Computer Security: Principles and Practice

Chapter 18: Security Auditing

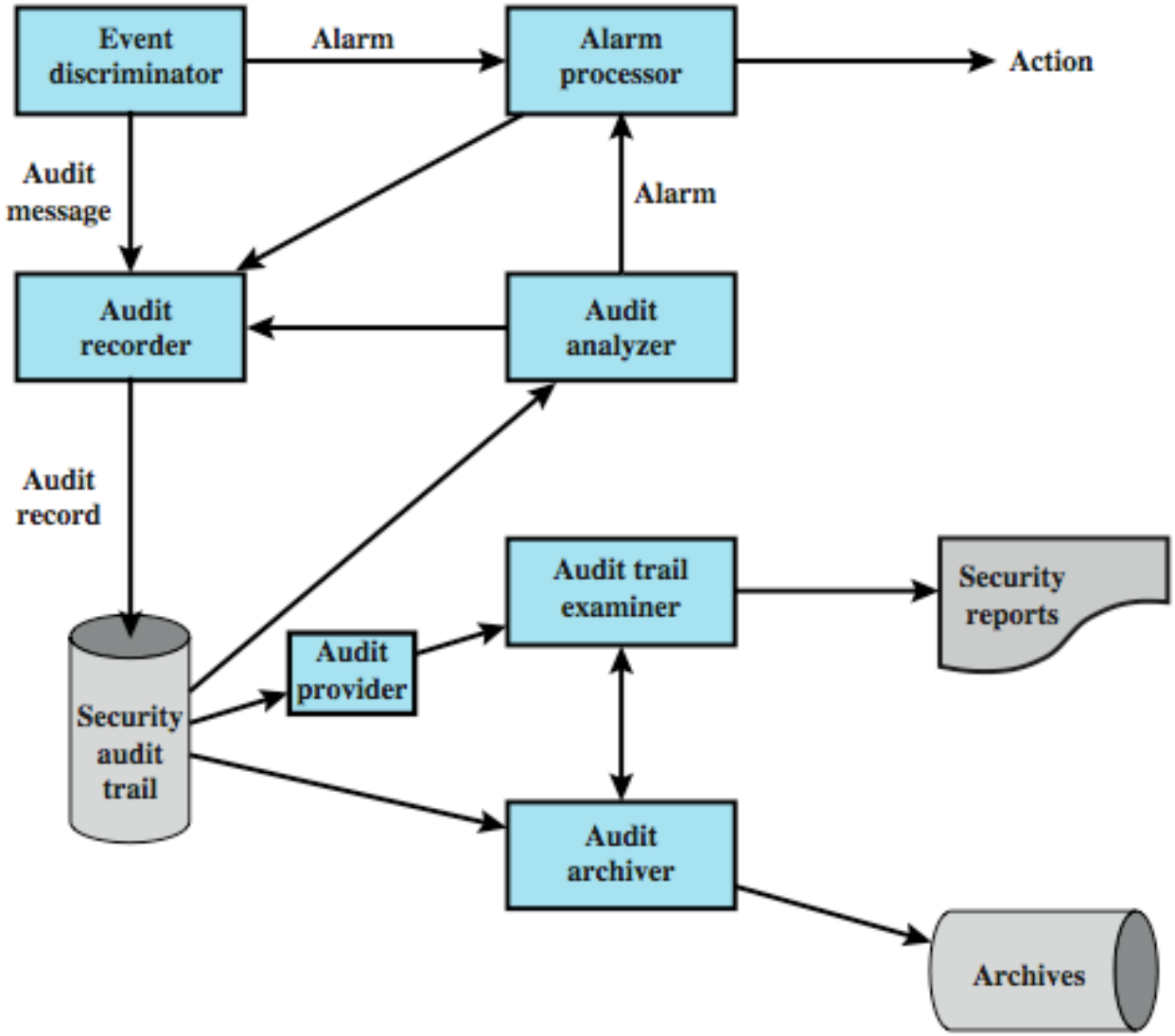
Security Audit Terminology (RFC 4949)

