Security of Computer Systems

Şafak Bilici

Contents

1 Key Security Concepts

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
Availability: Ensuring timely and reliable access to and use of information.

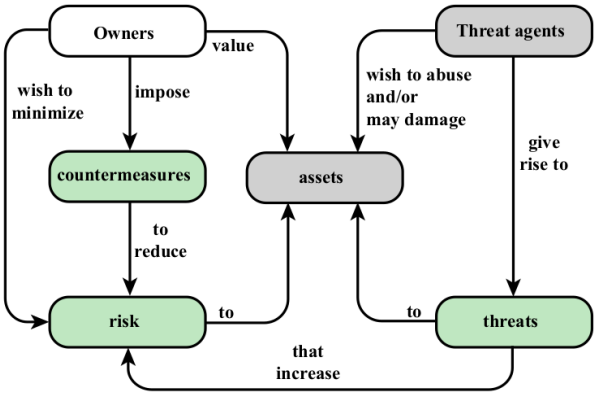
2 Levels of Impact

- **Low**: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate**: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- **High**: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

3 Computer Security Terminologies

- **Adversary**: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
- **Attack**: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **Countermeasure**: A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.
- **Risk**: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

- **Security Policy**: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.
- **System Resource**: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.
- **Threat**: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- **Vulnerability**: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.



4 Vulnerabilities, Threats and Attacks

Categories of vulnerabilities:

- Corrupted (loss of integrity)
- Leaky (loss of confidentiality)
- Unavailable or very slow (loss of availability)

Threats:

- Capable of exploiting vulnerabilities
- Represent potential security harm to an asset

Attacks (threats carried out)

- **Passive**: attempt to learn or make use of information from the system that does not affect system resources
  - Eavesdropping on, or monitoring of, transmissions
  - Goal of attacker is to obtain information that is being transmitted
  - Two types: Release of message contents, traffic analysis

- **Active**: attempt to alter system resources or affect their operation
  - Involve some modification of the data stream or the creation of a false stream
  - Four categories: Replay, Masquerade, Modification of messages, Denial of service.
- **Insider**: initiated by an entity inside the security parameter
- **Outsider**: initiated from outside the perimeter

5 Attack Surface Categories

5.1 Network Attack Surface

- Vulnerabilities over an enterprise network, wide-area network (WAN), or the Internet
- Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, isruption of communications links, and various forms of intruder attacks

5.2 Software Attack Surface

- Vulnerabilities in application, utility, or operating system code
- Particular focus is Web server software

5.3 Human Attack Surface

- Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

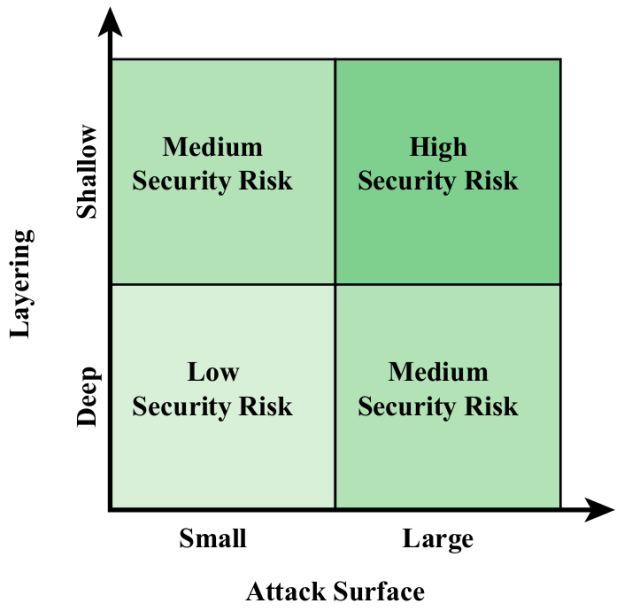


Figure 1: Defense in Depth and Attack Surface

6 Cryptographic Tools

6.1 Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption
- Two requirements:
  - Need a strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

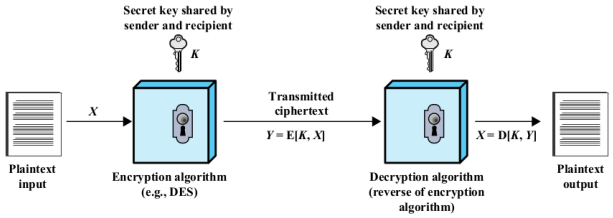


Figure 2: Simplified Model of Symmetric Encryption

6.2 Attacking Symmetric Encryption

6.2.1 Cryptanalytic Attacks

Rely on:

- Nature of the algorithm
- Some knowledge of the general characteristics of the plaintext
- Some sample plaintext- ciphertext pairs

Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used

- If successful, all future and past messages encrypted with that key are compromised

6.2.2 Brute-Force Attacks

Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained

- On average half of all possible keys must be tried to achieve success

7 Data Encryption Standard (DES)

- Until recently was the most widely used encryption scheme
  - FIPS PUB 46
  - Referred to as the Data Encryption Algorithm (DEA)
  - Uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block

- Strength concerns:
  - DES is the most studied encryption algorithm in existence
  - The speed of commercial off-the-shelf processors makes this key length woefully inadequate

8 Triple DES (3DES)

- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
  - 168-bit key length overcomes the vulnerability to brute-force attack of DES
  - Underlying encryption algorithm is the same as in DES
- Drawbacks:
  - Algorithm is sluggish in software
  - Uses a 64-bit block size

9 Advanced Encryption Standard (AES)

- Needed a replacement for 3DES. 3DES was not reasonable for long term use.
- NIST called for proposals for a new AES in 1997:
  - Should have a security strength equal to or better than 3DES
  - Significantly improved efficiency
  - Symmetric block cipher
  - 128 bit data and 128/192/256 bit keys

	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

Figure 3: Comparison of Three Popular Symmetric Encryption Algorithms

10 Practical Security Issues

- Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
- Modes of operation
  - Alternative techniques developed to increase the security of symmetric block encryption for large sequences
  - Overcomes the weaknesses of ECB

11 Block and Stream Ciphers

11.1 Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

11.2 Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

12 Message Authentication Without Confidentiality

- It is possible to combine authentication and confidentiality in a single algorithm by encrypting a message plus its authentication tag
- Typically message authentication is provided as a separate function from message encryption

