Monitoring & Control Systems

CSH6 Chapter 53

"Monitoring and Control Systems"

Caleb S. Coggins and
Diane E. Levine

Topics in CSH6 Ch 53

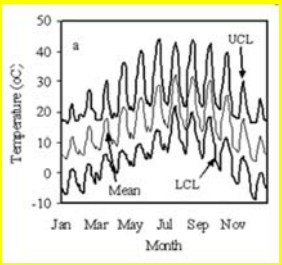
- Introduction
- Change & Security Implications
- System Models
- Targets & Methods
- Log Management
- Data Aggregation & Reduction
- Notifications & Reporting
- Monitoring & Control Challenges

Introduction (1)

- M&C systems involve
  - Prevention
  - Detection
  - Response
- Topics
  - Prevention, Detection & Response
  - Controlling vs Monitoring
  - Control Loop
  - Defining Scope & System Requirements

Introduction (2)

- Monitoring systems provides basis for
  - Quality control
  - Anomaly detection
- Key elements
  - System log files
  - Data reduction programs
- Additional resources
  - Application program log files
  - Statistical analysis tools and knowledge



Prevention, Detection & Response

- Cost-effective solutions to mitigate risks
  - IDS (intrusion detection systems, CSH6 Ch 27)
  - IPS (intrusion prevention systems, CSH6 Ch 26, 27)
  - UTM (unified threat management)
  - Anti-malware systems (CSH6 Ch 16, 17, 41)
- Detection: identifying problem
- Response
  - Monitoring system: logging, alarms
  - Control system: change parameters
- Failure to detect & respond may have business & legal implications (lack of *due diligence*)

Purpose of Monitoring & Control Systems

http://tinyurl.com/2o9frb

- Who is doing what when?
- Can contribute to self-regulation
  - Knowing that actions are monitored can reduce harmful behavior
  - Increases *self-awareness*
- Provide information for controlling system
  - Limiting access in response to observations
  - Changing conditions in response to trends
- Serve forensic investigations

Controlling vs Monitoring (1)

- Monitoring
  - Periodically checking aspects of operating environment
  - Encourages constant awareness and vigilance
  - Spot anomalies or trends
  - Predict and prevent problems and attacks
- Control
  - In this context, refers to comparing observations with policies and standards
  - May be referred to as *audits* or *assessments*

Controlling vs Monitoring (2)

- Monitoring modalities
  - Continuous Mode
    - ✓Real-time
    - ✓Firewalls, IDS, IPS, Anti-malware
  - Batch mode
    - ✓Periodic analysis
    - ✓Assessments and audits
- Controls
  - CobiT* (CSH6 Ch 44, 49, 53, 54, 67)
  - Based on well-defined policies

*Control Objectives for Information and Related Technology

Control Loop

- Humans usually remain in *control loop*
  - Controller
  - Target system
  - Bidirectional communication path
  - Transmitted data
- Some systems require automated response
  - E.g., dangerous breaches (gas pipeline) cannot wait for human intervention
  - But others should be *open loop* and require supervisory decisions (e.g., patch management)

Defining Scope & System Requirements

- Management must define
  - Extent of application (scope)
  - Capabilities required for success (requirements)
- Technical requirements depend on specific systems
- Often require
  - Hardware
  - Software
  - Intellectual property rights
  - Training
  - Personnel

Change & Security Implications

- Regulations, Policies & Frameworks
- Change Management
- Configuration Protection
- Performance Considerations

"What happened to the last VP who used this desk?"

Regulations, Policies & Frameworks

- Compliance requirements may determine specific needs; e.g.,
  - HIPAA (CSH6 Ch 71)
  - GLB (CSH6 Ch 64)
  - SoX (CSH6 Ch 54, 64)
- Frameworks support M&C; e.g.,
  - CobiT

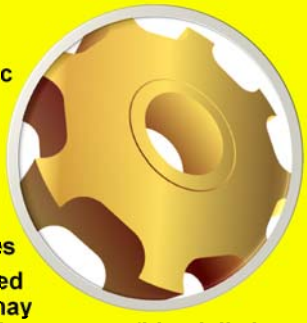
CobiT: Control Objectives for Information & Related Technology
GLB: Gramm-Leach-Bliley Act
HIPAA: Health Insurance Portability & Accountability Act
SoX: Sarbanes-Oxley Act

Change Management

- Immediate awareness of changes in operational status valuable
- Can identify tampering with production code & data
- Or can lead to identification of malware, attacks
- Records serve for diagnosis, analysis & prediction