- An independent review and examination of a system's records and activities
  - To determine the adequacy of system controls
  - To ensure compliance with established security policy and procedures, detect breaches in security services,
  - To recommend any changes that are indicated for countermeasures
- Objectives: to establish accountability for system entities that initiate or participate in security-relevant events and actions

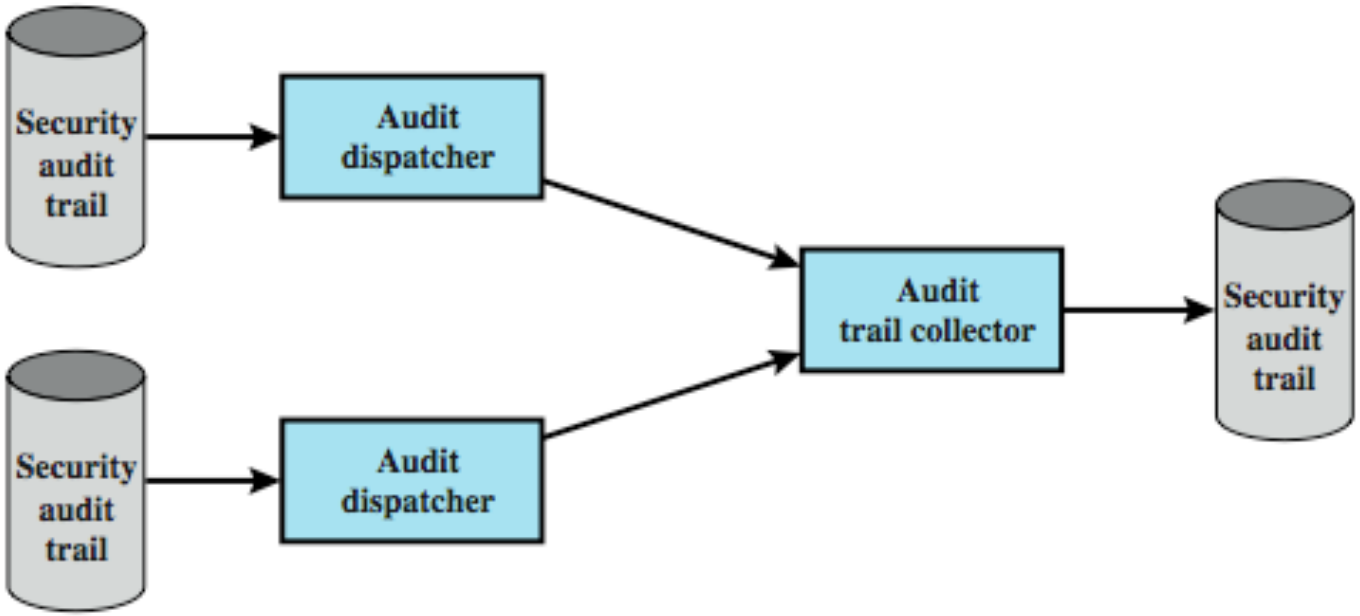
Security Audit Trail (RFC 4949)

