Information Labeling in Healthcare Systems
The Open Group Labeling Task Group
San Diego, CA
May 1, 1998
Agenda

• “Labeling” Issues
• What Label-Based Access Control (LBAC) Offers to Health Care
• PCASSO™: A Work in Progress
“Labeling” Issues

1. Can/should healthcare information be “compartmentalized?”
   – Hierarchically (sensitivity “levels”)
   – Vertically (categories)

2. Is label-based access control (a.k.a. mandatory access control) useful to healthcare?
Perspectives: Legislation

- Two Federal statutes establish special rules for protecting the records of patients seeking drug or alcohol abuse treatment.
- Many states have designated classes of information that require special protections:
  - “Deniable” (Institute of Medicine) information includes abortion, adoption, mental health, HIV/AIDS, sexually transmitted diseases, substance abuse, “celebrity”
Perspectives: Patient Advocates

- Privacy advocates argue that all identifiable healthcare information is sensitive and should be protected equally.
- “Special category” group advocates argue for special protections (e.g., HIV/AIDS, mental health).
Perspectives: HHS

- HHS (Privacy Advocate John Fanning) has taken the position that:
  - No distinction should be made among types of medical information
    - Largely based on data management challenges
  - But, providers should be granted access only to those types of information they need to do their job
Sites surveyed identified 4 classes:
- Public
- Internal confidential
- Confidential patient record
- Highly sensitive patient record

“Cannot ignore the possibility that individuals may be discriminated against on the basis of specific illnesses or conditions”

“Policy makers must assume that such discrimination is likely to continue in the future, particularly in light of the additional genetic information”

“...may well wish to limit the dissemination or availability of information that might be embarrassing (e.g., …sexually transmitted diseases, …depression, or …alcoholism)”
Perspectives: Behavioral Observations

- In past 2 weeks:
  - At HII98, several patients gave testimonials on how they used the Web to investigate their own health problems -- none involved “deniable” conditions
  - At Faulkner and Gray Healthcare Security Conference, physician giving testimonial on his use of email explained that only his HIV/AIDS patients demanded the use of public-key-based authentication
Perspectives: My Position

• “Special categories” of health information need to be given more rigorous protection than “standard” information
  ➞ Would you want your genetic information protected the same as the results of your allergy screening?

• Further, “special categories” of executable code and system data need to be given more rigorous protection than “standard” applications
Label-Based Access Control

• Called “Mandatory Access Control” (MAC) in *Trusted Computer Systems Evaluation Criteria* (TCSEC)

• Access decision based upon set of rules enforced by the system (OS, DBMS, network)
  – Contrast with Identity-Based Controls (a.k.a., “Discretionary,” or DAC), in which access decision is made by the user

• Labels stored in system data structures protected from users
LBAC/MAC Policy

- David Bell & Leonard LaPadula (MITRE Corporation) formally defined MAC policy
  1. Simple Security Rule: No read up.
  2. *-Property: No write down.

- #1 restricts the flow of data from higher levels of sensitivity to lower levels
- #2 protects the integrity of “mission-critical” data -- for example, system executables labeled “low” to protect from malicious application code
## DOD Access Control Matrix

<table>
<thead>
<tr>
<th>Horizontal Sensitivity Levels</th>
<th>Vertical Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Secret</td>
<td>A</td>
</tr>
<tr>
<td>Secret</td>
<td>B</td>
</tr>
<tr>
<td>Confidential</td>
<td>C</td>
</tr>
<tr>
<td>Unclassified</td>
<td>D</td>
</tr>
</tbody>
</table>

...  

n
## Commercial Enterprise Access Control Matrix (example)

<table>
<thead>
<tr>
<th>Horizontal Sensitivity Levels</th>
<th>Vertical Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Home Office</td>
</tr>
<tr>
<td>Executive Officers</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td></td>
</tr>
<tr>
<td>Employees</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
</tbody>
</table>
## Healthcare Access Control Matrix (example)

<table>
<thead>
<tr>
<th>Horizontal Sensitivity Levels</th>
<th>Vertical Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Abortion</td>
</tr>
<tr>
<td>Highly Sensitive</td>
<td></td>
</tr>
<tr>
<td>Patient Confidential</td>
<td></td>
</tr>
<tr>
<td>Internal Confidential</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
</tbody>
</table>
The Open Group

Windows 3.1
Windows 95
Mac OS

Data General AOS/VS
Digital Open VMS
IBM MVS with RACF
IBM OS400
Microsoft Windows NT Version 3.5
(Version 5.0, SQL Server in eval)
...

