USM IT Security Council

Guide for Security Event Logging

Version 1.1

23 November 2010

1. General

As outlined in the USM Security Guidelines, sections IV.3 and IV.4:

IV.3. Institutions must maintain appropriate audit trails of events and actions related to critical applications and data, as required by state and federal laws/regulations. Further, these significant actions and events must be reviewed and documented.

- Additions and changes to critical applications
- Actions performed by highly privileged users
- Additions and changes to users' access control profiles
- Direct modifications to critical data outside the application

IV.4. Institutions must ensure that all critical systems have the ability to log and report security incidents and attempted violations of system security based on an analysis of the risks to the institution. During the risk analysis process, institutions must determine the method and frequency with which the logs and reports will be reviewed.

This guidance document represents a compilation of some best practices for review and investigation of security logs. Each USM institution should review these best practices and consider implementing them based on an analysis of the risks to the institution.

2. Operating Systems

Operating systems (OS) for production servers, workstations, and networking devices (e.g., routers, switches) usually log a variety of information related to security. OS logs are most beneficial for identifying or investigating suspicious activity involving a particular host. The most common types of security-related OS data are as follows:

- **System Events.** System events are operational actions performed by OS components, such as shutting down the system or starting a service. Typically, failed events and the most significant successful events are logged, but many OSs permit administrators to specify which types of events will be logged. The details logged for each event also vary widely; each event is usually timestamped, and other supporting information could include event, status, and error codes; service name; and user or system account associated with an event.

- **Audit Records.** Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. OSs typically permit system administrators to specify which types of events should be audited

3. Applications

Some applications generate their own log files, while others use the logging capabilities of the OS on which they are installed. Applications vary significantly in the types of information that they log. The following lists some of the most commonly logged types of information and the potential benefits of each:

- **Client requests and server responses**, which can be very helpful in reconstructing sequences of events and determining their apparent outcome. If the application logs successful user authentications, it is usually possible to determine which user made each request. Some applications can perform highly detailed logging, such as e-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail; Web servers recording each URL requested and the type of response provided by the server; and business applications recording which financial records were accessed by each user. This information can be used to identify or investigate incidents and to monitor application usage for compliance and auditing purposes.

- **Account information** such as successful and failed authentication attempts, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. In addition to identifying security events such as brute force password guessing and escalation of privileges, it can be used to identify who has used the application and when each person has used it.
- **Usage information** such as the number of transactions occurring in a certain period (e.g., minute, hour) and the size of transactions (e.g., e-mail message size, file transfer size). This can be useful for certain types of security monitoring (e.g., a ten-fold increase in e-mail activity might indicate a new e-mail–borne malware threat; an unusually large outbound e-mail message might indicate inappropriate release of information).

- **Significant operational actions** such as application startup and shutdown, application failures, and major application configuration changes. This can be used to identify security compromises and operational failures.

Much of this information, particularly for applications that are not used through unencrypted network communications, can only be logged by the applications, which makes application logs particularly valuable for application-related security incidents, auditing, and compliance efforts.

Each institution should consider applying these measures to better protect their systems against threats and possible auditor comments. Additionally, any test, development and QA environments should be monitored if any sensitive data is being used.

4. Databases

Database systems generate their own log files that are useful for security. The following lists some of the most commonly logged types of information and potential benefits of each:

- Account information such as failed login attempts, account changes (e.g. creation of new accounts, deletion of accounts, changes in assigned roles) and use of privileges. Both user and system accounts activities should be logged and reviewed.

- Security events (e.g., grant/revoke/deny, role add/remove/configure), audit events (e.g., add audit, modify audit, stop audit), and server events (e.g., shutdown, pause, start), failed login attempts.

