BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Strategic Defense Mechanisms and Defense-in-Depth (DiD)

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Strategic Defense Mechanisms

Agenda

- Strategic Defense Mechanisms and Defense-in-Depth (DiD):
  - Technical, Operational, Managerial and Physical Defenses
  - Defense-in-Depth Approach and Layered Security Model
  - Defense mechanisms like
    - Encipherment, digital signatures, access control, intrusion detection, authentication exchange, routing control,
  - Pervasive mechanisms like
    - Security audit trail, event detection, security recovery, trusted functionality, anti-malware solutions, VPNs.

Pervasive Defense Mechanisms

Anti-Malware Solutions

innovate achieve lead

Overview

- Malware is a software, or script, or code designed to:
  - disrupt computer operation, gather sensitive information, or gain unauthorized access to a computer system without consent
- Malware is used by:
  - hackers, cybercriminals, hacktivists, and cyber terrorists to either steal, harm, or disrupt operations
- Today, there is no such thing as anti-virus program/software
  - Originally, anti-malware software focused on viruses
  - As malware expanded to include other malicious code such as Trojans, worms, spyware, and rootkits, anti-malware vendors expanded the abilities of their anti-malware software
  - Now, most anti-malware software will detect and block most malware, so technically it is anti-malware software

Source: CISSP Official Study Guide

Anti-Malware Solutions

Overview

- The most important protection against malicious code is the use of anti-malware software with up-to-date signature files and heuristic capabilities
- Attackers regularly release new malware and often modify existing malware to prevent detection by anti-malware software
- Anti-malware software vendors look for these changes and develop new signature files to detect the new and modified malware
- Years ago, anti-malware vendors recommended updating signature files once a week
- However, most anti-malware software today includes the ability to check for updates several times a day without user intervention

Source: CISSP Official Study Guide

Anti-Malware Solutions

Types of Malware

Family	General Description	Variants
Virus	Code that requires a host to execute and replicate	Macro, Boot sector, Stealth or a Script virus.
Worm	Self-contained programs that can replicate on its own Takes advantage of network transport to spread	Bots/Zombies, cryptos, APTs, or just generic worms
Trojan	Self-contained programs that appear legitimate and spread through user interaction	Embedded in music, in games, in greeting cards, or in utilities.
Rootkit	Self-contained program that has privileged system access	Firmware, kernel, boot record, and legitimate (anti-theft)
Spyware	Self-contained programs that collect user information and can manipulate configuration settings	Monitors, adware, tracking cookies, geolocators, and click fraud

Source: CISSP 2/e By Sari Greene

Anti-Malware Solutions

Malware Use Cases

- Facilitate extortion schemes, such as ransomware
- Weaponize our computers and devices, to turn them into bots and then into botnets and to be used in distributed denial of service attacks
- Collect authentication credentials for impersonation
- Exfiltrate data and intellectual property or IP
- Distributed SPAM or pornography or other illegal materials
- Carry out information warfare or sabotage

Source: CISSP Official Study Guide

Anti-Malware Solutions

innovate achieve lead

How do we get malware?

- The malware distribution channel is designed to entice users to unwittingly install and propagate malicious code by employing enticing tactics including:
  - Phishing emails with embedded links or attachments
  - Social media web links
  - Drive-by web download where it's just embedded in a website so when a user goes to that site, it just comes down to their system
  - Embedding malware in pictures, in movies, or in advertising
  - Embedding in portable media, like a USB