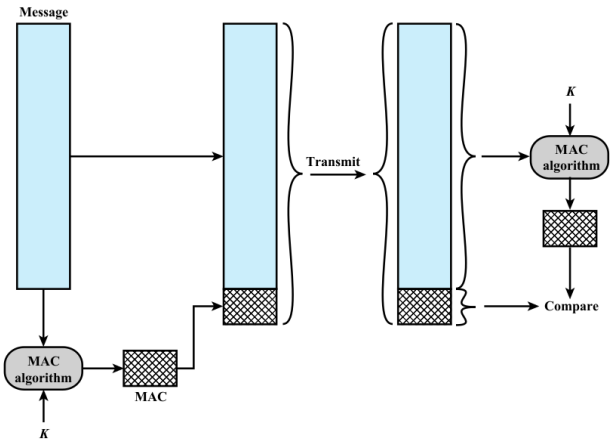


Figure 4: Message Authentication Using a Message Authentication Code (MAC)

13 Security of Hash Functions

- There are two approaches to attacking a secure hash function:
  - Cryptanalysis: Exploit logical weaknesses in the algorithm
  - Brute-force attack: Strength of hash function depends solely on the length of the hash code produced by the algorithm.

- SHA most widely used hash algorithm
- Additional secure hash function applications:
  - Passwords: Hash of a password is stored by an operating system
  - Intrusion detection: Store H(F) for each file on a system and secure the hash values

14 Public-Key Encryption Structure

- Based on mathematical functions.
- Asymetric:
  - Uses two separate keys
  - Public and private key
  - Public key is made public for others to use
- Some form of protocol is needed for distribution

15 Some Definitions

- Plaintext: Readable message or data that is fed into the algoritm as input
- Encryption algorithm: Performs transformations on the plaintext
- Public and Private Key: Pair of keys, one for encryption, one for decryption
- Ciphertext: Scrambled message produced as output
- Decryption key: Produces the original plainket

16 Asymmetric Encryption Algorithms

- **RSA**
  - Most widely accepted and implemented approach to public-key encryprion
  - Block cipher in which the plaintext and ciphertext are integers between 0 and $n-1$ for some n.
- **Diffie-Hellman Key Exchange Algorithm**:
  - Enables two users to securely reach aggrement about a shared secret that can be used as a secret key for subsequent symmetric encryption messages.
  - Limited to the exchange of the keys.
- **Digital Signature Standard (DSS)**
  - Provides only a digital signature function with SHA-1.
  - Cannot be used for encryption or key exchange.
- **Elliptic Curve Cryptography**
  - Security like RSA, but with much smaller keys.

16.1 Requirements

- Computationally easy to create key pairs.
- Useful if either key can be used for each role.
- Computationally infeasible for opponent to otherwise recover original message.
- Computationally infeasible for opponent to determine private key from public key.
- Computationally easy for receiver knowing private key to decrypt ciphertext.
- Computationally easy for sender knowing public key to encrypt messages.

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

Figure 5: Applications for Public-Key Cryptosystems

17 Digital Signatures

"The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."

- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block.

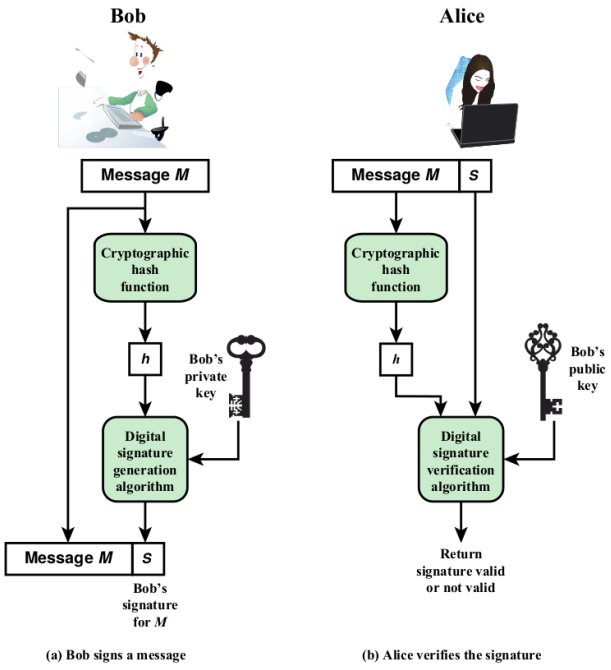


Figure 6: Simplified Depiction of Essential Elements of Digital Signature Process

18 Random Numbers

Uses include generation of:

- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Symmetric key for use as a temporary session key or in creating a digital envelope
- Handshaking to prevent replay attacks
- Session key

19 Authentication Process

- Fundamental building block and primary line of defense
- Basis for access control and user accountability
- Identification step
  - Presenting an identifier to the security system.
- Verification step
  - Presenting or generating authentication information that corroborates the binding between the entity and the identifier.

19.1 Basic Security Requirements

1. Identify information system users, processes acting on behalf of users, or devices.
2. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

19.2 Derived Security Requirements

1. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
2. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
3. Prevent reuse of identifiers for a defined period.
4. Disable identifiers after a defined period of inactivity.
5. Enforce a minimum password complexity and change of characters when new passwords are created.
6. Prohibit password reuse for a specified number of generations.
7. Allow temporary password use for system logons with an immediate change to a permanent password.
8. Store and transmit only cryptographically-protected passwords.

9. Obscure feedback of authentication information.

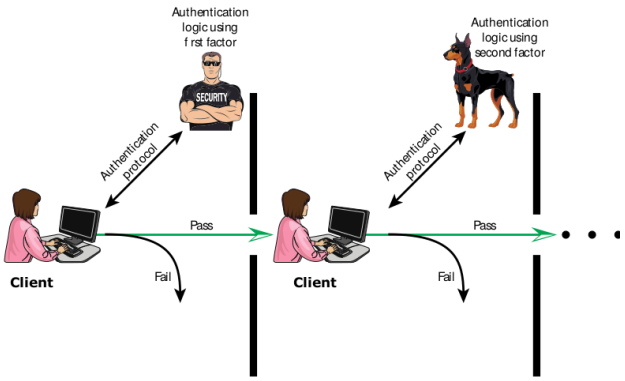


Figure 7: Multifactor Authentication

20 Risk Assessment for User Authentication

There are three separate concepts: Assurance Level - Potential Impact - Areas of Rist

20.1 Assurance Level

- Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity.
- More specifically is defined as:
  - The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued.
  - The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
- Four levels of assurance
  1. Litte or no confidence in the asserted identity's validty
  2. Some confidence in the asserted identity's validty.
  3. High confidence in the asserted identity's validty.
  4. Very hifg confidence in the asserted identity's validty.

