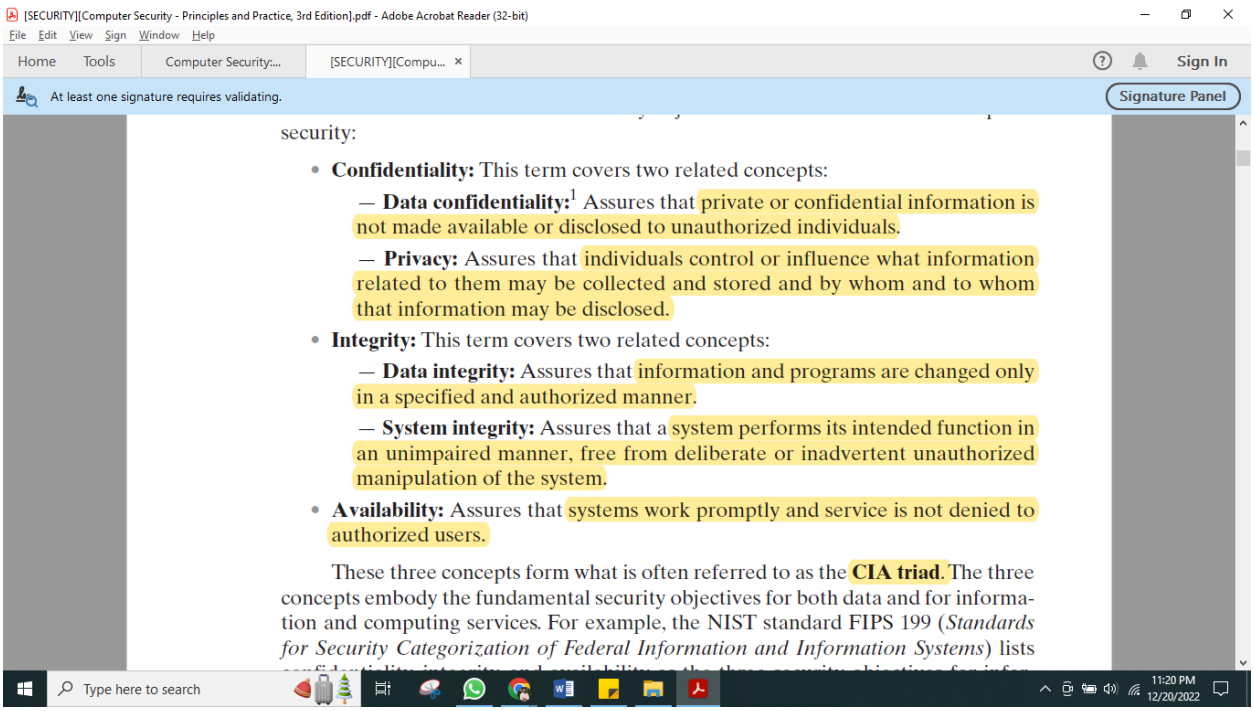
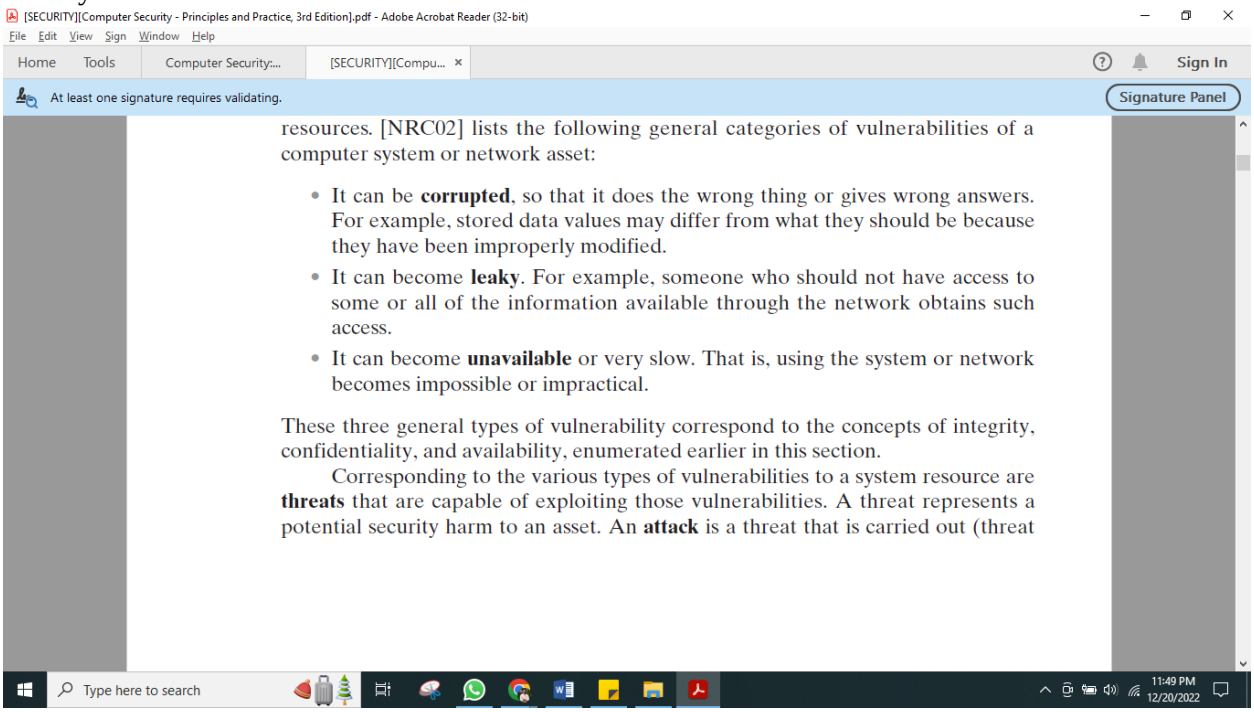
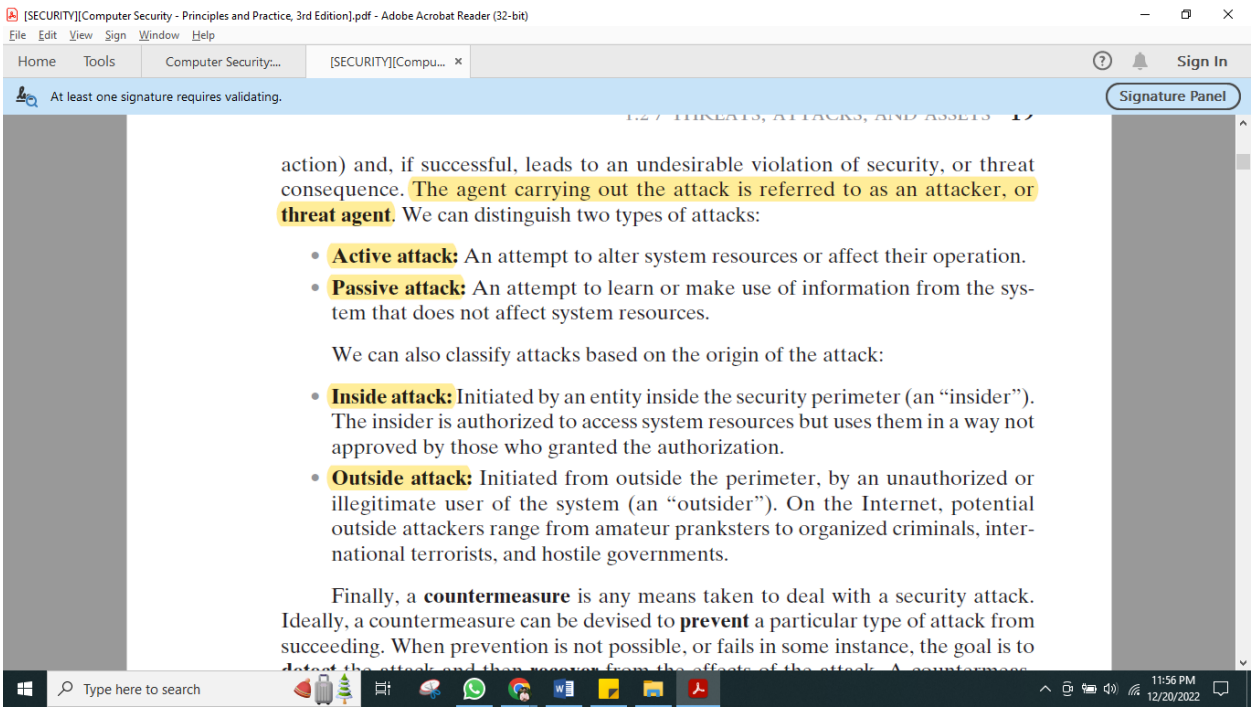


Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission





Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.

Table 1.3 **Computer and Network Assets, with Examples of Threats**

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

detection.

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

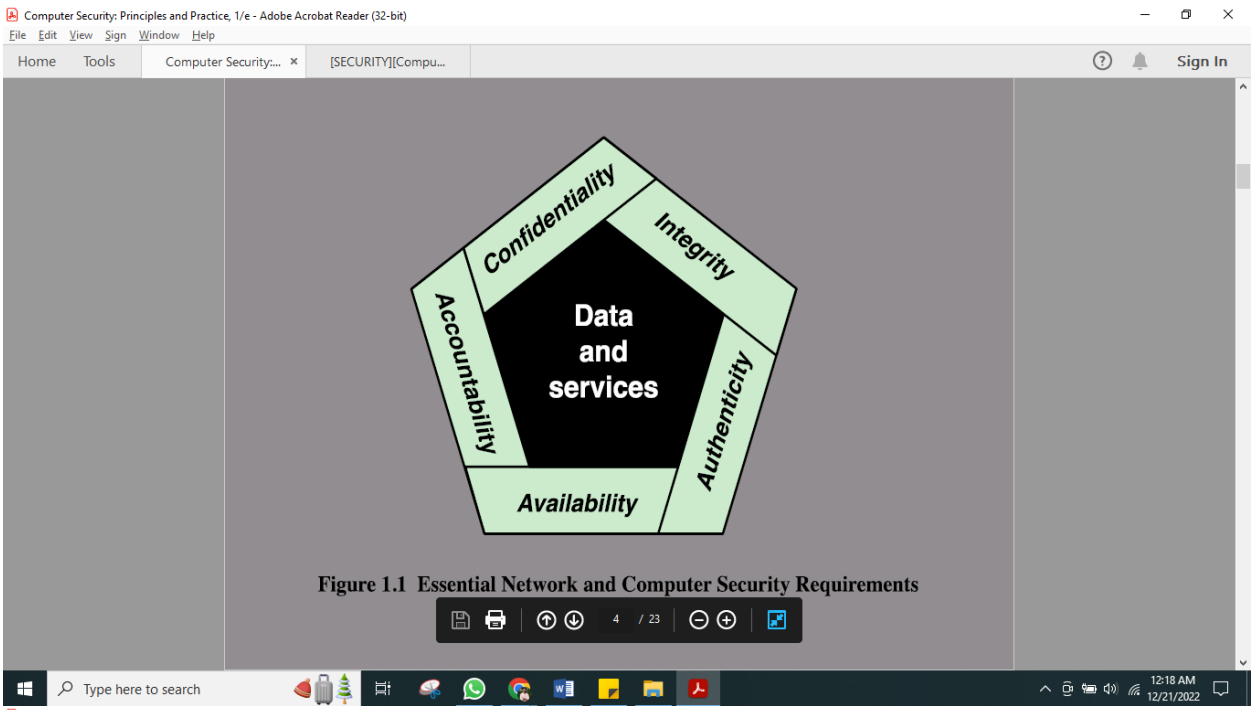
Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message stating, "Allow John Smith to read confidential file accounts" is modified to say, "Allow Fred Brown to read confidential file accounts."

The **denial of service** prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network,

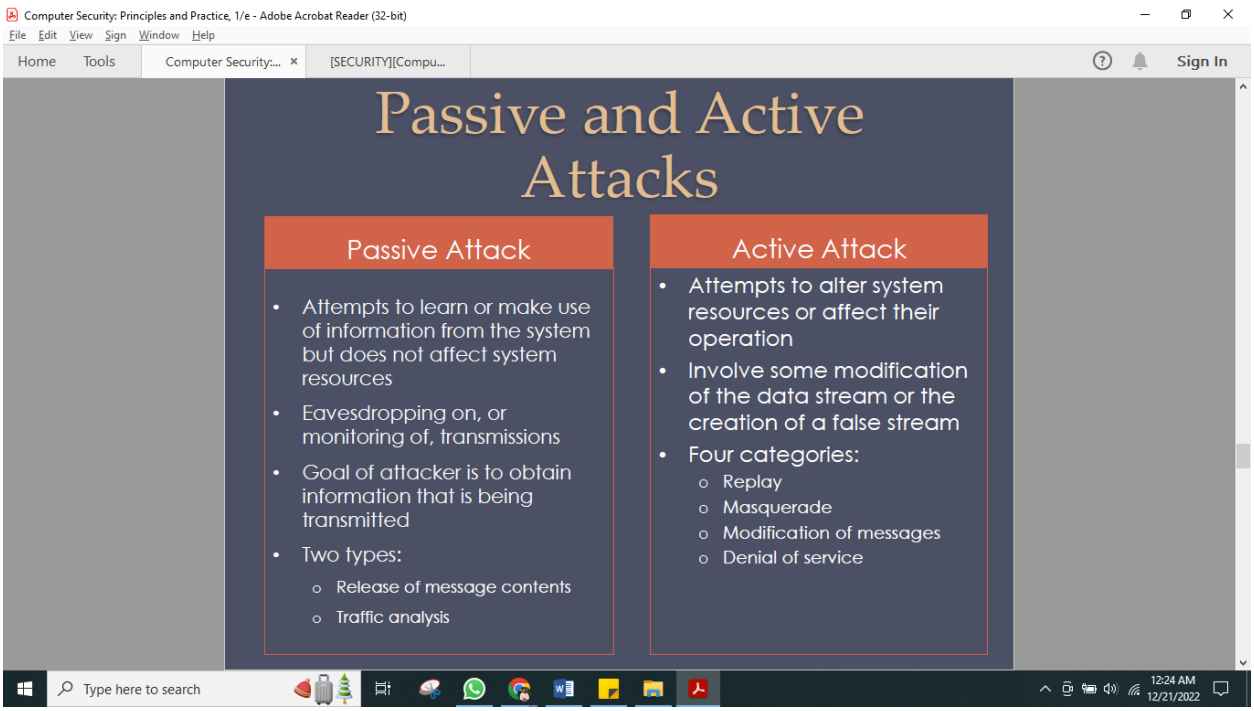
Security Implementation:
Prevention, Detection, Response, Recovery

assurance as the degree of confidence one has that the security measures,

Evaluation is the process of examining a computer product or system with respect to certain criteria. Evaluation involves testing and may also involve formal analytic or mathematical techniques