- A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results

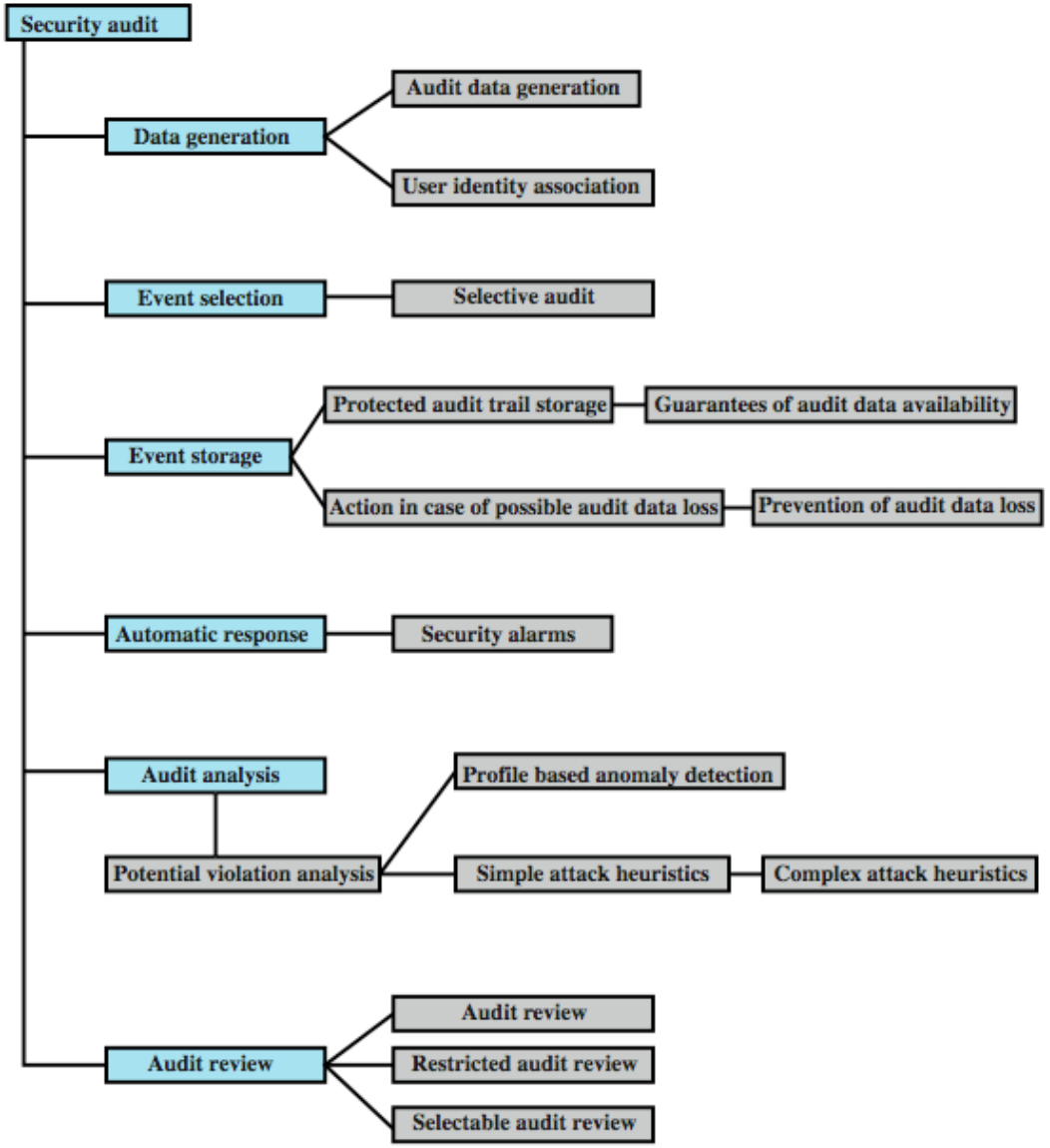
Security Audit Architecture (X.816)



Distributed Audit Trail Model



Security Auditing Functions



Security Audit Functions

- **Data generation:** Identifies the level of auditing, enumerates the types of auditable events
- **Event selection:** Inclusion or exclusion of events from the auditable set
- **Event storage:** Creation and maintenance of the secure audit trail
- **Automatic response:** reactions taken if detect a possible security violation event
- **Audit analysis:** automated mechanisms to analyze audit data in search of security violations
- **Audit review:** available to authorized users to assist in audit data review

Event Definition: Requirement

- Must define what are auditable events
- Common Criteria suggests:
  - introduction of objects
  - ***deletion of objects***
  - distribution or revocation of access rights or capabilities
  - changes to subject or object security attributes
  - policy checks performed by the security software
  - ***use of access rights to bypass a policy check***
  - use of identification and authentication functions
  - security-related actions taken by an operator/user
  - ***import/export of data from/to removable media***

Other Audit Requirements

- Event detection hooks in software and monitoring software to capture activity
- Event recording function with secure storage
- Event and audit trail analysis software, tools, and interfaces
- Security of the auditing function: data but also software and storage must be protected
- Minimal effect on functionality