20.2 Potential Impact

- Low: An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
- Moderate: An authentication error could be expected to have a serious adverse effect
- High: An authentication error could be expected to have a severe or catastrophic 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

Figure 8: Maximum Potential Impacts for Each Assurance Level

21 Password-Based Authentication

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID:
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control

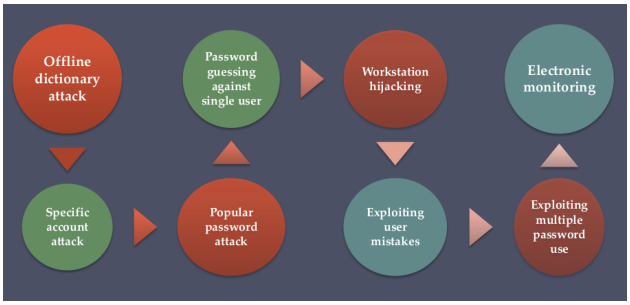


Figure 9: Password Vulnerabilities

22 Password Cracking

- Dictionary Attacks
  - Develop a large dictionary of possible passwords and try each against the password file
  - Each password must be hashed using each salt value and then compared to stored hash values
- Rainbow table attacks
  - Pre-compute tables of hash values for all salts
  - A mammoth table of hash values
  - Can be countered by using a sufficiently large salt value and a sufficiently large hash length.
- Password crackers exploit the fact that people choose easily guessable passwords
  - Shorter password lengths are also easier to crack

- John the Ripper
  - Uses a combination of brute-force and dictionary techniques

23 Modern Approaches

- Complex password policy
- However password-cracking techniques have also improved:
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
  - Studying examples and structures of actual passwords in use

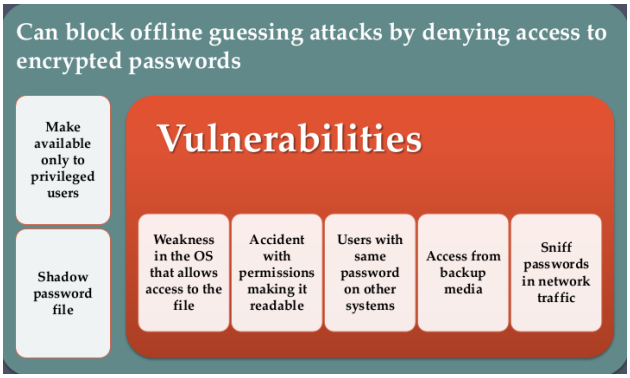


Figure 10: Password File Access Control

24 Proactive Password Checking

- Specific rules that passwords must adhere to
- Compile a large dictionary of passwords not to use
- Bloom filter:
  - Used to build a table based on hash values
  - Check desired password against this table

25 Cards Used as Tokens

25.1 Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room, ATM etc.

- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss of token
  - User dissatisfication

25.2 Smart Tokens

- Physical charactersitcs
  - Include an embed microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects
- User interface
  - Manual interfaces include a keypad and display for human/token interaction
- Electronic inferface
  - A smart card or other token requires an electronic inferface to communicate with a compatible reader/writer.
  - Contact and contactless interfaces
- Authentication protocol
  - classified into three categories: static, dynamic password generator, challenge-response

26 Smart Cards

- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
- Contains an entire microprocessor
- Typically include three types of memory: ROM (holds data does not change), EEPROM (holds application data), RAM (holds temp data).

27 Access Control Security

Basic Security Requirements:

1. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices
2. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements

1. Control the flow of CUI in accordance with approved authorizations.
2. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
3. Employ the principle of least privilege, including for specific security functions and privileged accounts.
4. Use non-privileged accounts or roles when accessing nonsecurity functions.
5. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
6. Limit unsuccessful logon attempts.
7. Provide privacy and security notices consistent with applicable CUI rules.
8. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
9. Terminate (automatically) a user session after a defined condition.
10. Monitor and control remote access sessions.
11. Route remote access via managed access control points.
12. Authorize wireless access prior to allowing such connections.
13. Protect wireless access using authentication and encryption.
14. Control connection of mobile devices.
15. Encrypt CUI on mobile devices.
16. Verify and control/limit connections to and use of external information systems.

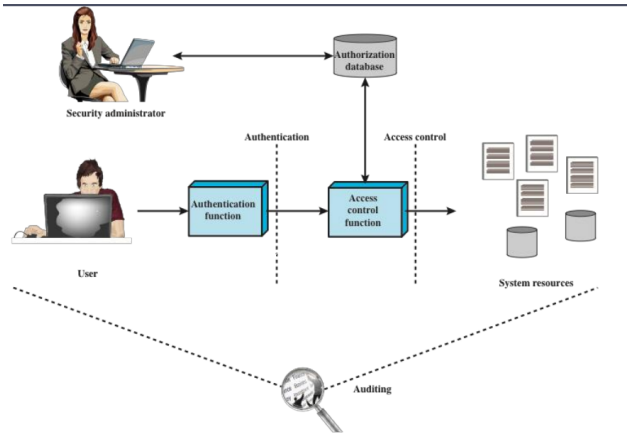


Figure 11: Relationship among access control and other security functions

28 Access Control Policies

28.1 Discretionary Access Control

- Controls access based on the identity of the requestor and on access rules (authorizations) stating what rquestors are (or are not) allowed to.
- This policy is termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource. (like google drive)

28.2 Mandatory Access Control (MAC)

- Controls access based on comparing security labels with security clearances
- This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource

28.3 Role-Based Access Control (RBAC)

- Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

28.3.1 Constraints of RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:
  - Mutually Exclusive Roles:
    - A user can only be assigned to one role in the set (either during a session or statically)
    - Any permission (access right) can be granted to only one role in the set.
  - Cardinality
    - Setting a maximum number with respect to roles.
  - Prerequisite roles
    - Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role.