Computer Security: Principles and Practice, 1/e - Adobe Acrobat Reader (32-bit)
File Edit View Sign Window Help
Home Tools Computer Security:... [SECURITY][Compu... Sign In
Confidentiality
Integrity
Accountability
Data and services
Authenticity
Availability
Figure 1.1 Essential Network and Computer Security Requirements
4 / 23
Type here to search
12:18 AM
12/21/2022


Computer Security: Principles and Practice, 1/e - Adobe Acrobat Reader (32-bit)
File Edit View Sign Window Help
Home Tools Computer Security:... [SECURITY][Compu... Sign In
Fundamental Security Design Principles
Economy of mechanism
Fail-safe defaults
Complete mediation
Open design
Separation of privilege
Least privilege
Least common mechanism
Psychological acceptability
Isolation
Encapsulation
Modularity
Layering
Least astonishment
Type here to search
12:24 AM
12/21/2022



Symmetric key encryption uses one key
Asymmetric key encryption uses two keys

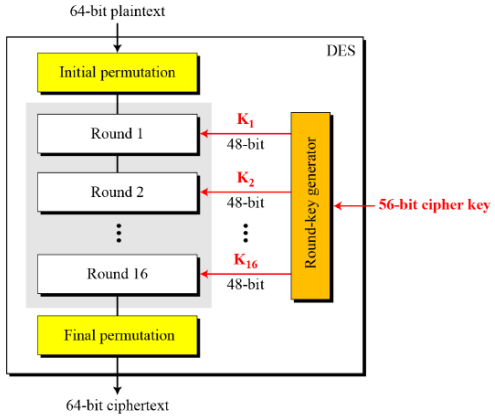
PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... × Sign In

6-2 Continue

Figure 6.2 *General structure of DES*



6.7

Type here to search 2:16 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

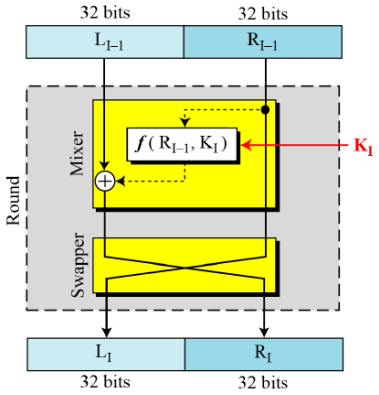
File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... × Sign In

6.2.2 Rounds

DES uses 16 rounds. Each round of DES is a Feistel cipher.

Figure 6.4
A round in DES (encryption site)



6.13

Type here to search 2:25 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... Sign In

6.2.2 Continued

DES Function

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

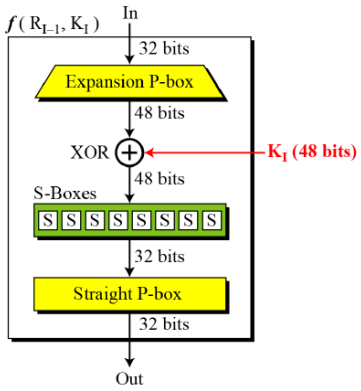


Figure 6.5
DES function

6.14

Type here to search 2:27 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

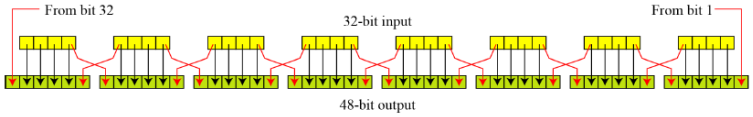
Home Tools [SECURITY][Compu... PowerPoint Present... Sign In

6.2.2 Continue

Expansion P-box

Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits.

Figure 6.6 *Expansion permutation*



6.15

Type here to search 2:29 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... Sign In

6.2.3 Continued

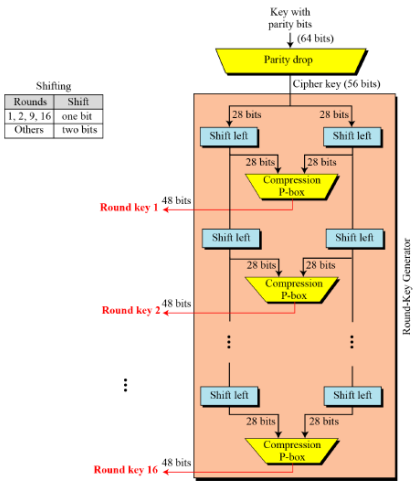


Figure 6.10
Key generation

6.31

Type here to search 2:34 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... Sign In

6.3.1 Properties

Two desired properties of a block cipher are the avalanche effect and the completeness.

Example 6.7

To check the avalanche effect in DES, let us encrypt two plaintext blocks (with the same key) that differ only in one bit and observe the differences in the number of bits in each round.

Plaintext: 0000000000000000 Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1

Plaintext: 0000000000000001 Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3

6.40

Type here to search 2:45 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... Sign In

6.3.1 Continued

Completeness effect

Completeness effect means that each bit of the ciphertext needs to depend on many bits on the plaintext.

6.42

Type here to search 2:45 AM 12/21/2022

PowerPoint Presentation - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... PowerPoint Present... Sign In

6.3.2 Design Criteria

S-Boxe

The design provides confusion and diffusion of bits from each round to the next.

P-Boxes

They provide diffusion of bits.

Number of Rounds

DES uses sixteen rounds of Feistel ciphers. the ciphertext is thoroughly a random function of plaintext and ciphertext.

