University of Waterloo

CS 898 Health Informatics

Security - Access Control & Role Management

Maxwell Young

Security – A Practical Concern?

- (1996) Health worker in Florida brought home names of 4000 HIV+ patients and sent names to newspapers.
- (1999) Univ. of Michigan Medical Center patient records open to the public via the Internet. Server thought to be password protected – it wasn't.
- (2000) Hacker stole 5000 cardiology and rehab patient records from Univ. Washington Medical Center
- (2000) Private correspondences of Kaiser Permanente (California based managed care institution) sent private correspondence of more than 850 members to ~19 people
- (2002) Recipients of kidneys learned names of deceased donors due to a mistake by Univ. of Minnesota researchers.

Incidents reported in: "A review of security of electronic health records", Khin Than Win, 2005.
And "Medical Privacy Stories", Health Privacy Project

General Overview

- Introduction to Security
  - “Perfect” security is a fiction
  - Goals of security in health informatics
- Access Control
  - Challenges for health informatics
  - Standard methods for access control
  - Role Management as a solution
- Auditing
  - What is it?
  - Examining how exception mechanisms are used
- Network Deployment
  - Centralized vs distributed
  - OASIS and Cassandra
  - Access over the Internet
- Authentication Mechanisms
  - Biometrics: pros and cons

Introduction to Security

Image taken from: www.security-management-systems.co.uk

Security - what are we talking about?

- Data security concerns in general:
  - Access Control
  - Anonymity
  - Corruption, recoverability, standardization, etc.

- All such issues are related
  - Interested in access control and role management
  - Threats include system penetration, data theft, data corruption, abuse of data, etc.
  - Dealing mostly with “inside attacks” – although we deal with some “outside attack” issues – and there is the issue of everyday mistakes

How Secure is Secure?

- “Perfect” security is a myth
  - Encryption: can be broken, misused, outdated
  - Trust: an entity (CA), a conjecture on hardness
- We need to be concerned with retroactive solutions
  - Can we detect bad events?
  - Can security be extended to protect against new threats?
- Security policy to define what is protected
  - Threat and Risk Assessment methodology is formalized, for example by Canadian Security Establishment (CSE)

Access Control

Past and Present Techniques

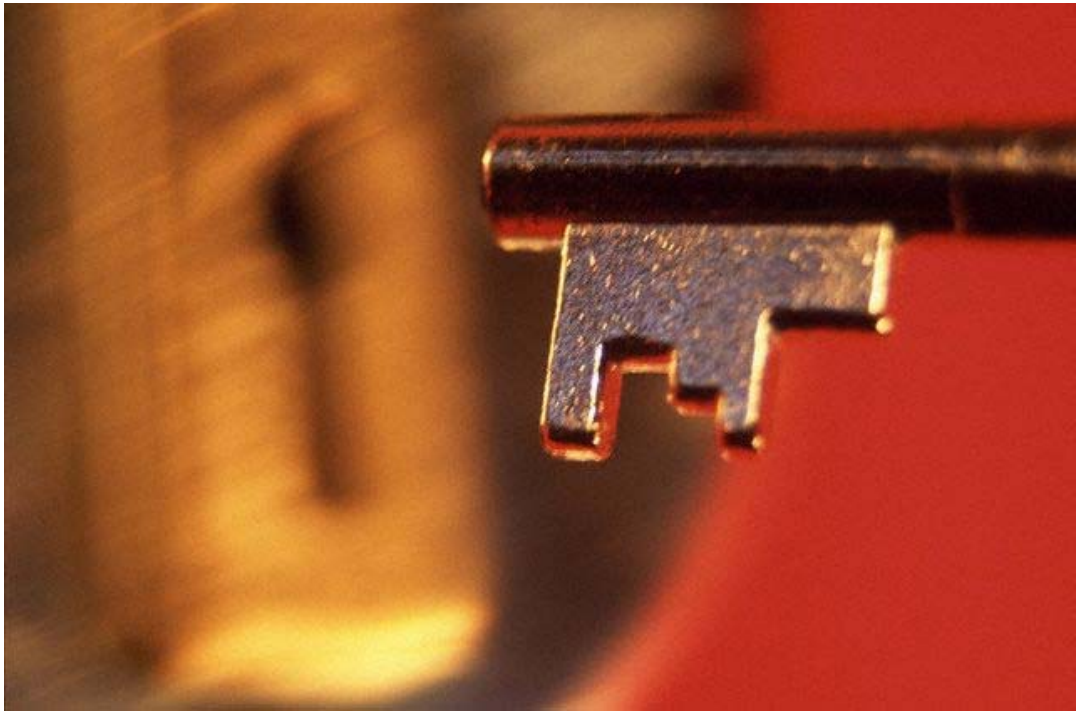


Image taken from: www.indentsolutions.com

Access Control – What is it?