5. Log format

Minimally each event being logged should contain the following elements:

- Data and time of the event
- User ID person performing the action
- Type of event
- Asset or source name and type of access
- Success or failure of event
- Source (terminal, port, location, IP address) where technically feasible

6. Alerts

Alerts should be constructed and sent automatically to appropriate parties as the institutional decides are appropriate. Each alerts should be logged and actions immediately taken to investigate and resolve the incident. Typical alerts to consider include the following:

6.1. General Alerts

- UPS equipment warnings
- Room alarms such as temperature, room access, intrusion detectors, etc.
- Disabling or attempts to disable logging
- Utilization rates over 90%
- Equipment temperature exceeds 90%
- # of errors every 5 minutes

6.2. Firewall Alerts

- Firewall failover/reboot
- Direct connections to firewall
- Translation errors

6.3. IDS Alerts

- Equipment failure
- Direct connections to IDS

6.4. Network/critical infrastructure Alerts (usually routers)

- Hardware failures related to memory, disk storage or processor performance
- Denied admin connection attempts
- Direct connections to routers

6.5. Host Alerts

- After a certain number of login failures per person/system
- Shutdown, pause or restart of servers
- Stop or pause of computer processes

6.6. Workstation Alerts

6.7. Database Alerts

- Failed login attempts for user and system accounts
- Stop, pause or restart of databases

6.8. Application Alerts

- Failed login attempts for user and system accounts
- Stop, pause or restart of applications

7. Reports

Automated weekly reports should be constructed for monitoring routine security occurrences. Each report should comply with the format as specified in the Maryland DoIT security policy and USM Security Guidelines. Typical reports to consider include the following:

7.1. General Security Report

- Brute force password attacks
- Emergency actions performed by administrators on highly privileged system or security resources
- Actions performed by system operators, system administrators and system engineers
- Any unauthorized attempts to modify software or to disable hardware configuration
- Two or more failed attempts to access or modify confidential information within a week

- Two or more failed attempts per system/day to access or modify security files, password tables or security devices
- Web server attacks
- P2P file sharing activities
- Backdoor attacks (Trojans, rootkits, etc.)
- Failed logins
- User account lockouts
- Excessive number of emails sent over given time from single source (mass mailing worm)
- Domain/audit policy modifications or changes
- System access granted to an account
- Changes to Windows local groups
- Attempts to change or delete audit logs
- Rouge WAPs

7.2. Firewall Reports

- Configuration rule changes to the firewall
- Failed logon attempts to the firewall

7.3. IDS Reports

- Attempts to evade IDSs
- DoS and buffer overflow attacks

7.4. Critical Network Infrastructure Reports

- Failed and successful login attempts
- Network configuration changes

7.5. Host Reports

- Escalation of host privileges

- Malware infected hosts not cleaned
- Web-based attacks (XSS, SQL Injection, etc.)

7.6. Workstation Reports

- Malware infected computers not cleaned

7.7. Database Reports

- Creation of new accounts
- Deletion of accounts
- Changes to assigned roles and privileges
- Direct additions, deletions or modifications to critical tables (does not include changes made via normal production programs)
- DBAs and developers making changes to critical tables (such as grades, student enrollment, payroll, etc.)
- Escalation of host privileges
- The use of critical privileges and objects
- Changes to audit events (modify audit, stop audit)

7.8. Application Reports

- Creation of new accounts
- Deletion of accounts
- Changes to assigned roles and privileges
- Escalation of host privileges

8. General logging

All USM institutions should develop retention policies or guidelines for logs, security reports and investigations.

Each institution should consider logging other activities that include port or network scans that include possible attack/exploitation, etc. These may or not require any action taken as determined by the institution.

Firewall log messages can be numerous and hard to manage. Therefore, institutions should consider determining which ones have to do with connections to firewalls themselves and change the specific messages to allow them to be received. This will reduce the volume of messages received from the firewall and allow more effective logging.

Logs should not be kept on the related device but on a separate syslog server or Security Information Event Management system. Logs should be retained according to the institutional policy or guideline. This is to allow analysis of events and troubleshooting of network or system problems.

There should be an independent review of the alerts and reports generated from the logs with follow-up and investigation of questionable items. Reviews and investigations will be documented and retained according to the institutional policy or guideline.

References:

- NIST SP 800-92, Guide to Computer Security Log Management
- Maryland Department of Information Technology Information Security Policy, version 2.3, dated September 2010