6.43

Type here to search 2:45 AM 12/21/2022

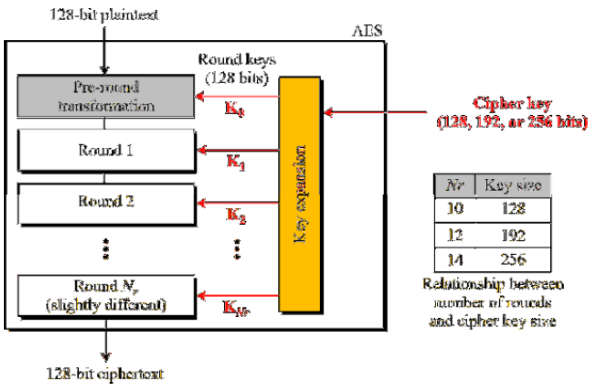
AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

7.1.3 Continue

Figure 7.1 *General design of AES encryption cipher*



N_r	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

7.7

Type here to search 3:05 AM 12/21/2022

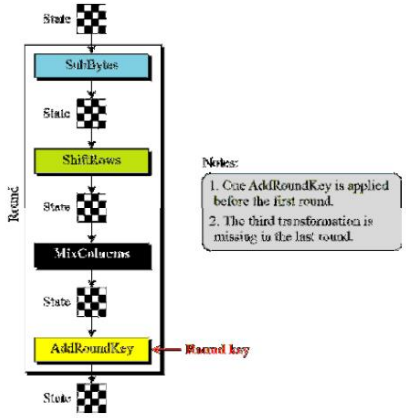
AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

7.1.5 Structure of Each Round

Figure 7.5 *Structure of each round at the encryption site*



7.11

Type here to search 3:07 AM 12/21/2022

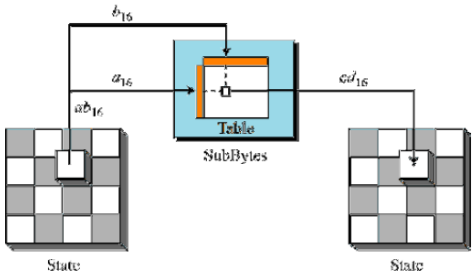
AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

7.2.1 Continue

Figure 7.6 *SubBytes transformation*



7.14

Type here to search 3:10 AM 12/21/2022

AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

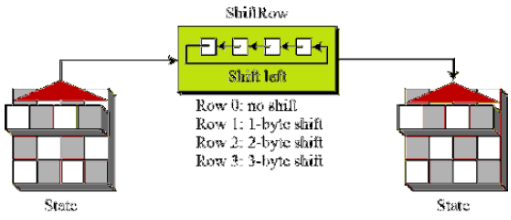
7.2.2 Permutation

Another transformation found in a round is shifting, which permutes the bytes.

ShiftRows

In the encryption, the transformation is called ShiftRows.

Figure 7.9 *ShiftRows transformation*



7.24

Type here to search 3:11 AM 12/21/2022

7.2.2 Continue

InvShiftRows

In the decryption, the transformation is called InvShiftRows and the shifting is to the right.

Algorithm 7.2 *Pseudocode for ShiftRows transformation*

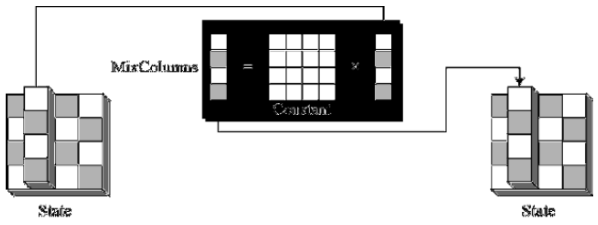
```
ShiftRows (S)
{
    for (r = 1 to 3)
        shiftrow (s_r, r)                    // s_r is the rth row
}
shiftrow (row, n)                            // n is the number of bytes to be shifted
{
   CopyRow (row, t)                          // t is a temporary row
   for (c = 0 to 3)
        row_((c – n) mod 4) ← t_c
}
```


7.2.3 Continue

MixColumns

The MixColumns transformation operates at the column level; it transforms each column of the state to a new column.

Figure 7.13 *MixColumns transformation*



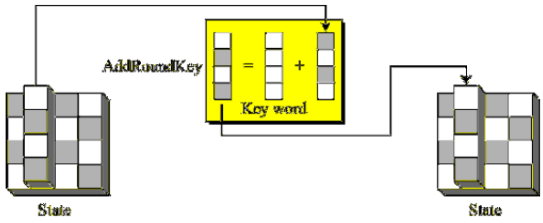
AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

7.2.4 Continue

Figure 7.15 *AddRoundKey transformation*



Algorithm 7.4 *Pseudocode for AddRoundKey transformation*

```
AddRoundKey (S)
{
    for (c = 0 to 3)
        s_c ← s_c ⊕ w_round + 4c
}
```

7.34

Type here to search 3:12 AM 12/21/2022

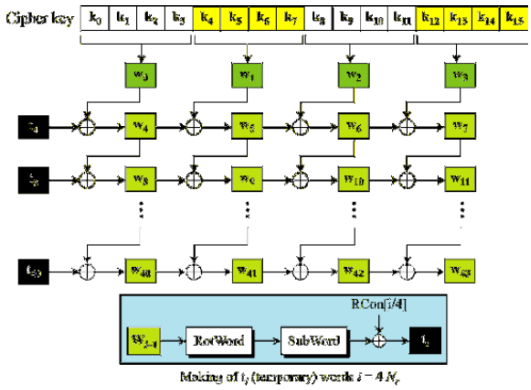
AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

7.3.1 Key Expansion in AES-128

Figure 7.16 *Key expansion in AES*



Making of t_i (temporary) words $i = 4 N_r$

7.37

Type here to search 3:14 AM 12/21/2022

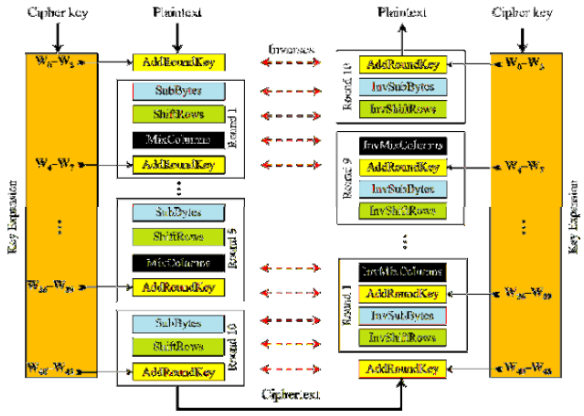
AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... AES.pdf Sign In