What to Collect

- Data items captured may include:
  - auditing software use
  - use of system security mechanisms
  - events from IDS and firewall systems
  - system management/operation events
  - operating system access (system calls)
  - access to selected applications
  - remote access
- A common concern: the of amount of data generated

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

Examples of System-Level Audit Trails

- Useful to categorize audit trails
- System-level audit trails:
  - Captures logins, device use, O/S functions, e.g.

```
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
```

Example of Application-Level Audit Trails

- To detect security violations within an application
- To detect flaws in application's system interaction
- For critical/sensitive applications, e.g. email, DB
  - email: sender, receiver, email size
  - database: queries, table insertion and removal
- Record appropriate security related details, e.g.

```
Apr 911:20:22 host1 AA06370: from=<user2@host2>,
  size=3355, class=0
Apr 911:20:23 host1 AA06370: to=<user1@host1>,
  delay=00:00:02,stat=Sent
Apr 911:59:51 host1 AA06436: from=<user4@host3>,
  size=1424, class=0
Apr 911:59:52 host1 AA06436: to=<user1@host1>,
  delay=00:00:02, stat=Sent
```

User-Level Audit Trails

- Trace activity of individual users over time
  - to hold user accountable for actions taken
  - as input to an analysis program that attempts to define normal versus anomalous behavior
- May capture
  - user interactions with system
    - e.g. commands issued
  - identification and authentication attempts
  - files and resources accessed
  - may also log use of applications

Physical-Level Audit Trails

- Generated by physical access controls
  - e.g. card-key systems, alarm systems
- Sent to central host for analysis/storage
- Can log
  - date/time/location/user of access attempt
  - both valid and invalid access attempts
  - attempts to change access privileges
  - may send violation messages to personnel

Audit Trail Storage Alternatives

- Read/write file on host
  - easy, least resource use, fast access
  - vulnerable to attack by intruder
- Write-once device (e.g. CD/DVD-ROM)
  - more secure but less convenient
  - need media supply and have delayed access
- Write-only device (e.g. printer)
  - paper-trail but impractical for analysis
- Must protect both integrity and confidentiality
  - e.g., change pay level, or rank
  - using encryption, digital signatures, access controls

Implementing Logging

- Foundation of security auditing facility is the initial capture of the audit data
- Software must include hooks (capture points) that trigger data collection and storage as preselected events occur
- Operating system/application dependent

Windows Event Log

- Each event an entity that describes some interesting occurrence and
  - each event record contains: numeric id, set of attributes, optional user data
  - Presented as XML or binary data
- Three types of event logs:
  - system: system related apps & drivers
  - application: user-level apps
  - security: for Local Sec Authority (LSA) only

Windows Event Log Example

- Event Type: Success Audit
- Event Source: Security Event
- Category: (1)
- Event ID: 517
- Date: 3/6/2006
- Time: 2:56:40 PM
- User: NT AUTHORITY\SYSTEM
- Computer: KENT
- Description: The audit log was cleared
- Primary User Name: SYSTEM
- Primary Domain: NT AUTHORITY
- Primary Logon ID: (0x0,0x3F7)
- Client User Name: userk
- Client Domain: KENT
- Client Logon ID: (0x0,0x28BFD)

Windows Event Categories

- Account logon events: acceptance/rejection of authentication
- Account management: account creation/deletion
- Directory service access: user access to active dir (that has a system access control defined)
- Logon events: user log in/log off, bad password
- Object access: same as DSL but to registry and similar
- Policy changes: admin changes to access policies
- Privilege use: user right changes
- Process tracking: start and termination
- System events: start, reboot, shut down

UNIX Syslog

- UNIX's general-purpose logging mechanism
  - Found on all UNIX/Linux variants
  - But with variants in facility and log format
- Elements:
  - syslog() API
  - /etc/syslog.conf configuration file
  - syslogd daemon to receive/route log events