- Access to protected information is restricted to those people who are authorized to access it
  - Authentication to verify your identity
  - Access control used heavily in the military
  - Technology does not necessarily make security easier

"Before I kill a hundred million people, I wanna get somebody on the ****ing phone"

- from the movie *Wargames*

- Similarities in the challenges faced
  - Human factor
  - Need to authenticate quickly
  - Need an extremely secure system
  - Consequences of failure are extreme

Access Control – Examples

- Eric Williams (1997):
  - Dallas Cowboys football player injured in a car accident. Blood alcohol level in dispute.
  - Medical records accessed via computer by unauthorized personnel, leaked to media.
  - "Curiosity. I'm a Cowboy fan. I had season tickets to the Cowboys."
- Patricia Galvin (2001):
  - After fiance's death, subsequent sessions with psychologist.
  - Session data given to insurance company, turned down for compensation after being rear-ended in a car accident

Incidents reported, respectively, at Information Systems Ethics (cyberethics.cbi.msstate.edu/mason2/williams.htm) and Institute for Health Freedom (http://www.forhealthfreedom.org/Newsletter/January2007.html)

Access Control - Threats

- Patient data used:
  - To satisfy curiosity
  - For economic gain
  - Many others…
- Who would like to see patient data?
  - Media
  - Insurance corporations
  - Research institutions
  - Pharmaceutical companies
- Consequences:
  - Degraded patient care – retroactively changing data, patients not disclosing info
  - Legal ramifications – ownership issues, corporation changes
  - Lack of faith in the medical system

Access Control

- Restrict access to a computer based resource
  - Who can access data – people, other systems, individual processes, etc.
  - Type of access – read only, remote vs. on-site, etc.
  - Dynamic – privileges granted and revoked
- What kinds of standards?
  - Trusted Computer System Evaluation Criteria (TCSEC)
    - Computer security control standards developed by DoD (1983)
  - Information Technology Security Evaluation Criteria (ITSEC)
    - European (Germany, UK, France, Netherlands) version (1990)
  - Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
    - Developed by CSE (1993)
- All replaced by the Common Criteria which is an international standard

DAC & MAC

- Two main types in the past:
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
- DAC:
  - User is thought to “own” data that is protected
  - Access control whereby privileged users can confer privileges to other users arbitrarily
  - Flexible (if you’re not too paranoid)
- MAC:
  - Do not have ability to confer privileges (administrative security policy)
  - Common technique is to assign sensitivity labels to all persons and all data
  - Sensitivity label of person must meet or exceed requirement of sensitivity label on data
  - OS Berkeley Software Distribution (TrustedBSD)
- Are DAC or MAC appropriate for, say, a hospital setting?

Role-Based Access Control (RBAC)

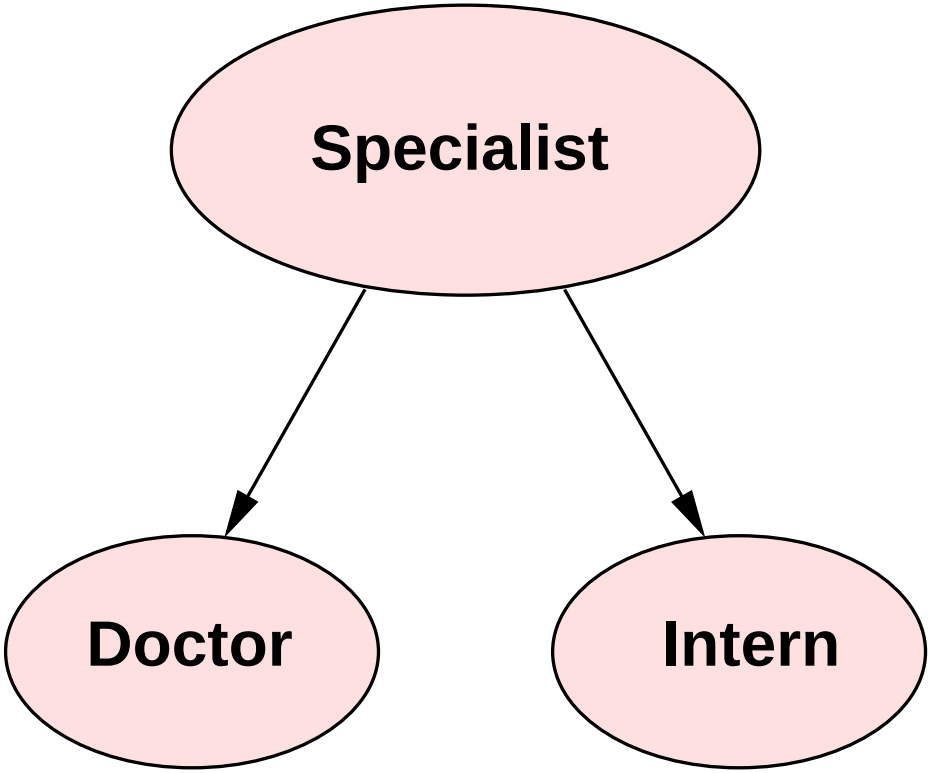
- More recent development than DAC and MAC
- Construct roles for all job positions and assign staff to these roles – more than 1 role possible
- Access rights are based on the “role” of the individual (doctor, nurse, intern, etc.) – can be fine grained
- Examples:
  - Doctor can prescribe medication to patient A but not patient B
  - Researcher can collect and analyze anonymous data on a subset of patients
  - Nurse restricted from viewing electronic health records of individuals not under his/her care