7.4.1 Original Design

Figure 7.17 *Ciphers and inverse ciphers of the original design*



7.48

Type here to search 3:15 AM 12/21/2022

AES.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

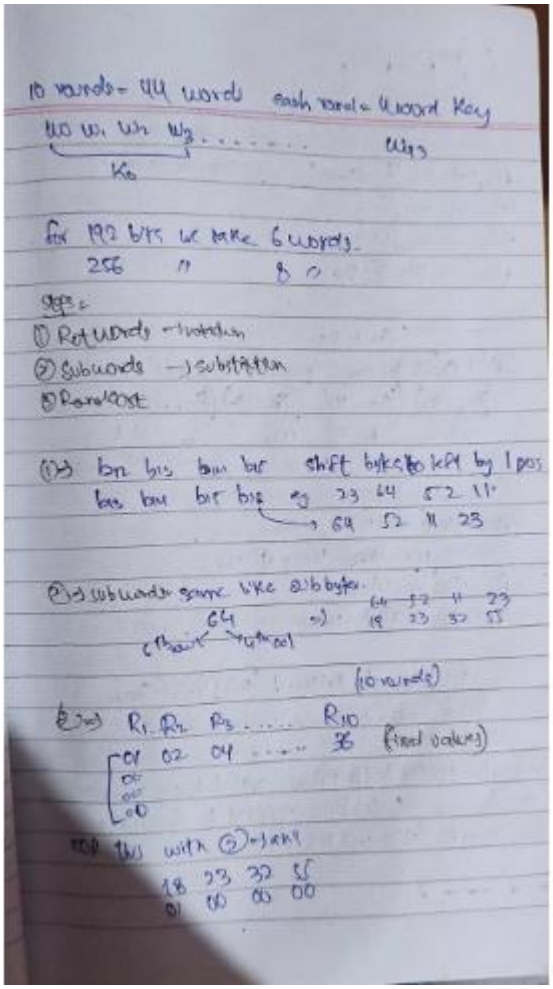
Home Tools [SECURITY][Compu... AES.pdf Sign In

7.6.2 Implementation

AES can be implemented in software, hardware, and firmware. The implementation can use table lookup process or routines that use a well-defined algebraic structure.

7.65

Type here to search 3:17 AM 12/21/2022


10 words = 44 words each word = 4 word Key

W0 W1 W2 W3 ..... W43

K0

for 192 bits we take 6 words.

256 " 8 "

Steps:

① RotWords → rotation

② SubWords → substitution

③ RoundKey

① b7 b6 b5 b4 b3 b2 b1 b0 shift bits to left by 1 pos

b6 b5 b4 b3 b2 b1 b0 b7 eg 23 64 52 11

→ 64 52 11 23

② SubWords same like 8 bit byte.

64 → 19 23 32 55

(Row → column)

(10 words)

③ R1 R2 R3 ..... R10

01 02 04 ..... 36 (fixed values)

00

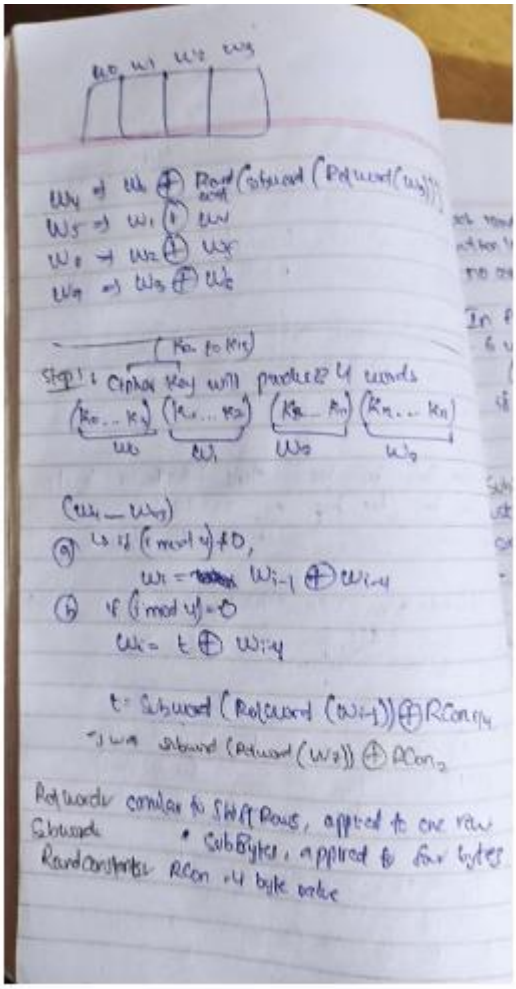
00

00

XOR this with ② → last

18 23 32 55

01 00 00 00



RSA.pdf - Adobe Acrobat Reader (32-bit)

File Edit View Sign Window Help

Home Tools [SECURITY][Compu... RSA.pdf Sign In

2 / 3

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 21.7 The RSA Algorithm

Search 'Bates'

Edit PDF

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

RSA.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

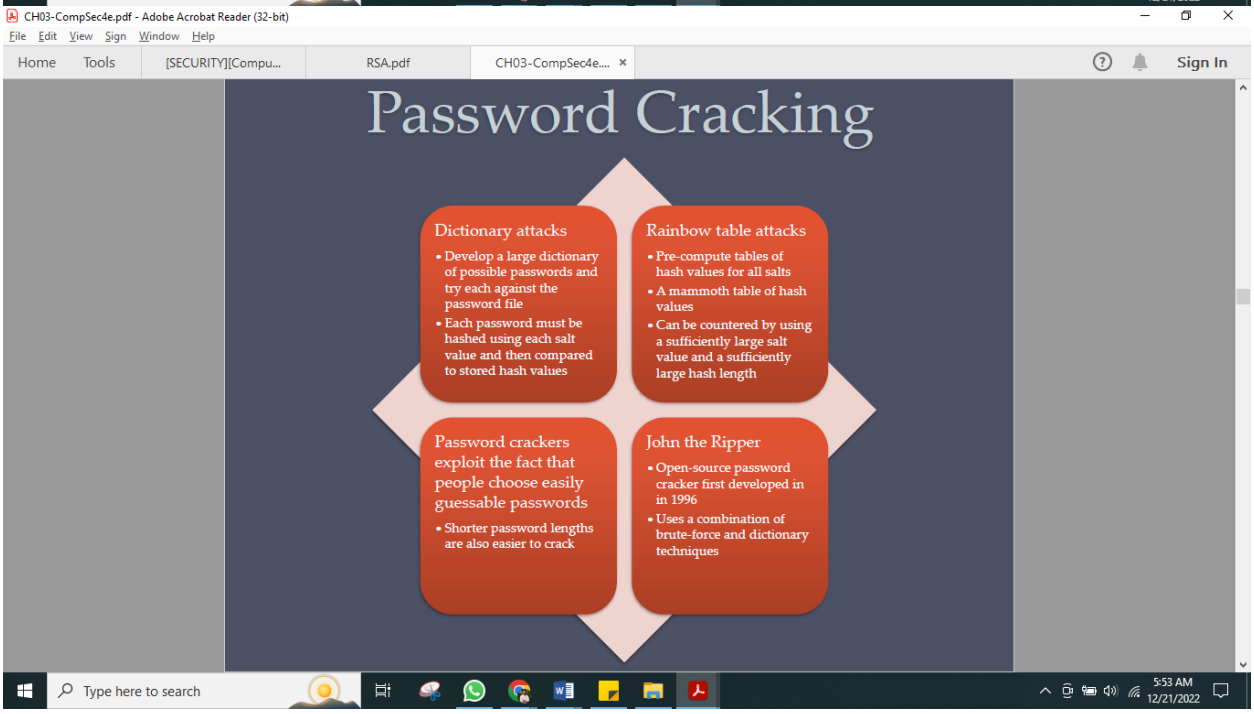
Convert, edit and e-sign PDF forms & agreements