28.4 Attribute-Based Access Control (ABAC)

- Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

28.5 Discretionary Access Control (DAC)

- Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource
- OFted provided using an access matrix

  - One dimension consists of identified subjects that may attempt data access to the resources
  - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

29 ABAC Model

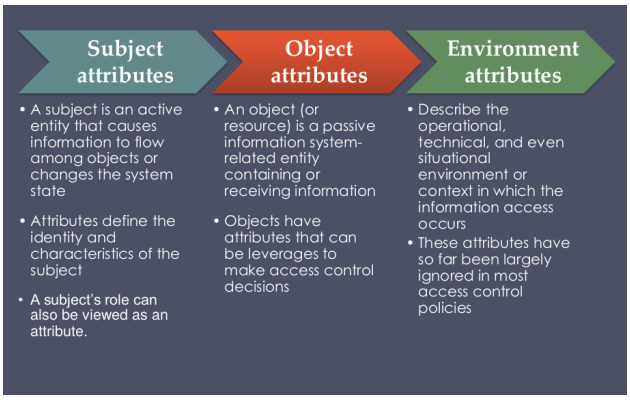


Figure 12: ABAC Attributes

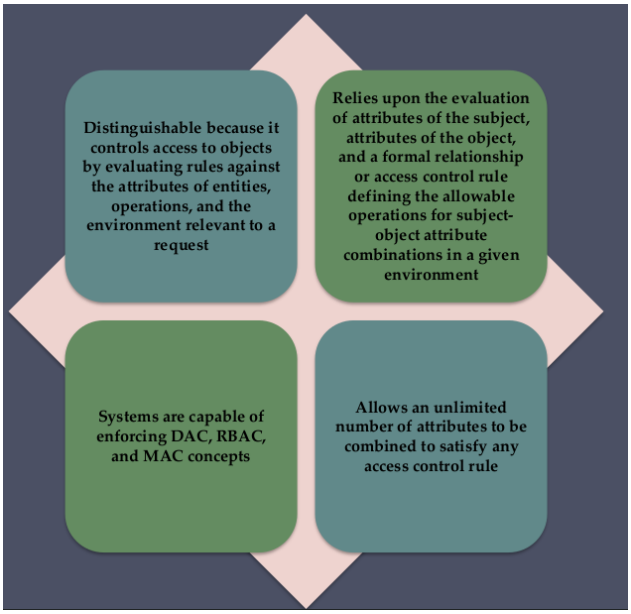


Figure 13: ABAC

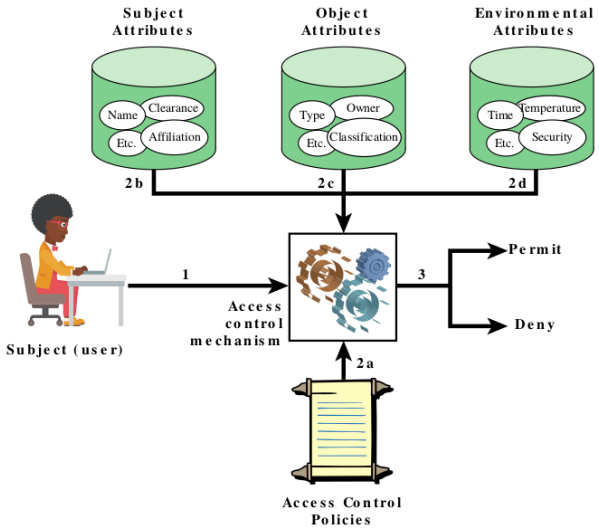


Figure 14: ABAC Scenario

30 Malware Terminology

Name	Description
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile Code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer Programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Malware Terminology

Figure 15: ABAC Attributes

31 Classification of Malware

Classified into two broad categories

- Based first on how it spreads or propagates to reach the desired targets
- Then on the actions or payloads it performs once a target is reached

Also classified by:

- Those that need a host program (parasitic code such as viruses)
- Those that are independent, self-contained programs (worms, trojans, and bots)
- Malware that does not replicate (trojans and spam e-mail)
- Malware that does replicate (viruses and worms)

32 Types of Malicious Software (Malware)

Propagation mechanisms include:

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

Payload actions performed by malware once it reaches a target system can include:

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealthing/hiding its presence on the system

33 Attack Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
  - The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware
- Toolkits are often known as "crimeware"
  - Include a variety of propagation mechanisms and payload modules that even novices can deploy
  - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Examples are: Zeus, Angler, Blackhole, Sakura, Phoenix.

34 Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- Techniques used:
  - Social engineering
  - Spear-phishing email
  - Drive-by-downloads from selected compromised websites likely to be visited by personnel in the target organization
- Aim:
  - Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure
- Intent:
  - To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
  - Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access

35 Viruses

- Piece of software that infects programs
  - Modifies them to include a copy of the virus
  - Replicates and goes on to infect other content
  - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
  - Executes secretly when the host program is run
- Specific to operating system and hardware. It takes advantage of their details and weaknesses.

36 Virus Components

- Inflection Mechanism:
  - Means by which a virus spreads or propagates
  - Also referred to as the infection vector
- Trigger:

  - Event or condition that determines when the payload is activated or delivered
  - Sometimes known as a logic bomb
- Payload:
  - What the virus does (besides spreading)
  - May involve damage or benign but noticeable activity