Advantages of RBAC

- Some advantages:
  - More natural to a business environment (vs military)
  - Individual rights can be simpler to manage
  - Do not have to administer on object-by-object basis
  - Can handle heterogeneous situations
    - Staff from different institutions
  - Already incorporates the level of access to data with fine-grained control and meaning:
    - MAC: a file might be read-only (fine grain)
    - RBAC: type of changes can be restricted to particular operations ie. inputting new experimental data based on your role as a researcher

RBAC Organization

- Roles can have overlapping privileges, many different roles
  - Hierarchy required to organize roles



RBAC

- Can purchase RBAC software – National Institute of Standards and Technology (NIST)
  - Standardized
  - This is state of the art

Audit Trails

Monitoring Access

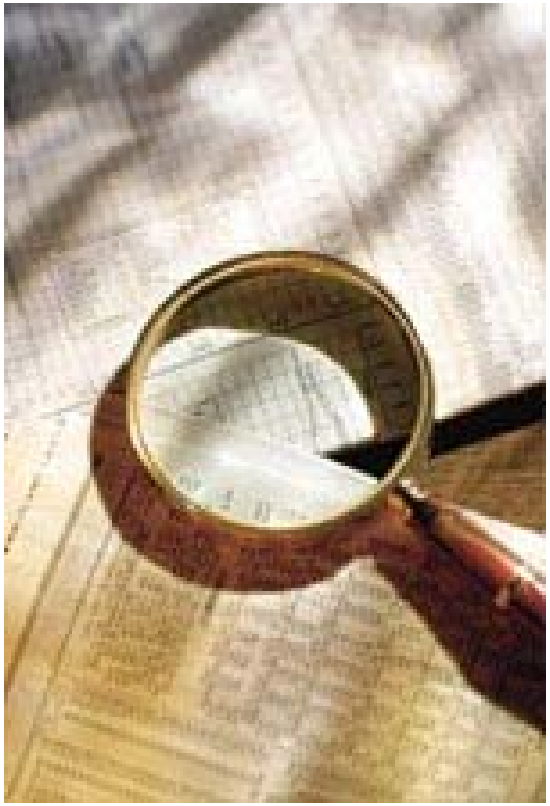


Image taken from: www.petersonco.com

Audit Trails

- “Rules are mostly made to be broken…”
  - General MacArthur
- Misuse of access privileges
  - Detection after the fact
  - Log of which individuals have accessed which information (records modifications)
  - More critical roles/instances audited more closely
- Example from paper: resident physician learned of nurse’s pregnancy

Emergency: Violating RBAC

- Problem: audit trails can contain so much information as to make human review impossible impractical
  - Information for access can be vague
  - Concise but also unreadable
- RBAC must be flexible to be used in healthcare:
  - Emergency situations may require bypassing usual access control
  - Dynamic events: patient transfer, doctors asking each other for second opinions
- Need an “exception mechanism”
- Clearly an exception mechanism is highly susceptible to abuse

Exception Mechanism Use

- Study conducted in Norway:
  - Data from Central Norway Health Region (CNHR)
  - Audit trails from 8 hospitals using RBAC
  - Data over 1 month (March 2006)

- Exception mechanism for access:
  - *Actualization:* user has access to a patient's EHR that is not available through normal access control in a single domain. Reason must be provided (8 predefined reasons or can make your own)
  - *Emergency Access:* user can open a single document in patient's HER – has to be used on a single document, but can access multiple domains. No predefined reasons.