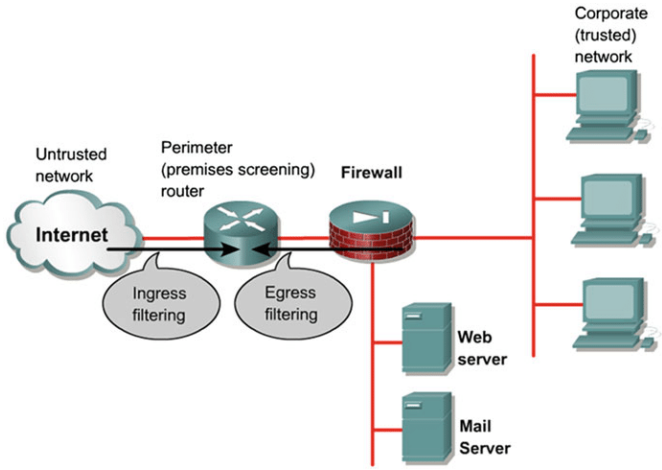
Source: CISSP Official Study Guide

Anti-Malware Solutions

innovate achieve lead

Malware Prevention and Disruption

- Malware prevention controls and techniques include:
  - Ingress and egress filtering and restrictions
  - Forbidding the receipt or the execution of certain file types
  - Restricting the use of removable media
  - Restricting cookies, pop-ups, mobile code execution, access to webmail and social media sites
  - Employing least privilege at the local level
  - Using Internet access sandboxes, so that we can isolate the activity
  - Educating users as to best practices, what they should and should not be doing



Source: CISSP Official Study Guide

Anti-Malware Solutions

innovate achieve lead

Strategies used by Anti-Malware Software

- Anti-malware software uses three strategies to protect systems:
  - signature-based detection
  - behavior-based detection and
  - sandboxing
- Signature-based malware detection
  - Uses a set of known software components and their digital signatures to identify new malicious software
  - Software vendors develop signatures to detect specific malicious software
  - The signatures are used to identify previously identified malicious software of the same type and to flag the new software as malware
  - This approach is useful for common types of malware, such as keyloggers and adware, which share many of the same characteristics

Source: https://searchsecurity.techtarget.com/definition/antimalware

Anti-Malware Solutions

innovate achieve lead

Strategies used by Anti-Malware Software

- Behavior-based malware detection
  - Uses an active approach to malware analysis
  - Identifies malicious software by examining how it behaves rather than what it looks like
  - It is sometimes powered by machine learning algorithms.
- Sandboxing
  - It is a technique used to isolate potentially malicious files from the rest of the system
  - It involves filtering out potentially malicious files and remove them before they have had a chance to do damage
  - For example:
    - when opening a file from an unknown email attachment, the sandbox will run the file in a virtual environment first
    - It grants access to a limited set of resources, such as a temporary folder, the internet and a virtual keyboard
    - If the file tries to access other programs or settings, it will be blocked, and the sandbox has the ability to terminate it

Source: https://searchsecurity.techtarget.com/definition/antimalware

Anti-Malware Solutions

Malware Detection and Analysis Techniques

Technique	Description
Use of anti-virus and anti-malware software	Incorporate signatures known as DAT files, and look for known characteristics and behavior
Post-infection scanners	Sometimes referred to as second-generation AV (E.g., Malwarebytes)
Log analysis	Use of security event and incident management (SEIM) or equivalent, to look at your logs to determine are there any indicators of compromise or indicators of attack
Malware intelligence	Knowledge of infection characteristics Connecting to a command-and-control server or known IP addresses or distribution URLs
Malware verification	Includes analysis of suspicious files and URLs For example, using a service like a VirusTotal
Reverse engineering	It is a process of analyzing and understanding characteristics Behavioral analysis Code analysis

Source: CISSP Official Study Guide

Anti-Malware Solutions

Malware Eradication Techniques

Technique	Description
Antivirus and anti-malware software	They will probably have disinfection, quarantine, and deletion capabilities
Regedit command	We could use regedit command if we needed to edit the Windows registry editor
Bootrec/fixmbr	We could use the Windows bootrec forward slash fixmbr if we need to fix the master boot record or repair the master boot record
Specialized bootable software	We could use specialized bootable software For example Microsoft Sysinternals Rootkit Revealer, or chkrootkit (www.chkrootkit.org) for a Linux or an OS X operating system
Restoration	We could just do a restoration, meaning, we reimage or rebuild the impacted system
Disposal	We could go really nuclear and dispose of the infected system, remove it, sanitize it, securely dispose of the infected device