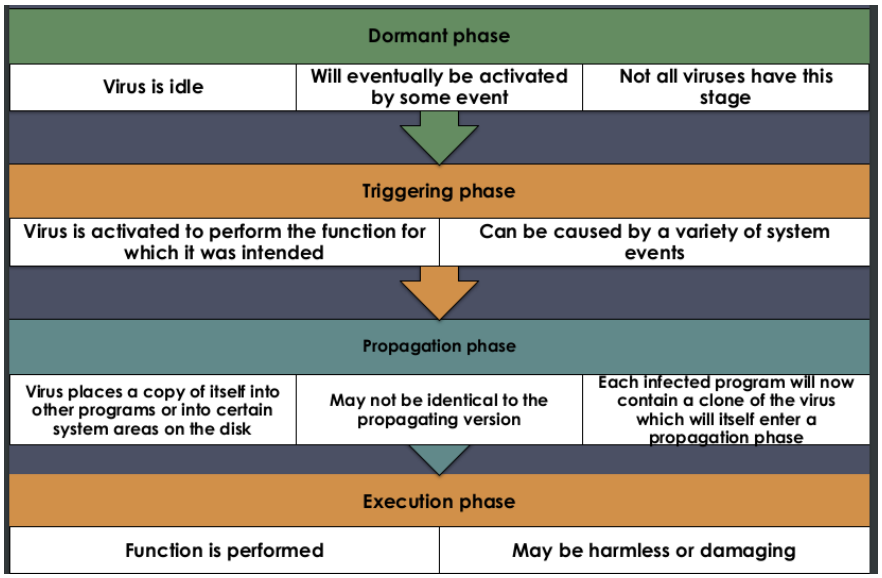


Figure 16: Virus Phases

37 Macro and Scripting Viruses

- a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate
- Macro viruses infect scripting code used to support active content in a variety of user document types
- Are threatening for a number of reasons:
  - Is platform independent
  - Infect documents, not executable portions of code
  - Are easily spread
  - Because they infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them
  - Are much easier to write or to modify than traditional executable viruses

38 Virus Classifications

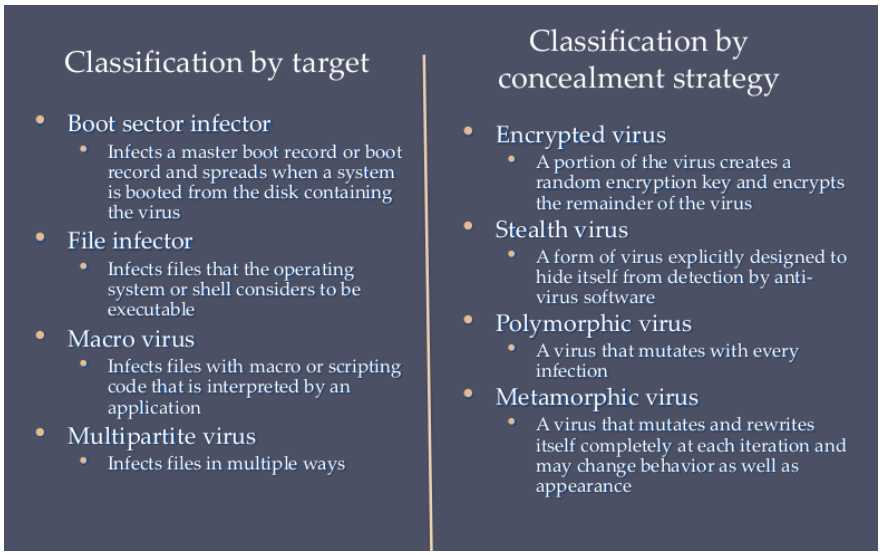


Figure 17: Virus Phases

39 Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation, the worm may replicate and propagate again
- Usually carries some form of payload
- Successful attacks achieved communication with the operating system command interpreter

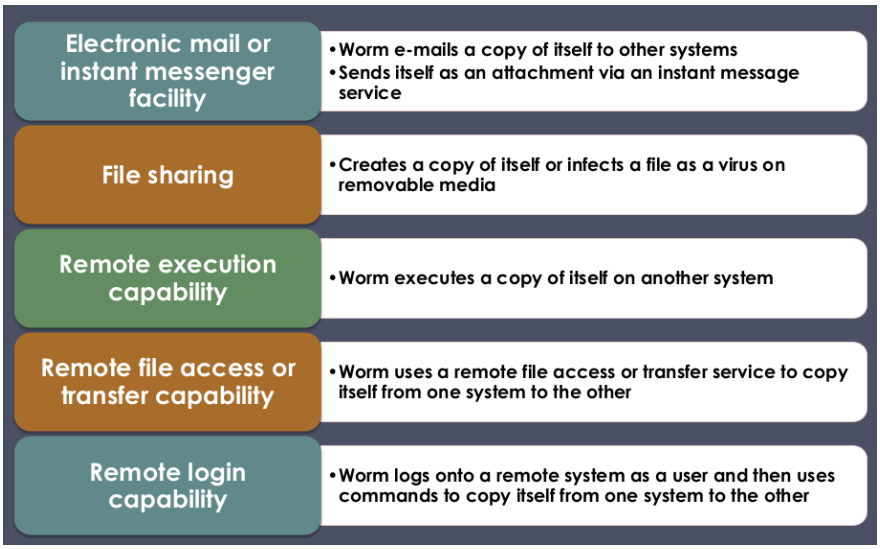


Figure 18: Worm Replication

40 Target Discovery

- Scanning (or fingerprinting)
  - First function in the propagation phase for a network worm
  - Searches for other systems to infect
- Random
  - Each compromised host probes random addresses in the IP address space using a different seed
  - This produces a high volume of Internet traffic which may cause generalized disruption even before the actual attack is lunched.
- Hit-list:
  - The attacker first compiles a long list of potential vulnerable machines
  - Once the list is compiled the attacker begins infecting machines on the list
  - Each infected machine is provided with a portion of the list to scan
  - This results in a very short scanning period which may make it difficult to detect that infection is taking place
- Topological
  - This method uses information contained on an infected victim machine to find more hosts to scan
- Local subnet
  - If a host can be infected behind a firewall that host then looks for targets in its own local network
  - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

41 Morris Worm

- Designed to spread on UNIX systems
  - Attempted to crack local password file to use login/password to logon to other systems
  - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
  - Exploited a trapdoor in the debug option of the remote process that receives and sends mail

42 Mobile Code

- Transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or Trojan horse
- Takes advantage of vulnerabilities to perform its own exploits
- Popular vehicles include
  - Java applets
  - ActiveX
  - JavaScript
  - VBScript
- Most common ways of using mobile code for malicious operations on local system are:
  - Cross-site scripting
  - Interacting and dynamic websites
  - e-mail attachments
  - Downloads from untrusted sites or of untrusted software

43 Mobile Phone Worms

- Communicate through Bluetooth wireless connections or MMS
- Target is the smartphone
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- 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

44 Drive-By-Downloads

- Exploits browser and plugin vulnerabilities so when the user views a webpage controlled by the attacker, it contains code that exploits the bug to download and install malware on the system without the user's knowledge or consent
- In most cases the malware does not actively propagate as a worm does
- Spreads when users visit the malicious Web page