"A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs", L. Rostad and O. Edsberg, 2006.

Exception Mechanism Use

- Who can do what?
  - # Users actualization permission: 74% (12,298)
  - # Users emergency permission: 0.25% (41)
  - # Total Users: 16, 723
- What percent of EPRs were accessed using:
  - Actualization: 54%
  - Emergency: 0.07%

Exception Mechanism Use

- Emergency access:
  - Numbers too low to analyze – seems reasonable
  - Only a relatively few number of people have this capability
- But actualization used to frequently to be considered an exception!
- Percentage of people with actualization capability should reflect perceived need for this ability

Break Down of Use

Role	Count	% Act	% Use
Nurse	9,234	61	22
Doctor	2,957	99	52
Health Secretary	1,934	97	51
Psychologist	196	99	57

Break Down of Use

Ward	Users	% Act	% Use
Medical (18)	2,834	86.9	49.8
Surgical (21)	2,150	75.2	33.2
Anaesthesia (8)	629	99.5	30.3
Emergency (10)	482	71.1	27.6
Out-Patient (43)	473	99.7	62.6

Break Down of Use

- Only 8% of reasons were self-defined
  - Other predefined reasons are less specific
  - Most common reasons were: physician referrals, handing over info to other health personnel on request, request for info by patient or next of kin, release info to insurance or legal entities, patient not properly registered
  - Should be integrated into normal access control
- Why do so many people have actualization capability?
  - By minimizing actualization, can cut down on audit file sizes

Network Deployment Issues

Image taken from: www.atariarchives.org/deli/computer_networking1.jpg

RBAC: Centralized versus Distributed

- A centralized system is “simple”:
  - Single administrative domain specifying security policy
  - Status of all users is known
  - Little to no heterogeneity: records are standardized
- A distributed system:
  - Network dynamics not as easy to observe
  - Scalability becomes a problem
  - Standardization
  - Many other large scale engineering issues…
- A distributed system is very realistic since even on a national level, interoperability between different systems will be required
- Very few implementations – two in the literature: OASIS and PERMIS

Example Systems: OASIS

- Open Architecture for Secure Interworking Services
  - Is a role-based access control model developed at the Cambridge Computer Laboratory (1996)
  - Distributed architecture: no central policy, no global name space, incorporates many administrative domains, etc.

- Devised as a prototype for managing EHRs with RBAC
  - Uses X.509 certificates, public key infrastructure
  - Handles heterogeneous data sources (basic interoperability is all that's required), different health care organizations can ``tune'' their own policies
  - Just the first steps, no specific administrative tools yet developed, no convenient auditing interface (no merging of audit data)

"OASIS role-based access control for electronic health records", D. Eyers, J. Bacon and K. Moody, (2006)

Example Systems: PERMIS

- PrivilEge and Role Management Infrastructure Standards validation (Univ. of Salford)
  - Another distributed access control architecture
  - Also uses PKI
- OASIS vs PERMIS:
  - Authors confess little difference
  - Persistent vs dynamic roles
    - PERMIS: roles are generic categories (ie. doctor)
    - OASIS: roles are appointments (doctor on duty requires initial credential “employed-as-doctor”)

“The PERMIS X.509 Role Based Privilege Management Infrastructure”, D. Chadwick and O. Otenko, (2002)

Policy Languages for RBAC

- How to develop a security policy over a large, *distributed* system
  - Want a standardized language
  - Scalability: systems can be numerous, lots of data
  - Can specify complicated role hierarchies
  - Revocation and delegation of privileges

- Examples:
  - Cassandra: rule based (310 rules) and 58 roles
  - Ponder, Rei are other languages

"Cassandra: Flexible trust management, applied to electronic health records", M. Becker and P. Sewell, (2005)

Accessing EHRs over the Internet

- Patients have the right to view/amend their medical records (in most circumstances)
  - “Enhance” doctor-patient relationship
  - Demystify own condition
- (UCSD, 2002) PCASSO: Patient-Centered Access to Secure Systems Online
  - Secure communication of health information over Internet
  - ID and Password confirmation
  - Doctors can deny patient access to records in cases of communicable diseases, mental health reasons, etc.