Configuration Protection

- Changes in (production) systems require careful attention to detail
  - ❑Checklists
  - ❑Approved equipment & specific parameters
  - ❑Approved software & specific patches
- Monitoring / logging systems simplify task of spotting unauthorized or incorrect changes
  - ❑E.g., installation of unauthorized WAP (wireless access point) may generate unusual traffic (and threaten confidentiality)



Performance Considerations

- Addition of monitoring hardware, software may affect performance
  - ❑Some systems run on host being monitored – may use system resources
    - ✓Process-table related
    - ✓CPU, RAM
  - ❑Others connect to network
    - ✓May affect throughput
- Avoid implementing new systems without performance trials
- Don't install during full production period

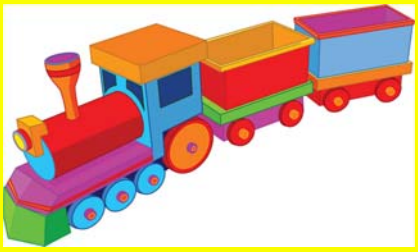
Volume Considerations

- Decide how often to close log files
  - ❑Disk space not much of an issue now
    - ✓In 1980, a 120 MB hard disk cost U$25,000
      - Approx U$100,000 in 2013 value
      - U$833/MB
    - ✓In 2015, a 3 TB Western Digital external hard disk cost $90
      - ~U$7.6294E-5/MB ($0.000076294/MB)
      - ~40% drop *per year* compounded over 35 years)
  - ❑Main issue today is preventing data loss if system or logging process crashes
  - ❑Especially important to fight *ransomware*

Image shows HP7925 120 MB drive c. 1980 (1980 cost U$25,000)

System Models

- Internal, 1:1, 1:N, Distributed
- Automation & HMI
- Snapshots vs Real Time
- Memory Dumps



Internal, 1:1, 1:N, Distributed

- Internal – monitor/control itself
- 1:1 – 1 system monitors another; e.g., firewall, fault-tolerant parallel systems
- 1:N – central M&C system for many systems; reduces costs, improves efficiency (more centralized logging, review, audit)
- Distributed – sensors & controls dispersed; central logging collector; ideal for heterogeneous systems

Automation & HMI

- 24-7-365 systems need automated M&C
- High volumes make manual inspection/response to alerts impractical
- Human-machine interface (HMI) allows operator to communicate with and control system
- Typically intervene for highly unusual events or patterns
- IPS can interact to defend against dispersed attacks (e.g., worms, DDoS)

Snapshots vs Real Time

- *One-point-in-time* records useful for
  - Auditing
  - Problem diagnosis
  - Incident response
  - Forensic analysis
- *Real-time* monitoring & control
  - Continuous sensing & response
  - E.g., industrial processes & systems such as gas pipelines or manufacturing systems
  - On Web sites, include IDS & IPS
  - Real-time log analysis → intelligent pattern recognition

Memory Dumps

- Overview
- Diagnostic Utilities
- Output to Magnetic Media or Paper
- Navigating the Dump Using Exploratory Utilities
- Understanding System Tables
- Security Considerations for Dump Data

Overview of Memory Dumps

- Files containing entire contents of RAM
- Useful for debugging and forensics
- Two types
  - Obtained through diagnostic utilities (debuggers) in real time
  - Captured after system shutdown from copies made to other media

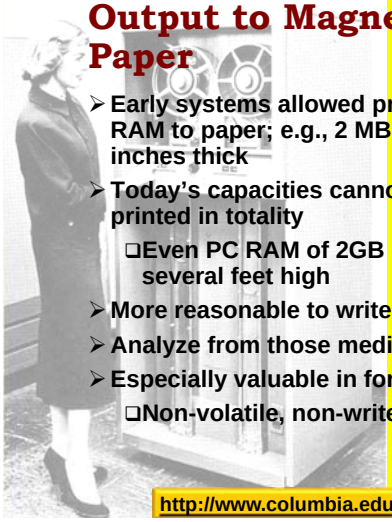
Memory Dumps

- Copy contents of RAM (main memory)
  - Typically taken after system failure
  - Useful in forensic research/analysis
- Methods
  - Diagnostic Utilities (debug)
    - ✓Read RAM without file-system restrictions
    - ✓Often include facilities for interpreting / representing system tables
  - Output to magnetic media or paper
    - ✓Printing difficult with large amounts of RAM
    - ✓Generally no longer print to paper