45 Watering-Hole Attacks

- A variant of drive-by-download used in highly targeted attacks
- The attacker researches their intended victims to identify websites they are likely to visit, then scans these sites to identify those with vulnerabilities that allow their compromise
- They then wait for one of their intended victims to visit one of the compromised sites
- Attack code may even be written so that it will only infect systems belonging to the target organization and take no action for other visitors to the site
- This greatly increases the likelihood of the site compromise remaining undetected

46 Malvertising

- Places malware on websites without actually compromising them
- The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them
- Using these malicious ads, attackers can infect visitors to sites displaying them
- The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems
- Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track
- Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

47 Clickjacking

- Also known as a user-interface (UI) redress attack
- Using a similar technique, keystrokes can also be hijacked
  - A user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the hacker.
- Vulnerability used by an attacker to collect an infected user's clikcs
  - The attacker can force the user to do a variety of things from adjusting the user's computer settings to unwittingly sending the user to websites that might have malicious code.
  - By taking advantage of Adobe Flash or JavaScript an attacker could even place a button under or over a legitimate button making it difficult for users to detect
  - A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page
  - The attacker is hijacking clicks meant for one page and routing them to another page

48 Social Engineering

"Tricking" users to assist in the compromise of their own systems

- Spam
  - Significant carrier of malware
  - Used for pishing attacks
- Trojan Horse:
  - Program or utility containig harmful hidden code
  - Used to accomplish functions that the attacker could not accomplish directly
- Mobile Phone Trojans

49 Ransomware

- When installed on infected systems, it encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
- Recovery of this information was generally only possible if the organization had good backups and an appropriate incident response and disaster recovery plan

50 Payload System Corruption

- Real-world damage
  - Causes damage to physical equipment: Chernobyl virus rewrites BIOS code
  - Stuxnet worm: Targets specific industrial control system software
  - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
  - Code embedded in the malware that is set to "explode" when certain conditions are met

51 Payload – Attack Agents Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- Botnet - collection of bots capable of acting in a coordinated manner
- Uses
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games

52 Remote Control Facility

- Distinguishes a bot from a worm
  - Worm propagates itself and activates itself
  - Bot is initially controlled from some central facility
- Typical means of implementing the remote control facility is on an IRC server
  - Bots join a specific channel on this server and treat incoming messages as commands
  - More recent botnets use covert communication channels via protocols such as HTTP
  - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

53 Payload – Information Theft Keyloggers and Spyware

53.1 Keylogger

- Captures keystrokes to allow attacker to monitor sensitive information
- Typically uses some form of filtering mechanism that only returns information close to keywords ("login", "password")

53.2 Spyware

- Subverts the compromised machine to allow monitoring of a wide range of activity on the system
- Monitoring history and content of browsing activity
- Redirecting certain Web page requests to fake sites
- Dynamically modifying data exchanged between the browser and certain Web sites of interest

54 Payload – Information Theft Phishing

- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source (clickjacking)
  - Include a URL in a spam e mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
  - Suggests that urgent action is required by the user to authenticate their account
  - Attacker exploits the account using the captured credentials

55 Payload – Stealthing Backdoor

- Also known as a trapdoor
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- Maintenance hook is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

56 Payload - Stealthing Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker

57 Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention
  - Policy
  - Awareness
  - Vulnerability mitigation
  - Threat mitigation
- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
  - Detection, Identification, Removal

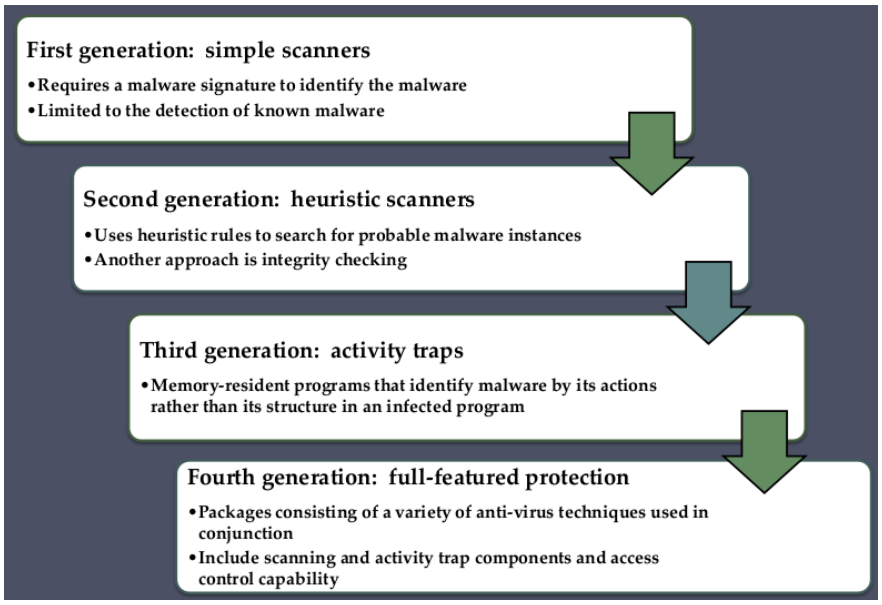


Figure 19: Generations of Anti-Virus Software

58 Sandbox Analysis

- Running potentially malicious code in an emulated sandbox or on a virtual machine
- Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system
- Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware

- The most difficult design issue with sandbox analysis is to determine how long to run each interpretation

59 Host-Based Behavior-Blocking Software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
  - Blocks potentially malicious actions before they have a chance to affect the system
  - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics
  - Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

60 Denial-of-Service (DoS) Attack

An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:
  - Network Bandwidth:
    - Relates to the capacity of the network links connecting a server to the Internet
    - For most organizations this is their connection to their Internet Service Provider (ISP)
  - System resources
    - Aims to overload or crash the network handling software
  - Application Resources
    - Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

61 Classic DoS Attacks

- Flooding ping command
  - Aim of this attack is to overwhelm the capacity of the network connection to the target organization
  - Traffic can be handled by higher capacity links on the path, but packets are discarded as capacity decreases
  - Source of the attack is clearly identified unless a spoofed address is used
  - Network performance is noticeably affected

