Auditing Data Access

2nd Nationwide Health Information Network Forum:
Health Information Network Security and Services
October 16-17, 2006

Houtan Aghili, PhD
Perry Vessels
IBM

Why Audit

- Assess user accountability
- Determine damage assessment
- Determine causes of security violations
- Assess security state of environment
- Determine if system enters unauthorized state
- Evaluate effectiveness of protection mechanisms
- Assess appropriateness of mechanisms
- Deter attacks because of presence of record

Scope of Audit

- **Who are you trying to monitor, deter or catch (hold accountable or prosecute)?**
  - Users
  - Admins
- **What problems are you attempting to find or analyze?**
- **What laws, regulations or policies are you required to follow?**

Structure of an audit system

- **Logger**
  - Records information
- **Analyzer**
  - Correlation and analysis of logged information looking for pertinent events
- **Notifier**
  - Historical results reporting
  - Specific event notification

Levels of Audit

- **Application level**
  - Transaction based
  - Strong user association
- **Services/middleware level**
  - Support services for applications, e.g. DBMS
- **Operating system level**
  - Memory management, scheduling and process control
  - File access
- **Network level**
  - Border gateways, firewalls, and intrusion detection systems

What should the audit contain?

- **Parties involved**
  - Clinicians
  - Patients
  - Proxies/Guardians (on behalf of…)
  - Trusted Processes (on behalf of…)
- **Trusted timestamps**
- **Sequence numbers**
- **Transaction ID**
  - Binding audits across systems
- **Requested action**
- **Result**

Requirements of an Audit System

- Trustworthy
- Reliable
- Never be bypassed
- Positive and negative events
- Analyze data from various levels

Audit Design

- **Centralized or Distributed**
  - *Distributed*: Audit collection and analysis takes place on each system or application; usually using tools built into each specific product
  - *Centralized*: Audit collection takes place at individual systems or application but is collected or sent to a central location for analysis
- **Multiple Levels or Single**
- **Assurance Tradeoffs**
  - Reliable transmissions
  - Digitally signed records
  - System reliance
    - Will system continue when audit is not accessible?

Distributed Pros and Cons

- **Pros**
  - No additional equipment required
  - Reduced network traffic
- **Cons**
  - Individual device storage and archive management
  - Review and analysis performed at many locations
  - Potential for alteration of audit by system intruder or rogue administrator

Centralized Pros and Cons

- **Pros**
  - Audit can be correlated from many sources
  - Single storage and archive management
  - Review and analysis performed at single location
  - Real time transmission can prevent audit alteration by system intruder or rogue administrator
- **Cons**
  - Additional equipment required for storage and processing
  - Increased network traffic
  - Increased processing on collections systems dependent on transmission and data security

Hybrid: Distributed and Centralized

- **Distributed systems collect, analyze and filter based on rules provided by centralized systems**
- **Centralized system correlates, analyzes and fine tunes rules**
- **Pros**
  - Processing split across systems
  - Data and network load can be reduced
  - Could function across enterprise boundaries
- **Cons**
  - More work and standards needed