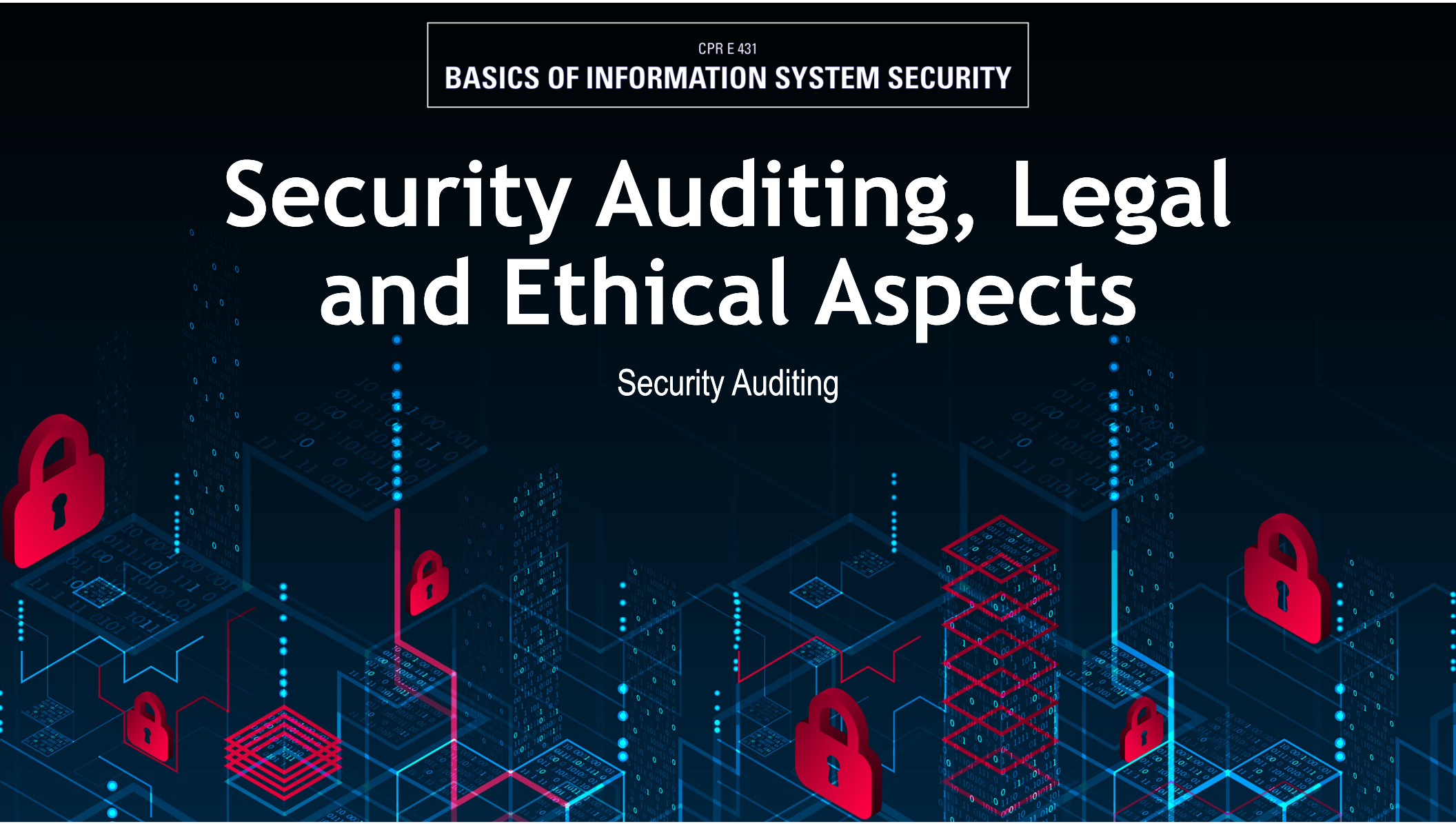
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Security Auditing, Legal and Ethical Aspects

Security Auditing



Video Summary

- What is Security Audit?
- Security Audit Model
- Security Audit Class Decomposition
- Event Definition and Detection
- Implementation Guidelines