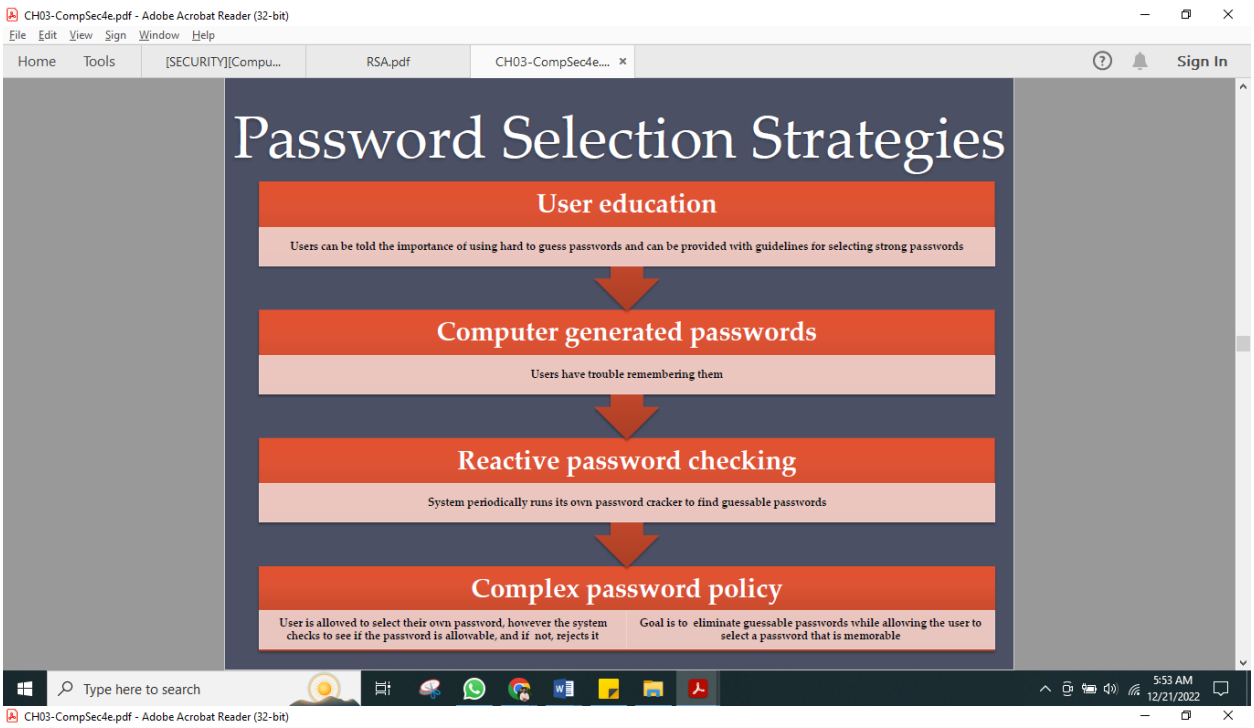
Free 7-Day Trial

Type here to search

4:15 AM 12/21/2022


CH03-CompSec4e.pdf - Adobe Acrobat Reader (32-bit)
File Edit View Sign Window Help
Home Tools [SECURITY][Compu... RSA.pdf CH03-CompSec4e.... Sign In
Password Vulnerabilities
Offline dictionary attack
Password guessing against single user
Workstation hijacking
Electronic monitoring
Specific account attack
Popular password attack
Exploiting user mistakes
Exploiting multiple password use
Type here to search
5:52 AM
12/21/2022


CH03-CompSec4e.pdf - Adobe Acrobat Reader (32-bit)
File Edit View Sign Window Help
Home Tools [SECURITY][Compu... RSA.pdf CH03-CompSec4e.... Sign In
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
• Open-source password cracker first developed in in 1996
• Uses a combination of brute-force and dictionary techniques
Type here to search
5:53 AM
12/21/2022


CH03-CompSec4e.pdf - Adobe Acrobat Reader (32-bit)
File Edit View Sign Window Help
Home Tools [SECURITY][Compu... RSA.pdf CH03-CompSec4e.... Sign In
Password Selection Strategies
User education
Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords
Computer generated passwords
Users have trouble remembering them
Reactive password checking
System periodically runs its own password cracker to find guessable passwords
Complex password policy
User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it
Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable
Type here to search
5:53 AM
12/21/2022


CH03-CompSec4e.pdf - Adobe Acrobat Reader (32-bit)
File Edit View Sign Window Help
Home Tools [SECURITY][Compu... RSA.pdf CH03-CompSec4e.... Sign In
Proactive Password Checking
Rule enforcement
Specific rules that passwords must adhere to
Password checker
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
Type here to search
5:53 AM
12/21/2022

Access Control Definitions 1/2

NISTIR 7298 defines access control as:

"the process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities"

Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- 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
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

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)

Virus Components

Infection 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

Virus Phases

Dormant phase

Virus is idle	Will eventually be activated by some event	Not all viruses have this stage

Triggering phase

Virus is activated to perform the function for which it was intended	Can be caused by a variety of system events

Propagation phase

Virus places a copy of itself into other programs or into certain system areas on the disk	May not be identical to the propagating version	Each infected program will now contain a clone of the virus which will itself enter a propagation phase

Execution phase

Function is performed	May be harmless or damaging

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

Social Engineering

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

Spam	Trojan horse	Mobile phone Trojans
Unsolicited bulk e-mail	Program or utility containing harmful hidden code	First appeared in 2004 (Skuller)
Significant carrier of malware	Used to accomplish functions that the attacker could not accomplish directly	Target is the smartphone
Used for phishing attacks		

Payload – Information Theft Keyloggers and Spyware

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")

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

Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention

Four main elements of 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

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

Intruder Skill Levels – Journeyman

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

Intruder Skill Levels – Master

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations
- Defending against these attacks is of the highest difficulty

Intruder Behavior

Target acquisition and information gathering	Initial access	Privilege escalation
Information gathering or system exploit	Maintaining access	Covering tracks

Intrusion Detection System (IDS)

- Host-based IDS (HIDS)
  - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
  - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
  - Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity

Comprises three logical components:

- **Sensors - collect data**
- **Analyzers - determine if intrusion has occurred**
- **User interface - view output or control system behavior**

IDS Requirements

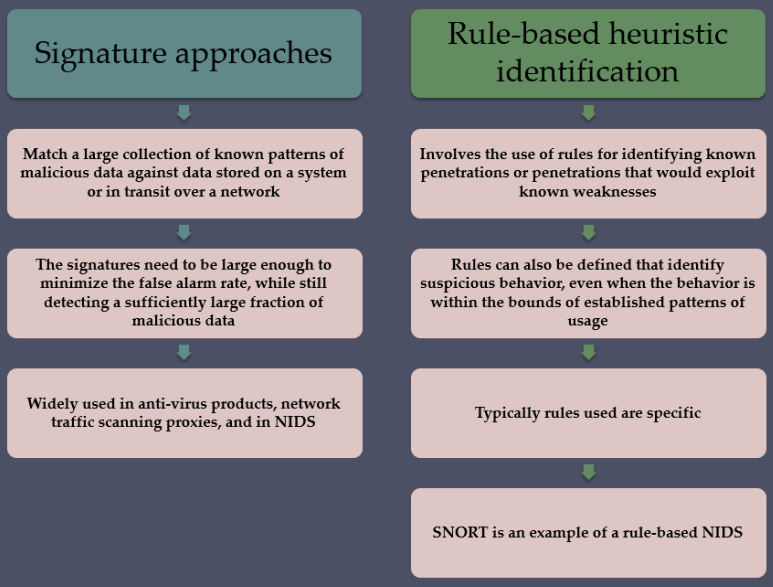
Run continually	Be fault tolerant	Resist subversion
Impose a minimal overhead on system	Configured according to system security policies	Adapt to changes in systems and users
Scale to monitor large numbers of systems	Provide graceful degradation of service	Allow dynamic reconfiguration