Syslog Examples

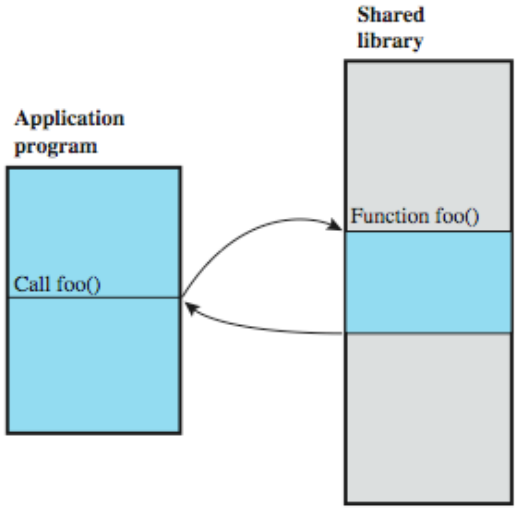
```
Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for
   server2 from 172.30.128.115 port 21011 ssh2
Mar 1 07:16:42 server1 sshd[9326]: Accepted password for
   murugiah from 10.20.30.108 port 1070 ssh2
Mar 1 07:16:53 server1 sshd[22938]: reverse mapping
   checking getaddrinfo for ip10.165.nist.gov failed -
   POSSIBLE BREAKIN ATTEMPT!
Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for
   server2 from 172.30.128.115 port 30606 ssh2
Mar 1 07:28:33 server1 su: BAD SU kkent to root on
   /dev/ttyp2
Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

Logging at Application Level

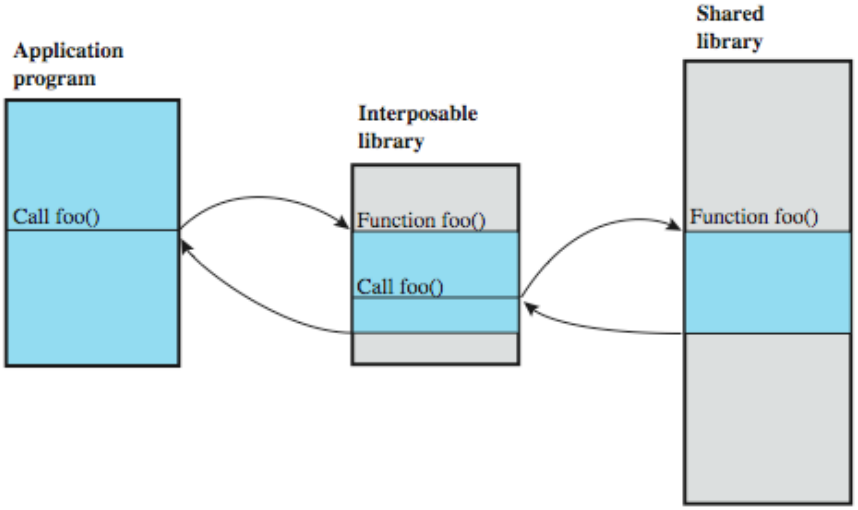
- Privileged applications have security issues
  - which system/user-level audit data may not see
  - a large percentage of reported vulnerabilities
  - e.g. failure to adequately check input data (that lead to buffer overflow)
- Hence need to capture detailed behavior

Interposable Libraries

Intercept calls to shared 100s of library functions; can carry out audit related functions

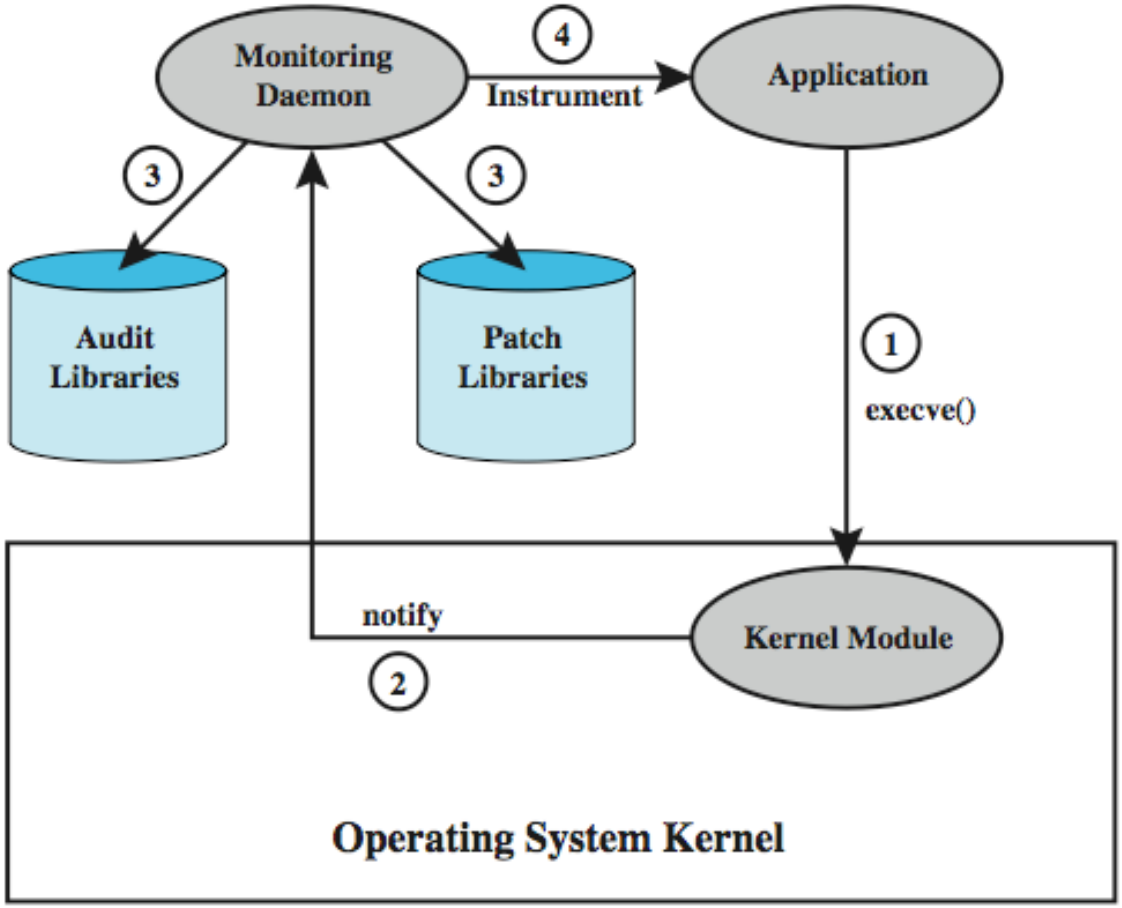


(a) Normal library call technique



(b) Library call with interposition

Dynamic Binary Rewriting



Audit Trail Analysis

- Analysis programs/procedures vary widely
  - cf. NIST SP 800-92 provide guidelines
- Must understand context of log entries
  - relevant info in same / other logs, config
  - possibility f unreliable entries
- Audit file formats mix of plain text / codes
  - hence must decipher manually / automatically
- Ideally regularly review entries to gain understanding of baseline