62 Source Address Spoofing

- Use forged source addresses
  - Usually via the raw socket interface on operating systems
  - Makes attacking systems harder to identify
- Attacker generates large volumes of packets that have the target system as the destination address
- Congestion would result in the router connected to the final, lower capacity link
- Requires network engineers to specifically query flow information from their routers

63 SYN Spoofing

- Common DoS attack
- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
- Thus legitimate users are denied access to the server
- Hence an attack on system resources, specifically the network handling code in the operating system

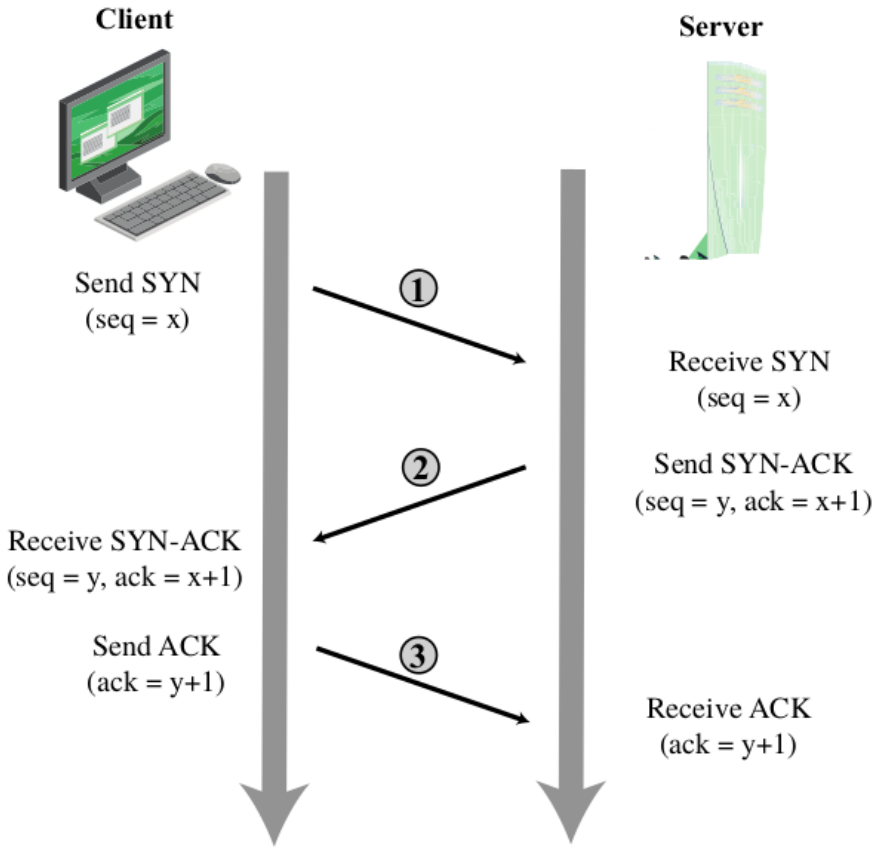


Figure 20: TCP Three-Way Connection Handshake

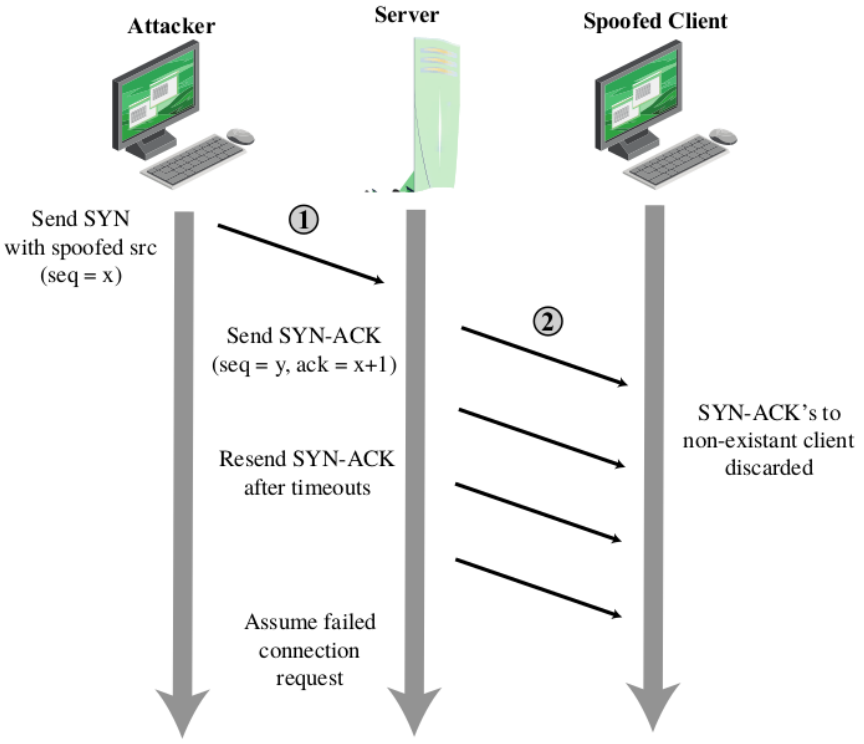


Figure 21: TCP SYN Spoofing Attack

64 Flooding Attacks

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used
  - ICMP Flood
    - Ping flood using ICMP echo request packets
    - Traditionally network administrators allow such packets into their networks because ping is a useful network diagnostic tool
  - UDP Flood
    - Uses UDP packets directed to some port number on the target system
  - TCP SYN Flood
    - Sends TCP packets to the target system
    - Total volume of packets is the aim of the attack rather than the system code

65 Distributed Denial of Service (DDoS) Attacks

- Use of multiple systems to generate attacks
- Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

- Large collections of such systems under the control of one attacker's control can be created, forming a botnet