Anomaly Detection

A variety of classification approaches are used:

Statistical	Knowledge based	Machine-learning
• Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics	• Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior	• Approaches automatically determine a suitable classification model from the training data using data mining techniques

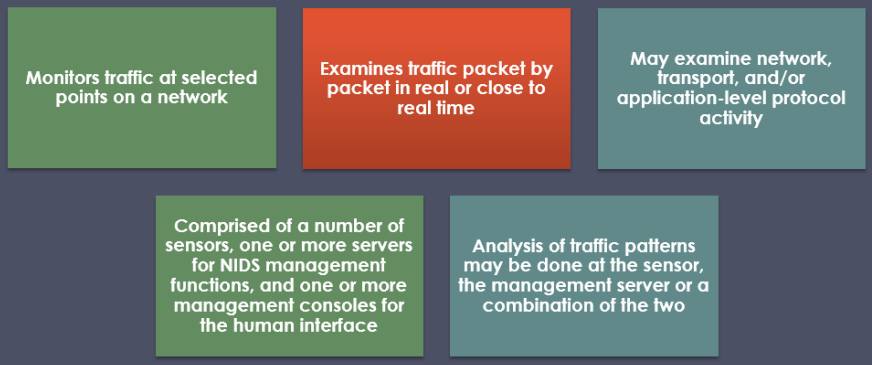
Signature or Heuristic Detection



Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behavior
  - Primary purpose is to detect intrusions, log suspicious events, and send alerts
  - Can detect both external and internal intrusions

Network-Based IDS (NIDS)



Stateful Protocol Analysis (SPA)

- Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
  - This distinguishes it from anomaly techniques trained with organization specific traffic protocols
- Understands and tracks network, transport, and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

IP address and protocol values	Application protocol	User identity	Network activity
This type of filtering is used by packet filter and stateful inspection firewalls	This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols	Typically for inside users who identify themselves using some form of secure authentication technology	Controls access based on considerations such as the time or request, rate of requests, or other activity patterns
Typically used to limit access to specific services			

Firewall Capabilities And Limits

Capabilities:

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec

Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
  - Typically a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match

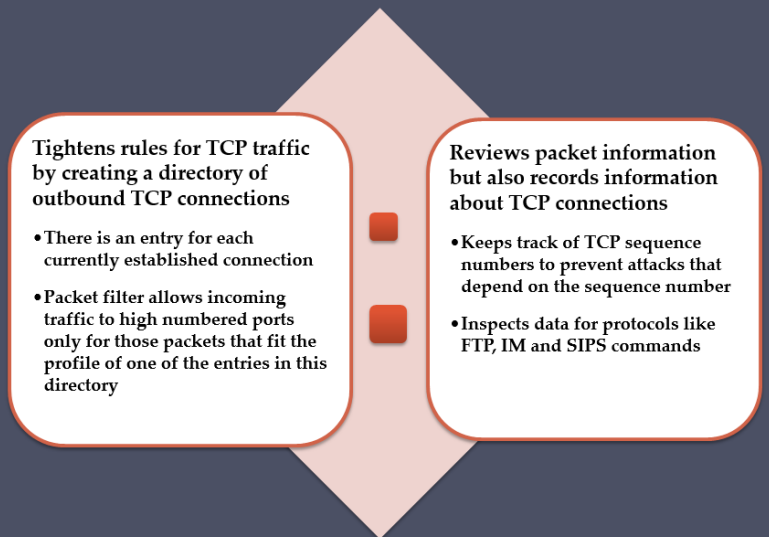
Filtering rules are based on information contained in a network packet
• Source IP address • Destination IP address • Source and destination transport-level address • IP protocol field • Interface

- Two default policies:
  - Discard - prohibit unless expressly permitted
    - More conservative, controlled, visible to users
  - Forward - permit unless expressly prohibited
    - Easier to manage and use but less secure

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic
  - User contacts gateway using a TCP/IP application
  - User is authenticated
  - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
  - May restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection

Stateful Inspection Firewall



Circuit-Level Gateway

Circuit level proxy

- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed

Typically used when inside users are trusted

- May use application-level gateway inbound and circuit-level gateway outbound
- Lower overheads

Host-Based IPS (HIPS)

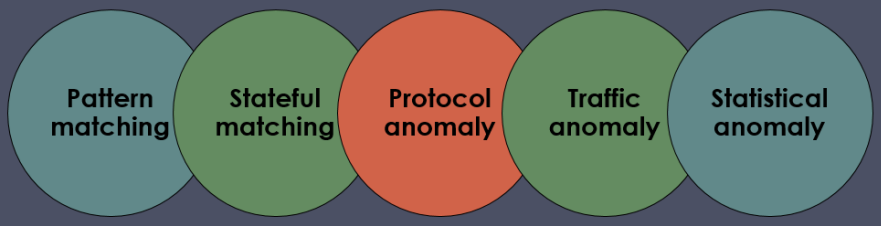
- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
  - Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
  - Anomaly: IPS is looking for behavior patterns that indicate malware
- Examples of the types of malicious behavior addressed by a HIPS include:
  - Modification of system resources
  - Privilege-escalation exploits
  - Buffer-overflow exploits
  - Access to e-mail contact list
  - Directory traversal

The Role of HIPS

- Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals
  - Thus security vendors are focusing more on developing endpoint security products
  - Traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, antispam, and personal firewalls
- Approach is an effort to provide an integrated, single-product suite of functions
  - Advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier
- A prudent approach is to use HIPS as one element in a defense-in-depth strategy that involves network-level devices, such as either firewalls or network-based IPSs

Network-Based IPS (NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature/heuristic detection and anomaly detection
- May provide flow data protection
  - Requires that the application payload in a sequence of packets be reassembled
- Methods used to identify malicious packets:



Security Risk Assessment

Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

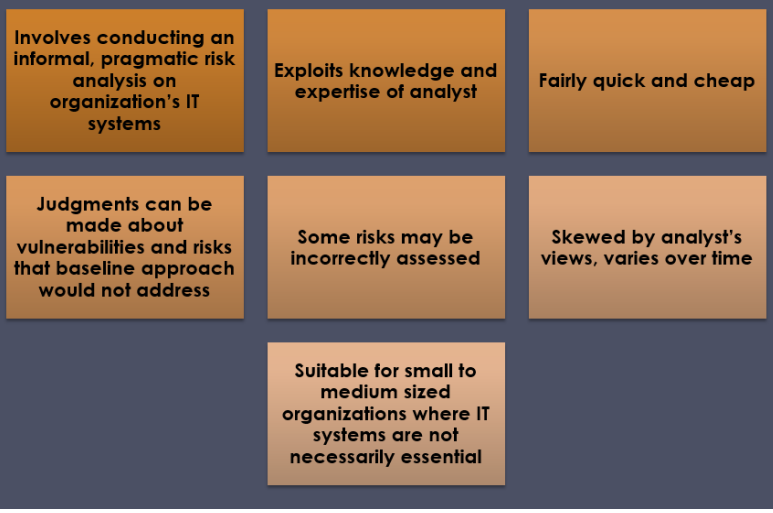
Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

Baseline Approach

- Goal is to implement agreed controls to provide protection against the most common threats
- Forms a good base for further security measures
- Use "industry best practice"
  - Easy, cheap, can be replicated
  - Gives no special consideration to variations in risk exposure
  - May give too much or too little security
- Generally recommended only for small organizations without the resources to implement more structured approaches

Informal Approach



Types of Computer Crime

- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:

Computers as targets	Computers as storage devices	Computers as communications tools
Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability	Using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software	Crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

European Union (EU) Directive on Data Protection

- Adopted in 1998 to:
  - Ensure member states protect fundamental privacy rights when processing personal information
  - Prevent member states from restricting the free flow of personal information within EU
- Organized around principles of:

Notice	Consent	Consistency	Access
Security	Onward transfer	Enforcement	

Data Privacy

- In terms of policy, guidelines are needed to manage the use and reuse of big data, ensuring suitable constraints are imposed in order to preserve privacy
  - Consent
    - Ensuring participants can make informed decisions about their participation in the research
  - Privacy and confidentiality
    - Privacy is the control that individuals have over who can access their personal information
    - Confidentiality is the principle that only authorized persons should have access to information
  - Ownership and authorship
    - Addresses who has responsibility for the data, and at what point does an individual give up their right to control their personal data
  - Data sharing – assessing the social benefits of research
    - The social benefits that result from data matching and reuse of data from one source or research project in another
  - Governance and custodianship
    - Oversight and implementation of the management, organization, access, and preservation of digital data

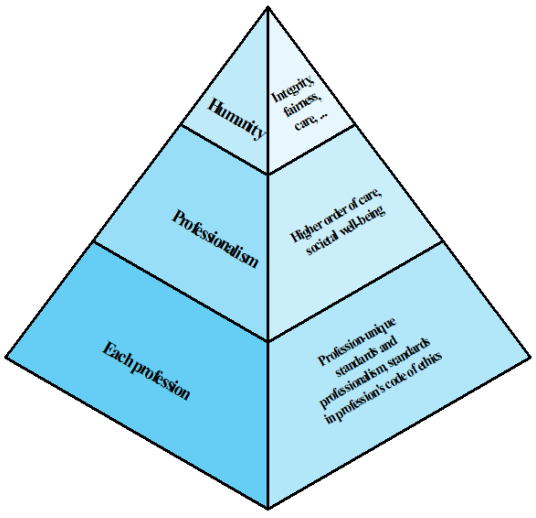


Figure 19.5 The Ethical Hierarchy

Injection Technique

The SQLi attack typically works by prematurely terminating a text string and appending a new command

Because the inserted command may have additional strings appended to it before it is executed the attacker terminates the injected string with a comment mark "- -"

Subsequent text is ignored at execution time

SQLi Attack Avenues

User input

- Attackers inject SQL commands by providing suitable crafted user input

Server variables

- Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers

Second-order injection

- A malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself

Cookies

- An attacker could alter cookies such that when the application server builds an SQL query based on the cookie's content, the structure and function of the query is modified

Physical user input

- Applying user input that constructs an attack outside the realm of web requests

Inband Attacks

- Uses the same communication channel for injecting SQL code and retrieving results
- The retrieved data are presented directly in application Web page
- Include:

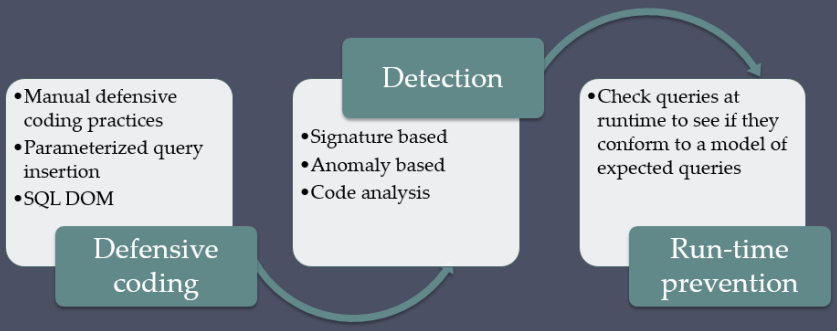
Tautology	End-of-line comment	Piggybacked queries
This form of attack injects code in one or more conditional statements so that they always evaluate to true	After injecting code into a particular field, legitimate code that follows are nullified through usage of end of line comments	The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request

Inferential Attack

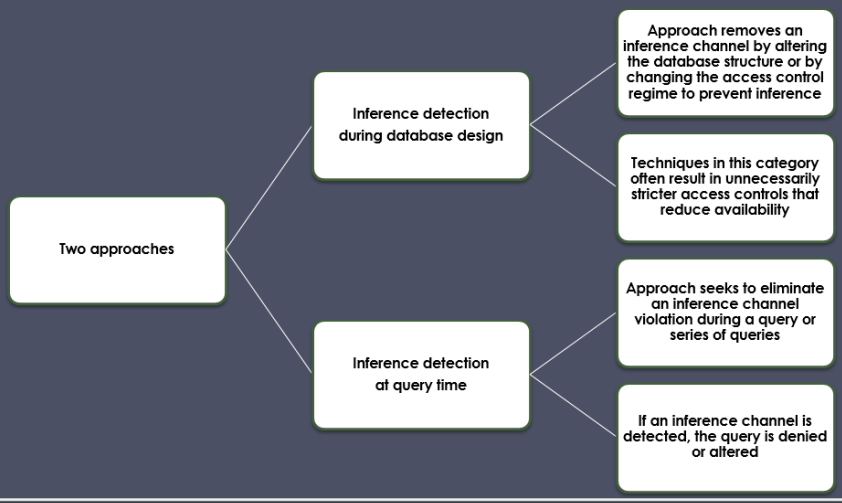
- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server
- Include:
  - Illegal/logically incorrect queries
    - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application
    - The attack is considered a preliminary, information-gathering step for other attacks
  - Blind SQL injection
    - Allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker

SQLi Countermeasures

- Three types:



Inference Detection



- Some inference detection algorithm is needed for either of these approaches
- Progress has been made in devising specific inference detection techniques for multilevel secure databases and statistical databases