Types of Audit Trail Analysis

- Audit trails can be used in multiple ways
- Possibilities include:
  - Audit trail review after an event
    - triggered by event to diagnose cause & remediate
  - Periodic review of audit trail data
    - review bulk data to identify a pattern that suggests problem
  - Real-time audit analysis
    - as part of an intrusion detection function

Audit Review: Specific Purpose

- Audit review capability provides admin with information from selected audit records
  - actions of one or more users
  - actions on a specific object or resource
  - all or a specified set of audited exceptions
  - actions on a specific system / security attribute
- May be filtered by time / source / freq etc

Approaches to Data Analysis

- Basic alerting (simplest)
  - indicates interesting type of event has occurred
- Baselining (anomaly detection)
  - define normal vs unusual events/patterns
  - anomaly detection
  - thresholding (e.g., # of refused connections)
- Windowing
  - of events within a set of parameters (e.g., time)
- Correlation
  - seek relationships among events

Example: Cisco MARS

- More elaborate than syslog
- Support a wide variety of systems
- Agentless with central dedicated server
- Wide array of analysis packages
- An effective GUI
- Server collects, parses, normalizes, correlates and assesses events to then check for false positives, vulnerabilities, and profiling

Summary

- Introduced need for security auditing
- Audit model, functions, requirements
- Security audit trails
- Implementing logging
- Audit trail analysis
- Integrated SIEM products