Source: CISSP Official Study Guide

Anti-Malware Solutions

Multipronged Approach

- Many organizations use a multipronged approach to block malware and detect any malware that gets in

Technique	Description
Firewalls	Firewalls with content-filtering capabilities are commonly used at the boundary between the internet and the internal network to filter out any type of malicious code
Email Servers	Specialized anti-malware software is installed on email servers to detect and filter any type of malware passed via email
Other Systems	Additionally, anti-malware software is installed on each system to detect and block malware
Central Servers	Organizations often use a central server to deploy anti-malware software, download updated definitions, and push these definitions out to the clients

Source: CISSP Official Study Guide

Anti-Malware Solutions

innovate achieve lead

Single Anti-Malware Software

- Anti-malware software on each system in addition to filtering internet content helps protect systems from infections from any source
- For example
  - Using up-to-date anti-malware software on each system will detect and block a virus on an employee's USB flash drive
- Anti-malware vendors commonly recommend installing only one anti-malware application on any system
- When a system has more than one anti-malware application installed, the applications can interfere with each other and can sometimes cause system problems
- Additionally, having more than one scanner can consume excessive system resources

Source: CISSP Official Study Guide

Anti-Malware Solutions

innovate achieve lead

Following the Principle of Least Privilege

- Following the principle of least privilege also helps
- Users will not have administrative permissions on systems and will not be able to install applications that may be malicious
- If a virus does infect a system, it can often impersonate the logged-in user
- When this user has limited privileges, the virus is limited in its capabilities
- Additionally, vulnerabilities related to malware increase as additional applications are added
- Each additional application provides another potential attack point for malicious code

Source: CISSP Official Study Guide

Anti-Malware Solutions

innovate achieve lead

Educating Users

- Educating users about the dangers of malicious code, how attackers try to trick users into installing it, and what they can do to limit their risks is another protection method
- Many times, a user can avoid an infection simply by not clicking on a link or opening an attachment sent via email
- Social engineering tactics, including phishing, spear phishing, and whaling are used to install malware into users computers
- When users are educated about these types of attacks, they are less likely to fall for them
- Although many users are educated about these risks, phishing emails continue to flood the internet and land in users' inboxes
- The only reason attackers continue to send them is that they continue to fool some users