Security Audit Terminology

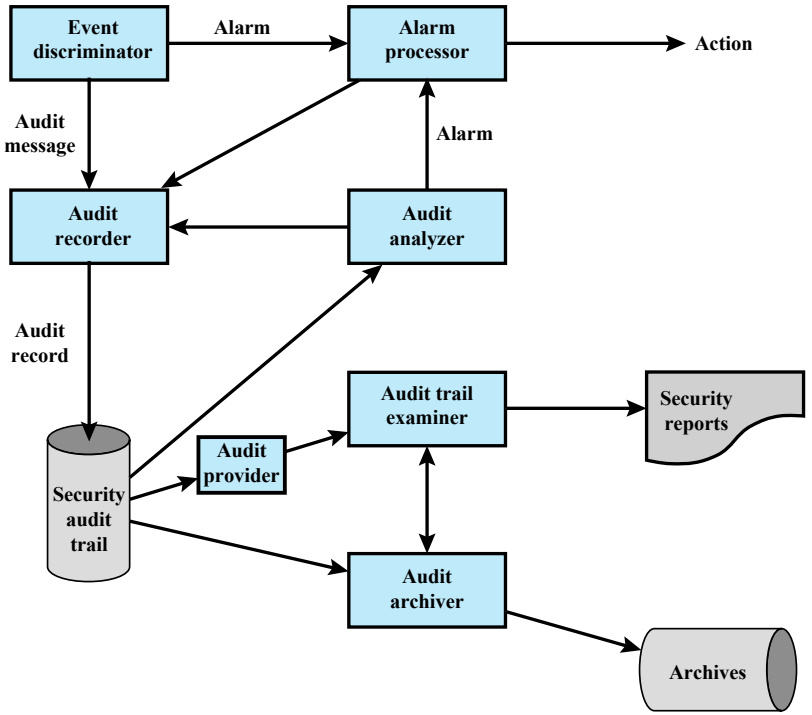
Two key concepts are Security audits and Security audit trails
"our concern is with the collection, storage, and analysis of data related to IT security."

Security audit An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.

The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate attacks and security compromises.

Security Audit Trail 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 and Alarm Model