Navigating the Dump Using Exploratory Utilities

- RAM too large to explore "manually"
  - I.e., by inspecting everything
  - Suppose we use 256 characters x 88 lines = 22,528 bytes/page
  - Then 1 MB would take ~46.55 pp
  - So 2 GB would take 95,325 pp
  - If inspection rate were 1 minute per page (FAST), would take 66 days to read the dump once
- Use utilities to navigate through tables at will
- Search for strings

Output to Magnetic Media or Paper



- Early systems allowed printing contents of RAM to paper; e.g., 2 MB filled stack a few inches thick
- Today's capacities cannot reasonably be printed in totality
  - Even PC RAM of 2GB on paper could be several feet high
- More reasonable to write to disk, DVD
- Analyze from those media
- Especially valuable in forensic examination
  - Non-volatile, non-writeable media preferred

http://www.columbia.edu/acis/history/701-tape.html

Diagnostic Utilities

- System-level DEBUG utilities give complete access to RAM
- Thus allow total bypass of system security
  - Extremely powerful = dangerous tools
  - Can copy or alter any portion of memory
  - Usually access system tables by name, make changes
  - Stop processes, alter priorities etc.
- Critically important to control access to these tools
  - Separation of duties – approval, supervision

Memory Dumps

- Security important for dumps
  - Much sensitive information in clear
    - ✓Passwords, keys
    - ✓Confidential data from databases etc.
    - ✓Classified data
  - Therefore must safeguard physical and electronic access
- Label clearly and unambiguously to prevent accidental usage
- Store securely in physically-restricted facilities
  - Vault, safe
  - ID & signature required for acces

Security Considerations for Dump Data

- Be aware that dumps can be major security vulnerability
- Contain cleartext versions of vast amounts of confidential and encrypted data
- Includes I/O buffers such as input from keyboards and files or output to displays and files
- Can be disaster to release dump
- Serious question about whether vendor should be permitted to see memory dump

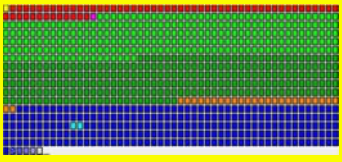
System Tables

Examples of Critically Important System Tables

- Process control block (PCB) – pointers to all the running processes ("Task Manager" listing in Windows)
- Process tables – all current details for every process
- Data stacks – variables for each process & stack markers showing trail of execution
- I/O Buffers – data in transit
- Memory-management tables
- Inter-process communication (IPC) tables
  - Flags, semaphores, status fields

Understanding System Tables

- Operating systems differ in detail
- Basic concepts similar
- Key tables include
  - Process control table
  - Process tables
  - Data stacks
  - Buffers
  - Memory management tables
  - IPC tables



Targets & Methods of Logging

- Overview
- Process Flow & Job Scheduling
- Network Connectivity
- Environmental Concern
- System State
- System Components
- Process Activities
- File System
- Access Controls

Overview of Targets & Methods

- Choices depend on specific context
- Consider mission-critical operations / systems; e.g.,
  - Process flow
  - Job scheduling
  - Network connectivity
  - Environmental measurement
  - System states
  - System components
  - Process activities
  - Configuration settings
  - File system information
  - Access control

Process Flow & Job Scheduling

- Batch job scheduler tracks jobs
- Ideally, use centralized job scheduler/logger
- May have to connect to remote systems
- If necessary, plan for incremental, gradual migration
  - Allow for adaptation, learning
  - Reduce stress on mission-critical production systems

Network Connectivity

- Devices, protocols, media
- Network operations center (NOC) monitors
  - Status of links
  - Status of key devices
  - Bandwidth utilization
- Zigbee standard
  - IEEE 802.15.4 standard
  - Local, ad hoc network connectivity usually applied to M&C
- Need to plan for distributed systems to interconnect

Environmental Concerns

- Physical factors
  - HVAC: Temperature, humidity
  - Electrical power: voltage, amplitude (spikes, brownouts), continuity
  - Fire, smoke, water threats
  - Perimeter breaches (breakins, intruders, vandalism)
- Critical for business continuity (see CSH6 Ch 58)
  - Ideally monitoring & trend analysis provides early warning
  - Allows preemptive action to stop problem or initiate emergency responses

System State

- Critical variable on target system
  - E.g., M&C system for electrical power grid looks at electricity flow & individual components of network (generators, transformers, transmission lines)
- Software *agents* run on target (host) system & report to monitoring hub
- Host intrusion prevention systems (HIPS) monitor nodes in network
  - Centralized reporting
  - Attack correlation
  - Useful data for postmortem analysis