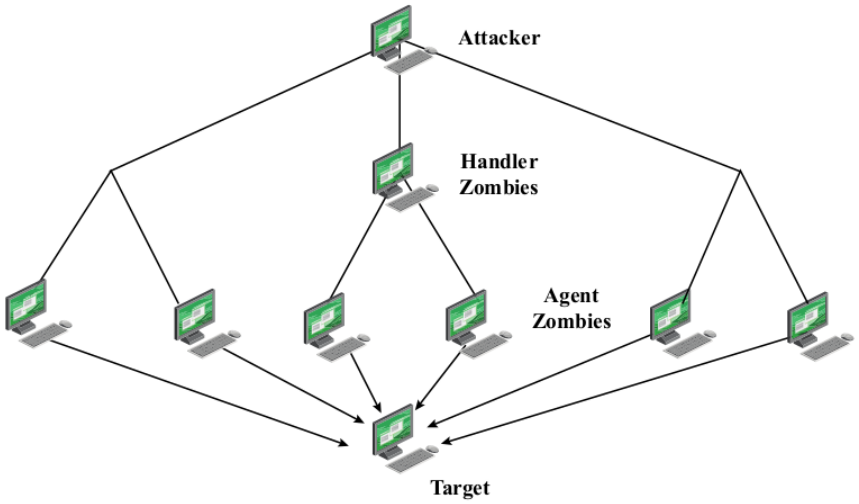


Figure 22: DDoS Attack Architecture

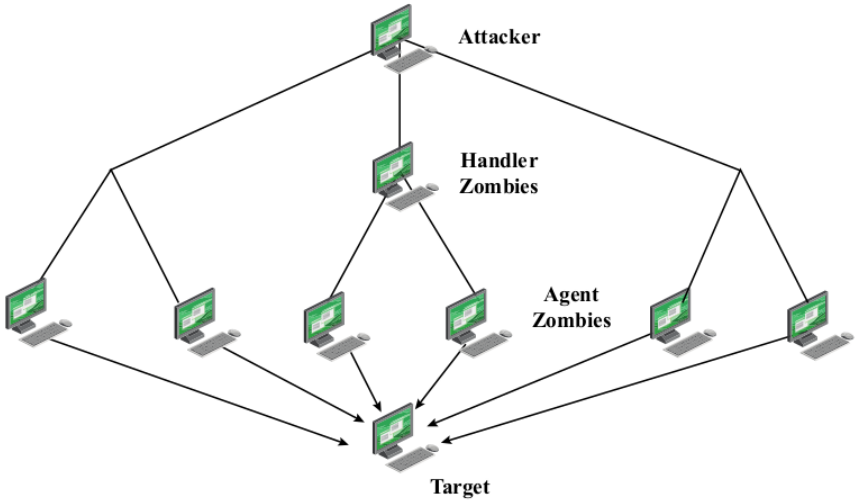


Figure 23: SIP INVITE Scenario

66 Hypertext Transfer Protocol (HTTP) Based Attacks

66.1 HTTP Flood

- Attack that bombards Web servers with HTTP requests
- Consumes considerable resources
- Spidering
  - Bots starting from a given HTTP link and following all links on the provided website in a recursive way.

66.2 Slowloris

- Attempts to monopolize by sending HTTP requests that never complete
- Eventually consumes Web server's connection capacity
- Utilizes legitimate HTTP traffic
- Existing intrusion detection and prevention solutions that rely on signatures to detect attacks will generally not recognize Slowloris

67 Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- "Reflects" the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- The basic defense against these attacks is blocking spoofed-source packets

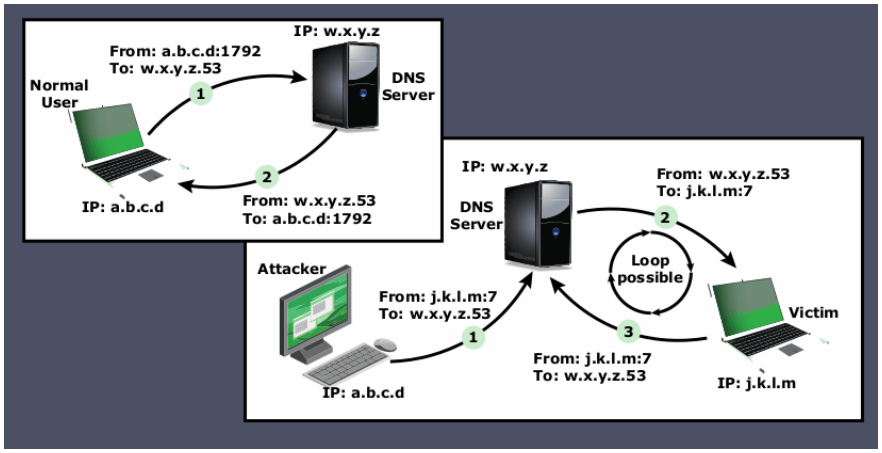


Figure 24: DNS Reflection Attack

68 DNS Amplification Attacks

- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source addresses

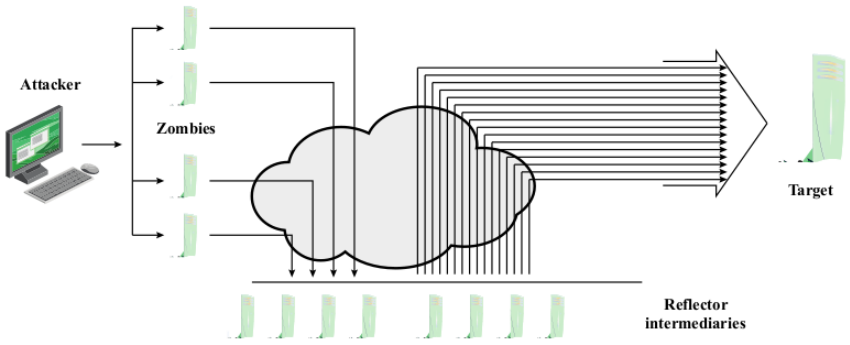


Figure 25: Amplification Attack

69 DoS Attack Defenses

- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
  - High publicity about a specific site
  - Activity on a very popular site
  - Described as slashdotted, flash crowd, or flash event

Four lines of defense against DDoS attacks:

- Attack prevention and preemption (before attack)
- Attack detection and filtering (during the attack)
- Attack source traceback and identification (during and after the attack)
- Attack reaction (after the attack)

70 DoS Attack Defenses 2

- Block spoofed source addresses
- Filters may be used to ensure path back to the claimed source address is the one being used by the current packet
- Use modified TCP connection handling code
  - Cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
  - Drop an entry for an incomplete connection from the TCP connections table when it overflows
- Block IP directed broadcasts
- Block suspicious services and combinations

- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

71 Responding to DoS Attacks

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns
- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if planning legal action
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan
  - Analyze the attack and the response for future handling