Distributed Audit Trail Model

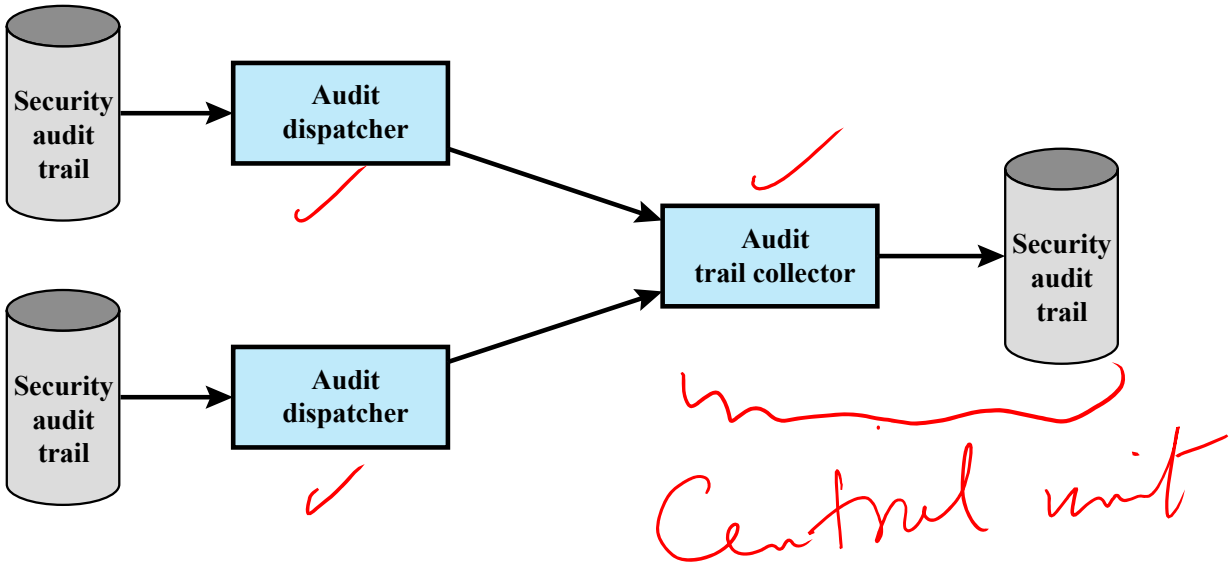
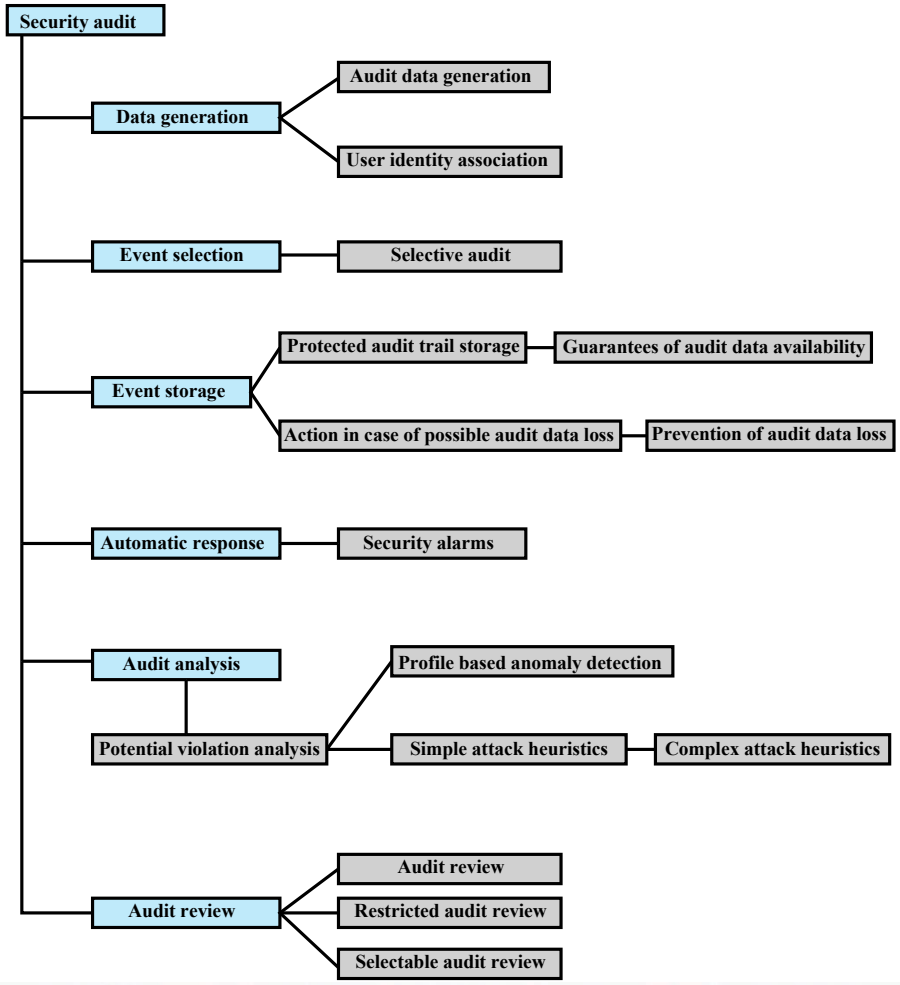


Figure 18.2 Distributed Audit Trail Model (X.816)