Authentication Mechanisms

Beyond Passwords

Image take from: www.techsvg.com

Access Control - Authentication

- Passwords are a common form of access control
  - Easily forgotten – time consuming to recover
  - Not sufficiently difficult to break
  - Need to be changed regularly
- Biometric Identification:
  - Sharing something you know vs. something you are
  - Stable in comparison to, say, home address
  - Fingerprints, facial recognition, retinal scan, signature recognition, etc.
- Have been employed in limited fashion for access control purposes in hospitals

Access Control - Biometrics

- Biometrics company Ultra-Scan
  - Patient identification through finger-print scanning
  - Catholic Health System, Buffalo, N.Y.
  - Used initially in methadone clinic
  - Take 2-3 fingerprints on left and right hands to set up patient in the system
  - Fingerprint data is stored in such a way as to prevent reproduction of original fingerprint
- St. Vincent's Hospital
  - Electronic signatures
  - Fingerprint authentication for single-sign on

Access Control - Biometrics

- Other examples:
  - UC Davis Medical Center
    - Voice recognition, badges around the neck responding to verbal commands
    - Uses Wi-Fi over wide area network, calls between badges
    - Avoids problems of interference from cell phones
    - Developed by Vocera
  - Rex Healthcare (N. Carolina)
    - Developed by Schlage
    - 39 Hand-key terminals (hand verification, <1 sec)

Info from: “Biometrics in Computerized Patient Record”, slides by Qi Ling and Temo Bardzimashvili, “Schlage Recognition Systems Biometric HanReaders Secure 3,500 Employee North Carolina Hospital”, http:recognitionsystems.schlage.com and “Vocera brings ‘Star Trak’ to the enterpris”, Infoworld.

Biometrics: Obstacles

- Signatures can be forged
  - Even with hundreds of documents having been scanned, recognition is not perfect
  - False positive: 20% (50% if experienced forger)
  - False negative: 1%
- Voice recognition, retinal scan, fingerprinting, etc. all suffer from similar problems
- Wear and tear on technology

Access Control Authentication

- Radio-Frequency Identification (RFID) chip
  - Small: can be implanted under the skin, can't feel it
  - Emits a 16-digit identification number
  - Read up to 10 cm away
  - Can be used to access medical record of unresponsive patient
  - Used by US military
- Boston's CareGroup Healthcare System
  - Called a VeriChip made by Applied Digital in Florida
  - Would cost patients $200

Story "Implantable RFID Chip Takes Root in CIO ... Literally" from: http://www.mywire.com/
US Military: http://www.embedded.com/showArticle.jhtml?articleID=10700142

Concluding Points

- Health informatics poses its own challenges for access control
  - RBAC is a good start, but issues of exception mechanisms, dynamism
- Audit trails are invaluable, but:
  - Time intensive to review; this could be reduced
- Implementing RBAC poses many large scale engineering problems
  - Interoperability and standardization
- Biometrics offers many advantages, but:
  - Comes with own security problems

Some References

- Daniel Masys, Dixie Baker, Amy Butros and Kevin Cowles. "Giving Patients Access to their Medical Records via the Internet: the PCASSO Experience". Journal of the American Medical Informatics Associatino, 9:2, 2002.
- Stephen Ross and Chen-Tan Lin. "The Effects of Promoting Patient Access to Medical Records: A Review". Journal of the American Medical Informatics Association, 10:2, 2003.
- Khin Than Win. "A Review of Security of Electronic Health Records". Health Information Management, 34:1, 2005.
- Lillian Rostad and Ole Edsberg. "A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs". Proceedings of the 22nd Annual Computer Security Applications Conference, 2006.
- R. Brandner, M. van der Haak, M. Hartmann, R. Haux and P. Schmucker. "Electronic Signature for Medical Documents - Integration and Evaluation of a Public Key Infrastructure in Hospital". Methods of Information in Medicine, 41: 321-330, 2002
- Randolph Barrows and Paul Clayton. "Privacy, Confidentiality, and Electronic Medical Records". Journal of Medical Informatics Association, 3:139-148, 1996.
- Ab Bakker. "Access to EHR and Access Control at a Moment in the Past: a Discussion of the Need and an Exploration of the Consequences". International Journal of Medical Informatics, 73:267-270, 2004.
- National Institute of Standards and Technology. "An Introduction to Role-Based Access Control", 1995.
- Suzy Buckovich, Helga Rippen and Michael Rozen. "Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information". Journal of Medical Informatics Association, 6:122-133, 1999.
- E. Smith and J. Eloff. "Security in Health-Care Information Systems - Current Trends". International Journal of Medical Informatics, 54: 39-54, 1999.
- Richard Scott, Penny Jennett and Maryann Yeo. "Access and Authorisation in a Global e-Health Policy Context". International Journal of Medical Informatics, 73: 259-266, 2004.