Source: CISSP Official Study Guide

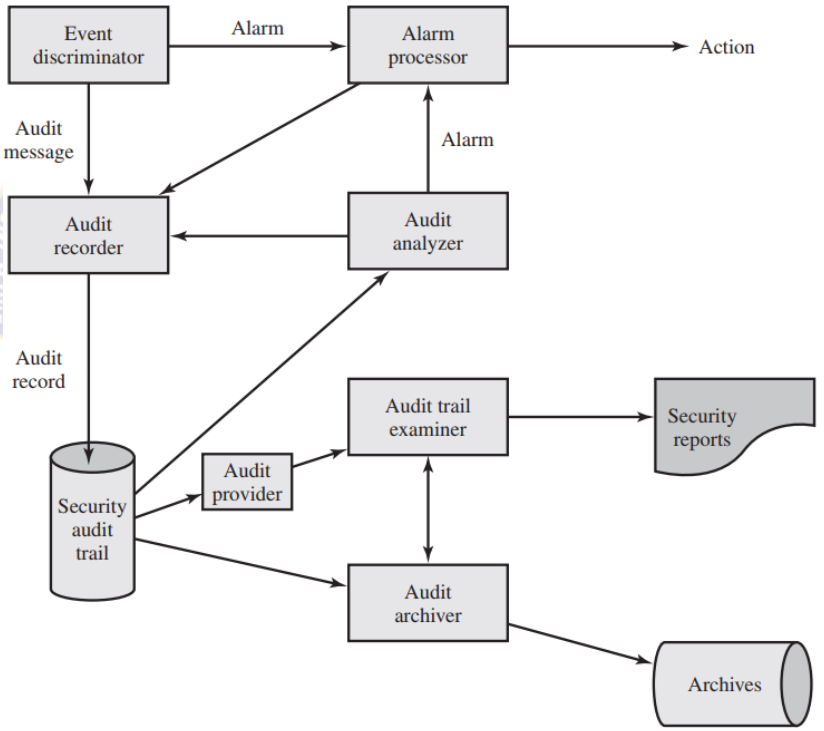
Security Audit Trail

Security Audit Trail

innovate achieve lead

Security Audit and Alarms Model

ITU-T Recommendation X.816 develops a model that shows the elements of the security auditing function and their relationship to security alarms



Security Audit and Alarms Model (X.816)

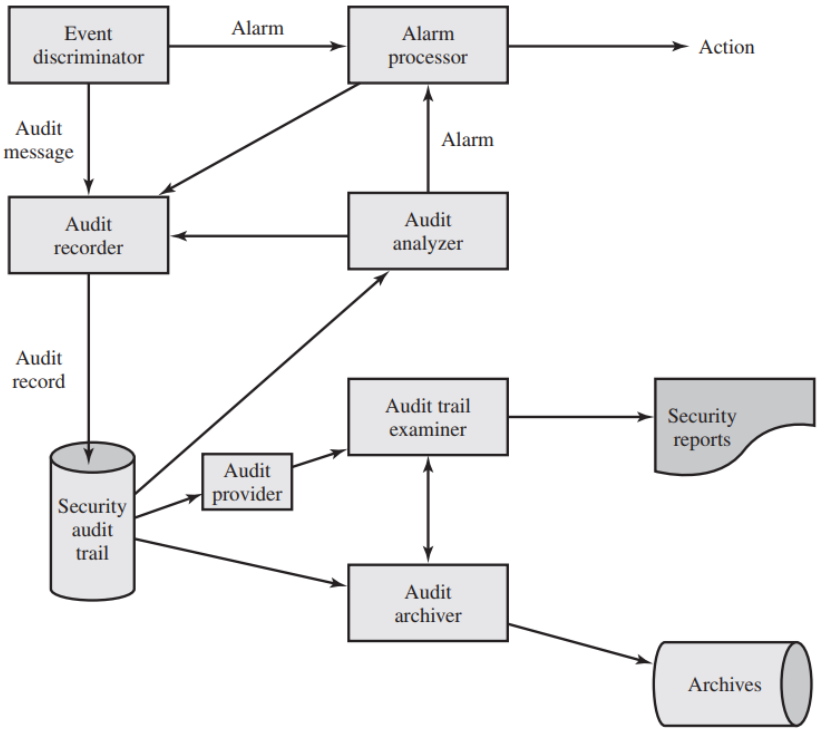
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

innovate achieve lead

Security Audit and Alarms Model

- Event discriminator
- Audit recorder
- Alarm processor
- Security audit trail
- Audit analyzer
- Audit archiver
- Archives
- Audit provider
- Audit trail examiner
- Security reports



Security Audit and Alarms Model (X.816)

Security Audit Trail

Data Collection

- Questions to be asked
  - Type of data to be collected
  - Amount of data to be collected
  - Granularity of data to be collected
- Cautions to keep in mind
  - There is a trade-off between quantity and efficiency
  - The more data are collected, the greater is the performance penalty on the system
  - Larger amounts of data also burden the algorithms used to examine and analyze the data
  - Presence of large amounts of data also creates a temptation to generate security reports (excessive in numbers and length)
- With these cautions in mind, the first step in security audit trail design is the selection of data items to capture

