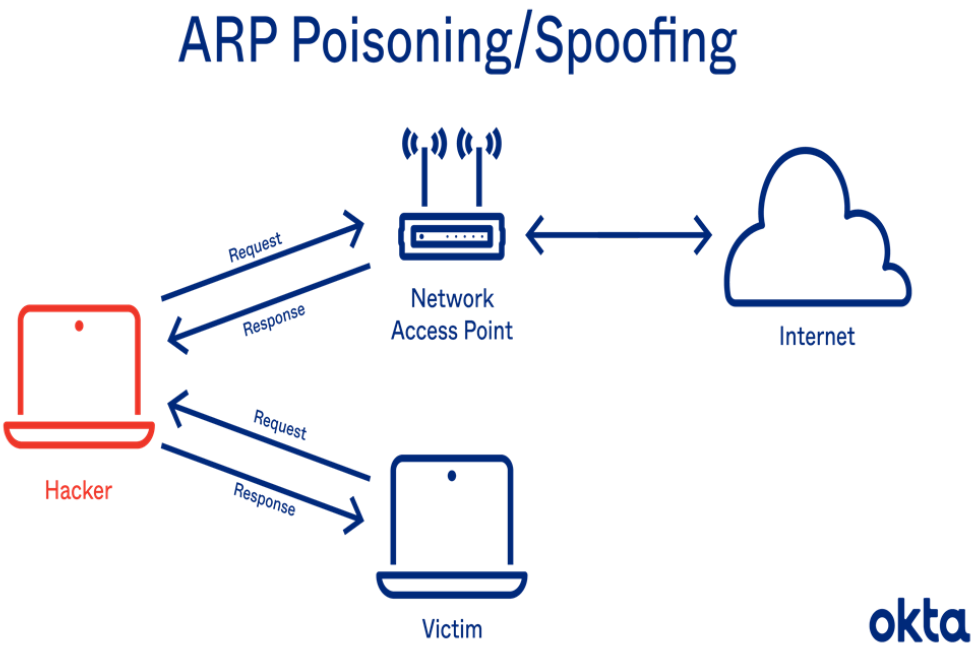
Routing under normal operation



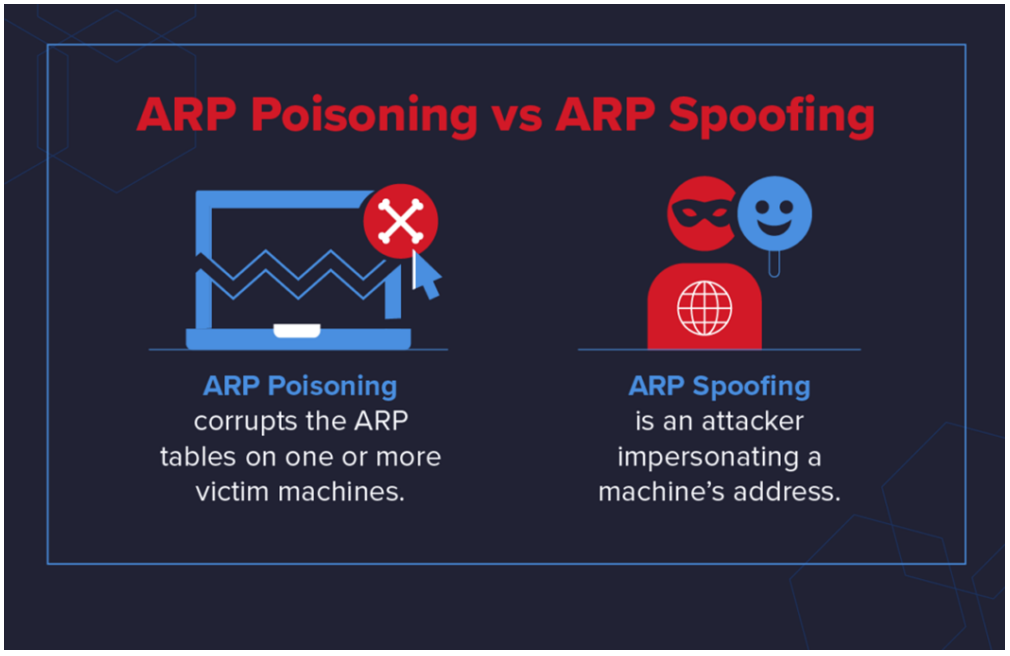

Routing subject to ARP cache poisoning

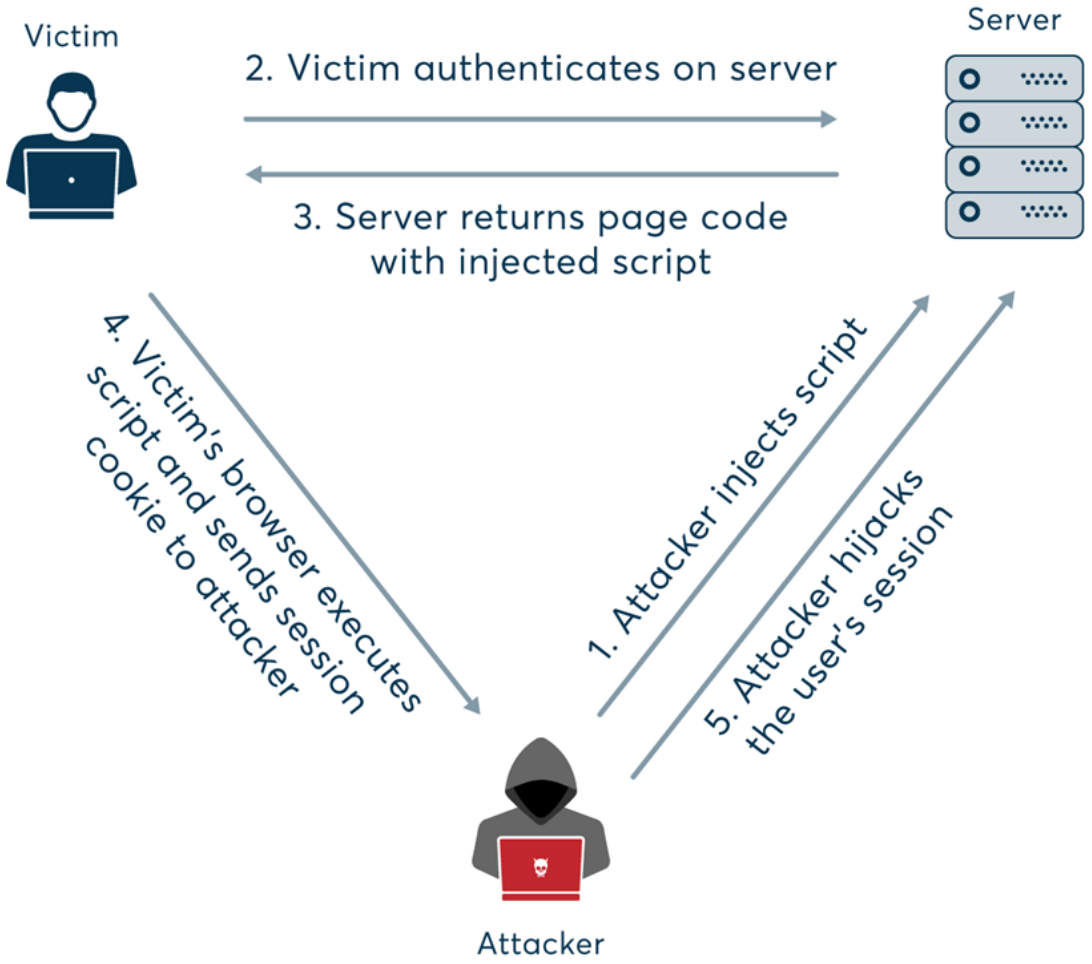



-




- 
    - bir kurban seçer
    - tool başlatır ve atak başlar
    - trafiği yanlış yönlendirecek bir şeyler yapar

- **ARP Poisoning & ARP Spoofing**
    - spoofing → başka bir makinenin kimliğine bürünme (MAC adresini taklit etme)
    - poisoning → corrupting the ARP Tables on victims
    - 




- spoofing yaparsa neler yapabilir:
    - continue routing
    - perform session hijacking
    - alter (değiştirmek) communication
    - DDoS

**ARP Poisoning olduğunu nasıl anlarız?**

- arp -a komutu ile tabloları kontrol edebiliriz (IP2MAC address mappings)
- arpwatch veya X-ARP gibi uygulamalar da kullanılabilir
    - arpwatch → sürekli kontrol eder ve değişiklik bilgisi ister adminden mail ile

**ARP Poisoning nasıl engellenir?**

- **static arp tables** → sürekli değiştirerek (admin kontrolü gerekir sürekli ve manuel elle değiştirmek gerekiyor)
    - büyük şirketlere uygun değil o yüzden
- **switch security** → çoğu switch Dynamic ARP Inspection (DAI) kullanır.
    - DoS ataklarını engellemek içi trafik kontrolü yapar
    - şüpheli paketleri iletmez vs.
    - büyük network yapılarında da kullanılır
    - diğer switch yapılarına bağlı olanlar hariç bütün portlara uygulanır genelde

    - bir şeyler daha yazıyor tam anlamadım
- **network isolation** → VPN Services
    - local subnet içinde ilerleyemez
    - herkes kendi subnet yapısını korursa engellenebilir diye anladım ben
- **encryption** → yine trafiği etkileyebilir hacker ama bir şey yapamaz çünkü encrypted
    - girmesini engellemez bir şeyler yapmasını engeller
- **Physical Security** → fiziksel erişimi takip edip kontrol etmek
    - fiziksel erişimi olmalı veya network dahilindeki bir cihazı ele geçirmiş olmalı
    - wired or wireless, the use of technology like **802.1x** can ensure that only **trusted** and/or **managed** devices can connect to the network.
- **run an ARP Poisoning attack** → tatbikat yap