System Components

- Track usage of specific elements
  - CPU
  - RAM
  - Storage
- Operating systems may include resources
- Specialized software available
- Data support trend and anomaly analysis

Process Activities

- Process in particular execution of specific piece of code on specific CPU by specific user at particular time
  - Process = {code X CPU X user X time}
- Every process should be
  - Known
  - Authorized
- Antimalware products monitor for unauthorized processes
- May also monitor processes for *chargeback* systems
  - Organizational users pay for their share of resource investment & operational costs
  - Plus: useful in anomaly detection

File System

- Who is doing what to which data when?
- Helps in diagnosing system / application errors
- Log files have different types of records corresponding to different type of file activities
  - More later….

Access Controls

- Recording who asks for and receives (or doesn't receive) access to resources
  - Critically important for security management
  - May identify malefactors before they can do damage
- Also generally supports resource management
  - Identify anomalies
  - E.g., "Nurse Betty" has been logged on to terminal for 72 hours….

Log Management

- Log Generation
- Types of Log File Records
- Automation & Resource Allocation
- Log Record Security

Log Generation

- Log files are records of *events*
  - Basic building block for M&C systems
  - Digital audit trail
  - Often *not enabled* by default
- Many different types typically available
  - Must *configure* logging appropriately
  - May ignore some events; e.g., opening utility file of no sensitivity
- *Transaction logs*
  - Often store copies of original records
  - Plus copies of change instructions or images of changed records (takes more space)
- Must define policies for *log retention*

Types of Log-File Records

- Log file = audit trail
- Many types (not discussed in detail in this presentation – see 53.5.2.1-18)

System boot	System shutdown	Process initiation
Process termination	Session initiation	Session termination
Invalid logon attempt	File open	File close
Invalid file access attempt	File I/O	System console activity
Network activity	Resource utilization	Central processing unit
Disk space	Memory	

Data Aggregation and Reduction

- Centralized Data Stores
- Filtered Queries
- Analyzing Log Records

Automation & Resource Allocation

- Keeping logs defined, organized and available contributes to effective & efficient system management
- Data retention requirements growing
  - Include log files in policies
- Weigh retention policies and centralization / consolidation policies
  - Scalability important
  - Estimate operational / financial costs of collecting, analyzing & storing logs from disparate systems in central repository

Log Record Security

- Protect log records against unauthorized access
- Methods
  - Access control lists (ACLs)
  - Checksums
  - Encryption
  - Digital signatures
- Chain of custody important
  - Track all transfers
  - Use secure off-site repositories

Analyzing Log Files

- Volume Considerations
- Archiving Log Files
- Platform-Specific Programs for Analysis
- Exception Reports
- Artificial Intelligence
- Chargeback Systems

Archiving Log Files

- Decide how long to keep log files
- Usually legal requirements
- Establish definite policies
- Monitor and enforce
- Safeguard archives (environmentally-sound and secure storage facilities)

Platform-Specific Programs for Analysis

- Each operating system can have particular variations in log file structure
- Look for log-file analysis tools specific for your environment
- GOOGLE provides wealth of references with keywords "operating system log file analysis"
  - AWStats – GNU GPL
  - Argus – Sun Solaris, UNIX variants
  - Sawmill – Web-related files

Exception Reports

- Often impossible to examine all records
  - May be millions of events in single log file
- Need to break out unusual events
- Can set filters to scan for unusual conditions
- Systems define baselines events (the norm) and spot unusual ones
- Human beings often scan the exception reports
- Sophisticated systems use AI to spot patterns and anomalies

http://www.thehousehistorians.co.uk/Images/Books.gif

Artificial Intelligence

- AI systems can be based on statistical quality control (SQC)
- Spot multi-sigma deviations; e.g.,
  - No more than one user logon in a thousand has used an ID from the accounting department between the hours of midnight and 06:00
    - ✓ So why is "Ralph" trying to logon at 03:30?
  - What's more, "Ralph" has not had to try his password more than twice in 1523 logons
    - ✓ So why is "Ralph" trying his 18th password at this time in the morning?
- Can handle more sophisticated patterns

Chargeback Systems

- Log files used to allocate costs to all possible resource utilization; e.g.,
  - $0.00001 /disk I/O;
  - $0.00002/process initiation; etc.
- Users receive itemized bills (e.g., monthly) showing resource utilization
- Promotes optimization with help of users
- Can alert user to unusual events or misuse: "Why is our bill 3 times higher this month??"
  - *Because there's a serious error in your code; or*
  - *Because you've been hacked!*