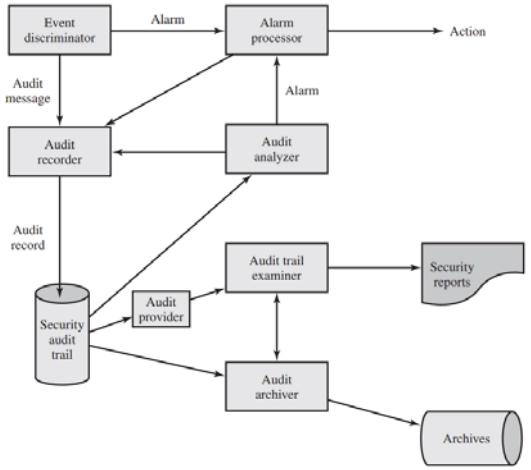
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

innovate achieve lead

Data Collection

- Selection of data items to capture
  - Events related to the security mechanisms on the system
  - Events related to the use of the auditing software (i.e., all the components of the Figure)
  - Any events that are collected by the various security detection and prevention mechanisms
    - These include items relevant to intrusion detection and items related to firewall operation
  - Events related to system management and operation
  - Operating system access (e.g., via system calls)
  - Application access for selected applications
  - Remote access



Security Audit and Alarms Model (X.816)

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

innovate achieve lead

Data Collection

Auditable Items Suggested in X.816

Security related events related to a specific connection
- Connection requests
- Connection confirmed
- Disconnection requests
- Disconnection confirmed
- Statistics appertaining to the connection

Security related events related to the use of security services
- Security service requests
- Security mechanisms usage
- Security alarms

Security related events related to management
- Management operations
- Management notifications

The list of auditable events should include at least
- Deny access
- Authenticate
- Change attribute
- Create object
- Delete object
- Modify object
- Use privilege

In terms of the individual security services, the following security-related events are important
- Authentication: verify success
- Authentication: verify fail
- Access control: decide access success
- Access control: decide access fail
- Non-repudiation: non-repudiable origination of message
- Non-repudiation: non-repudiable receipt of message
- Non-repudiation: unsuccessful repudiation of event
- Non-repudiation: successful repudiation of event
- Integrity: use of shield
- Integrity: use of unshield
- Integrity: validate success
- Integrity: validate fail
- Confidentiality: use of hide
- Confidentiality: use of reveal
- Audit: select event for auditing
- Audit: deselect event for auditing
- Audit: change audit event selection criteria

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

innovate achieve lead

Data Collection

a) user IDs b) system activities c) dates, times and details of key events, e.g. log-on and log-off d) device identity or location if possible and system identifier e) records of successful and rejected system access attempts f) records of successful and rejected data and other resource access attempts g) changes to system configuration	h) use of privileges i) use of system utilities and applications j) files accessed and the kind of access k) network addressees and protocols l) alarms raised by the access control system m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems n) records of transactions executed by users in applications

Monitoring Areas Suggested in ISO 27002

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

Data Collection

- The standard points out that both normal and abnormal conditions may need to be audited
- For instance, each connection request, such as a TCP connection request, may be a subject for a security audit trail record
  - Regardless of whether or not the request was abnormal and irrespective of whether the request was accepted or not
- Data collection for auditing goes beyond the need to generate security alarms or to provide input to a firewall module
- Data representing behavior that does not trigger an alarm can be used to identify normal versus abnormal usage patterns and thus serve as input to intrusion detection analysis
- In the event of an attack, an analysis of all the activity on a system may be needed to diagnose the attack and arrive at suitable countermeasures for the future

Security Audit Trail

System-Level Audit Trails

- System-level audit trails are generally used to monitor and optimize system performance but can serve a security audit function as well
- The system enforces certain aspects of security policy, such as access to the system itself
- A system-level audit trail should capture data such as login attempts, both successful and unsuccessful, devices used, and OS functions performed
- Other system-level functions may be of interest for auditing, such as system operation and network performance indicators

