Audit logs at an academic medical center

_Soumitra Sengupta_

Associate Clinical Professor,
Dept of Biomedical Informatics, Columbia University
Information Security Officer, NewYork-Presbyterian Hospital
and Columbia University Medical Center

SITH 2, May 2012
NewYork-Presbyterian Hospital, Columbia University Medical Center, Weill-Cornell Medical College

• Largest tertiary care in New York City (Rank 6th, 8th, 16th)

• Complex
  – Goals: Care, Research and Education
  – Different boards
  – Physicians, students, researchers, staff in the Universities
  – Residents, nurses, techs, staff in the Hospital (in and outpatient)
  – Faculty Practices represent University private office (outpatient) business
  – Centralized IT in NYP, Decentralized in the Universities: Control, standardization, heterogeneity are issues
  – HIPAA legal standing: Organized Health Care Arrangement

• Hundreds of applications for care and research
Accidental leakage of sensitive information (phi, pii, pci) to a public environment such as the Internet

✓ Stolen or improperly modified sensitive data by external hackers using public access (the Internet or the wireless)

Loss of sensitive information at a business partner organization

✓ Accidental changes or destruction of sensitive information

Significant system downtime due to malware outbreak

✓ Improper sensitive information access of famous people such as celebrities or public figures or colleagues, relatives and acquaintances by internal users

✓ Improper change of sensitive information by internal users for fraudulent reasons

Environmental failures due to natural or man-made disasters

Participation in a SPAM ring, or Denial-of-service attack, or Copyright violation due to a Bot infection

Loss or theft of physical device that contains sensitive information (phi, pii) that requires breach notification per regulatory requirements

✓ Stolen or improperly modified sensitive data by internal hackers using wired network

Copyright violations cause NYP to lose "safe harbor status" and thus can be fined by copyright holders
Threats for Clinical Data

• Big spills
  – Theft at large (identity, medical identity)
  – Accidental loss (unencrypted device/storage, web + Google/cloud)
  – Malicious hack activities (internal or external)

• Relatively smaller scope
  – Targeted, malicious access (child custody, divorce, court cases)
  – Celebrity snooping
  – Acquaintance/colleague snooping

• Solutions are statistical analysis of aggregated Audit logs (the next day)

• Techniques are detective, with follow up investigation
  – 100+ investigations per year (for 6 years)
  – Lack of standards on audit logs is a serious problem
Standards for clinical application audit logs

  - Log infrastructure, planning, operational procedures
  - Information system access review (HIPAA)
  - Process focused, but not content of the logs
- Audit Trail and Node Authentication (ATNA) from Integrating the Healthcare Enterprise (IHE)
  - RFC 3881 (2004!)
  - XML schema
  - NTP
ATNA Standard

• Security administrative events, Audit access events, Security-mediated events
• Patient care data events
  – What was done (Action, Data; borrows from HL7, DICOM)
  – By whom (UserId)
  – Using which resources
  – From what access points (IP addresses, workstation names)
  – To whose medical data (PatientId)
• FairWarning lists 50+ application audit logs
  – including ATNA log format as a separate instance
  – Most vendors do not follow ATNA standard