Protecting Log Files Against Alteration

- Checksums
- Digital Signatures
- Encryption
- Physically Sequestering Media

Checksums

- Can generate *hash total* and append to each record
- Any change that does not use the right algorithm to change the checksum will be identified
- If checksum includes data from previous record, chaining makes changes very difficult for attacker
- Attacker has to recreate entire chain of records starting at modified or deleted one

Digital Signatures

- Can sign an entire file using public key cryptography (PKC)
  - Create checksum
  - Encrypt using a private key
  - Check by decrypting using public key
- Check validity by recomputing signature and comparing value against decrypted original signature
- See next slide for reminder of how PKC works

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 8.1
Comment: Digitally signed by M. E. (Mich) Kabay, PhD, CISSP-ISSMP
```


Encryption

- Can also just encrypt the entire file
- Then an attacker who lacks the appropriate key can do nothing with the file at all except delete it

Physically Sequestering Media

- Same principles apply to log files as to any other form of valuable data
- Can make backups
- Store media in secure, safe storage facilities
  - Access controls
  - Environmentally stable
  - Fire-resistant
- E.g.,
  - Iron Mountain
  - ArchiveAmerica
  - Many others….

Notifications and Reporting

- Alerts
- Trend Analysis and Reporting

Alerts

- Crying “wolf” not good – don’t overwhelm operators with stream of minor alerts
- Judge operational value of information
- Out-of-band monitoring can detect errors undetectable by monitored system itself
- Alerts: email, pager, phone, SMS
- Human Machine Interface (HMI)
  - Situational awareness
  - Virtual buttons, meters, graphs
  - Management dashboard to report on ignored alerts

Trend Analysis and Reporting

- Analyze pace of security improvements
- Consistency of internal controls
- Peaks in violation of security policies between audits – danger sign
- Chargeback (discussed earlier) can spark serious examination of trends
- Exception reports identify anomalies

Monitoring and Control Challenges

- Industrial Control Systems
- Mobile Computing
- Virtualization

Industrial Control Systems (ICS)

- Distributed Control Systems (DCS)
  - Relatively autonomous, little human interaction
  - E.g., oil refineries
- Supervisory control and data acquisition (SCADA)
  - Extensive HMI
  - Direct communication with programmable logic controllers (PLCs)
  - Increasing use of networking
  - Often unsecured logically and physically

Mobile Computing

- Data in transit
  - To/from PCs, laptops, tablets, phones & radio-frequency identification (RFID) systems
  - Often over unsecured channels
  - Must move to virtual private networks (VPNs)
- Data at rest
  - In PCs, laptops, tablet and phones
  - Often unsecured
  - Must move to data encryption
- BYOD: Bring Your Own Device
  - Increasing complexity for sysadmins
  - Wide range of hardware & software to monitor & control

Virtualization

- Virtualization supports hardware sharing
  - Physical hardware
  - Virtualization interface (VI)
  - Virtual machines (VMs)
    - ✓Entire operating systems or
    - ✓Specific applications
- Hypervisors can support different VMs
- Migration
  - VMs can move from hardware device to device
  - Must define and monitor security policies
    - ✓E.g., could prohibit hypervisor from managing internal, high-security systems & public, low-security systems on same hosts

Review Questions (1)

1. How can monitoring system data contribute to information assurance?
2. Which type of log file record includes information about the following events and how can you use these records for IA purposes?
   a) When the system started?
   b) When the system stopped?
   c) Who launched a process and when?
   d) Total amount of various system resources (CPU, I/O, swaps of VM, maximum priority, etc.) used by a process during its lifetime?
   e) Who started a session on the system and when?
   f) Total system activity carried out by a user during a session?
   g) Number of bad passwords entered during logon attempts?
   h) Who opened which file at what time for which purposes?
   i) How much I/O a specific file was involved in while it was open?
   j) Who tried to access files in unauthorized ways?
   k) Detailed records of exactly what information was written into a database?
   l) What messages were sent to the system operator?
   m) Data about Internet connections?

Review Questions (2)

3. Why do most sites no longer worry about the disk space consumed by log files?
4. Whom should you consult when deciding on how long to keep log files? Why?
5. What are exception reports and why do we need them?
6. How can chargeback systems help us improve IA?
7. What mechanisms are there to protect log files against tampering?
8. Why are memory dumps highly sensitive from an IA perspective?
9. Why do we need special diagnostic utilities to navigate through today's memory dumps?