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

innovate achieve lead

System-Level Audit Trails

- Figure from [NIST95], is an example of a system-level audit trail on a UNIX system
- The shutdown command terminates all processes and takes the system down to single-user mode
- The su command creates a UNIX shell.

```
Jan 27  17:14:04   host1  login: ROOT LOGIN console
Jan 27  17:15:04   host1  shutdown: reboot by root
Jan 27  17:18:38   host1  login: ROOT LOGIN console
Jan 27  17:19:37   host1  reboot: rebooted by root
Jan 28  09:46:53   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
Jan 28  09:47:35   host1  shutdown: reboot by user1
Jan 28  09:53:24   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 12  08:53:22   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 17  08:57:50   host1  date: set by user1
Feb 17  13:22:52   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
```

(a) Sample system log file showing authentication messages

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

Application-Level Audit Trails

- Application-level audit trails may be used to detect security violations within an application or to detect flaws in the application's interaction with the system
- For critical applications, or those that deal with sensitive data, an application-level audit trail can provide the desired level of detail to assess security threats and impacts
- For example, for an e-mail application, an audit trail can record sender and receiver, message size, and types of attachments
- An audit trail for a database interaction using SQL queries can record the user, type of transaction, and even individual tables, rows, columns, or data items accessed.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

Application-Level Audit Trails

- An example of an application-level audit trail for a mail delivery system

```
Apr 9 11:20:22   host1   AA06370:  from=<user2@host2>, size=3355, class=0
Apr 9 11:20:23   host1   AA06370:  to=<user1@host1>, delay=00:00:02,stat=Sent
Apr 9 11:59:51   host1   AA06436:  from=<user4@host3>, size=1424, class=0
Apr 9 11:59:52   host1   AA06436:  to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 12:43:52   host1   AA06441:  from=<user2@host2>, size=2077, class=0
Apr 9 12:43:53   host1   AA06441:  to=<user1@host1>, delay=00:00:01, stat=Sent
```

(b) Application-level audit record for a mail delivery system

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

User-Level Audit Trails

- A user-level audit trail traces the activity of individual users over time
- It can be used to hold a user accountable for his or her actions
- Such audit trails are also useful as input to an analysis program that attempts to define normal versus anomalous behavior
- A user-level audit trail can record user interactions with the system, such as commands issued, identification and authentication attempts, and files and resources accessed
- The audit trail can also capture the user's use of applications

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

User-Level Audit Trails

- An example of a user-level audit trail on a UNIX system

```
rcp        user1    ttyp0    0.02 secs Fri Apr 8 16:02
ls         user1    ttyp0    0.14 secs Fri Apr 8 16:01
clear      user1    ttyp0    0.05 secs Fri Apr 8 16:01
rpcinfo    user1    ttyp0    0.20 secs Fri Apr 8 16:01
nroff      user2    ttyp2    0.75 secs Fri Apr 8 16:00
sh         user2    ttyp2    0.02 secs Fri Apr 8 16:00
mv         user2    ttyp2    0.02 secs Fri Apr 8 16:00
sh         user2    ttyp2    0.03 secs Fri Apr 8 16:00
col        user2    ttyp2    0.09 secs Fri Apr 8 16:00
man        user2    ttyp2    0.14 secs Fri Apr 8 15:57
```

(c) User log showing a chronological list of commands executed by users

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail

Physical-Level Audit Trails

- Equipment that controls physical access can generate audit trails
  - For example, card-key systems and alarm systems
- This data can be transmitted to a central host for subsequent storage and analysis
- The following are some examples of the type of data of interest:
  - The date and time the access was attempted to made
  - Gate or door through which the access was attempted
  - The individual user ID that attempted to access the gate or door
  - Invalid attempts
  - Attempts made to access during unauthorized hours or outside of the normal working hours
  - Attempts to add, modify, or delete physical access privileges
    - E.g., granting a new employee access to the building
    - E.g., grating access to the building to visitors
  - Valid and invalid attempts to gain access to controlled spaces


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!