Security Audit Class Decomposition



Event Definition

- Must define the set of events that are subject to audit

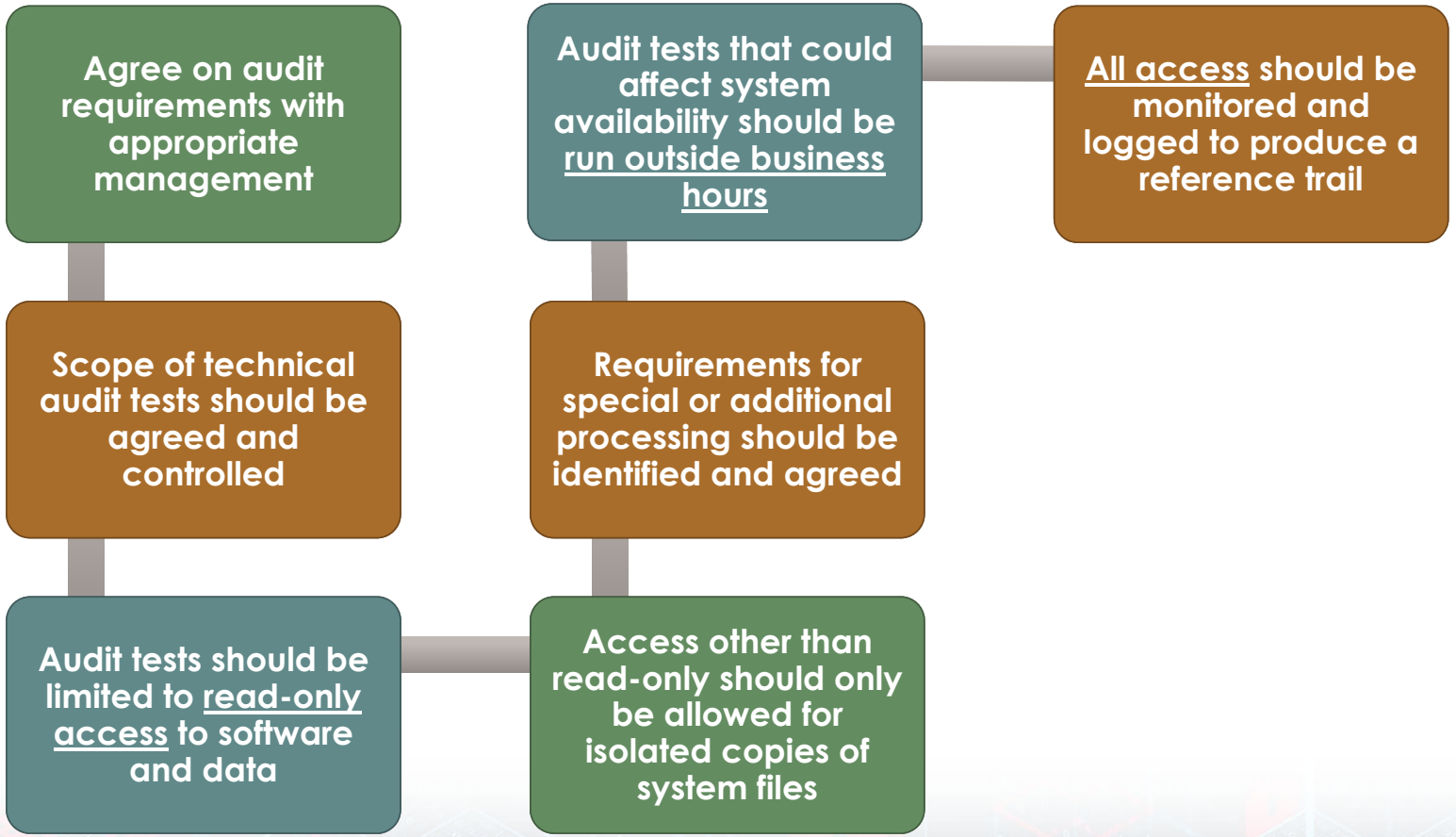
Common criteria suggests:

- Introduction of objects
- Deletion of objects
- Granting or revocation of access rights
- Changes to subject or object security attributes
- Policy checks performed by the security software as a request by a user
- Security-related actions taken by an operator/user
- Import/export of data from/to removable media

Event Detection

- Appropriate hooks must be available in the system software to enable event detection
- An event recording function is needed, which includes the need to provide for a secure storage resistant to deletion
- Event and audit trail analysis software may be used to analyze collected data and for investigating data trends and anomalies
- Auditing system should have a minimal effect on functionality

Implementation Guidelines



What to Collect

- Events related to the use of the auditing software
- Events that are collected for use by the various security detection and prevention mechanisms (anomaly detection)
- Events related to system management and operation
- Operating system access
- Application access for selected applications
- Remote access

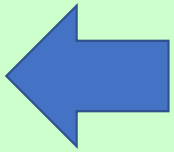
Auditable Items

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

Monitoring Areas Suggested in ISO 27002

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

Examples of Audit Trails

```
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

```
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

```
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

Video Summary

- What is Security Audit?
- Security Audit Model
- Security Audit Class Decomposition
- Event Definition and Detection
- Implementation Guidelines