ATT SystemV/MLS
MVS/RACF
Trusted Oracle7
Informix On-Line Secure
Sybase Secure SQL Server
Digital SEVMS
HP-UX BLS
IBM MVS/ESA
Silicon Graphics Trusted IRIX/B
...

TIS Trusted Xenix
General Kinetics VSLAN
HFSI XTS-200
Data General DG/UX (in eval)

Boeing MLS LAN
Gemini Trusted Network Processor

For complete Evaluated Product List, see
http://www.radium.ncsc.mil/tpep/epl/epl-by-class.html

Trusted Systems

Fundamental architectural deficiencies (no hardware protection of the OS, no process isolation)

Authentication
Identity-based access control
Auditing
Object Reuse

Label-based access control

Trusted path for login
Least privilege
Covert storage channel controls

Extended trusted path
Covert timing channel controls

Real-time audit notification
What Can LBAC Provide for Healthcare?

• LBAC can be used to provide separation between sensitivity levels
• LBAC can be used to implement Role-Based Access Control (RBAC)
• LBAC can be used to provide containment of user actions (similar to JVM concept): user processes executing within a single
  ➔ More robust systems
The Open Group

PCASSO™
(Patient Centered Access to Secure Systems Online)

- Research project funded by NIH’s National Library of Medicine (NLM)
  - Health Applications for the National Information Infrastructure (NII) Initiative
- SAIC partnered with UCSD School of Medicine and Healthcare Network
- Purpose: To enable secure use of the Internet to access sensitive patient information
Design Constraints

- Architecture must be generalizable and adaptable to broad range of clinical environments.
- Usability and protection features must be acceptable to both caregivers and patients.
- Client users should not need to purchase any special hardware or software to use PCASSO.
Design Elements

User Roles:
1) Primary Provider
2) Secondary Provider
3) Emergency Provider
4) Patient
5) Researcher

Data Sensitivity Levels:
1) Patient Deniable
2) Guardian Deniable
3) Public Deniable
4) Standard
5) Low
Security Policy for Model System

• Researchers can view non-patient-identifiable data
• Patients can:
  – View their own data
  – Review audit trail
• Providers can take actions with respect to their patients
  – Secondary providers can view their patients’ data
  – Primary providers can view their patients’ data, plus:
    • Upgrade data
    • Downgrade data (but not below patient-identifiable)
    • Give other caregivers a provider role
  – Emergency providers can view their patients’ data, but:
    • For a limited period of time
    • With additional monitoring and misuse detection
PCASSO™ Design

PCASSO server runs on Data General B2 DG/UX Platform, retrieves data from Trusted Oracle 7 CDR, enforces role-based security policy.

Client application in Java applet

PCASSO importer/loader labels HL7 messages.

User’s public/private keys and certificate stored on diskette; user authenticated via password and challenge-response.

Intrusions, misuse detected by Computer Misuse Detection System.
Role = (Level, patientID, privilege_set, expiration)
PCASSO Use of LBAC

- To enforce separation of sensitivity levels
  - “Hierarchical” relationship among sensitivity levels
  - Vertical categories are recommended -- but not implemented in model system (so far)
  - “Tranquility” is not enforced -- can switch levels during single login session

- To provide containment
  - Minimize threat to those similarly authorized
  - Minimize exposure should “something go wrong”

- To provide integrity protection for critical system code
Server Assurance

• High-assurance “B2” OS
  – Provides same level of assured protection as DOD requires for classified information
  – Users are “logged into” OS
• “Minimalist” design
• Centralized mediation
• Role-based access control
  – Labels separate sensitivity levels & provide containment
  – Privilege sets enforce “least privilege” principle
  – Identity-based controls limit access to specific patient
  – Clinical Data Repository accessed by role
• Auditing and intrusion/misuse detection
Transmission Assurance

- Client and server mutually authenticated using SSL
- Following authentication, all transmissions are encrypted (RC4 with 128-bit key)
- Data contain no patient identifiers
Client Assurance

- Assume Win95 environment for patients
  - NO ASSURANCE is provided by the platform - securing Win95 is NOT POSSIBLE.
  - Thus objective is to provide features and countermeasures that raise the level of sophistication and costs necessary to compromise patient data.
  - Environment integrity checked, monitored

- Providers use NT (in unprivileged mode) or network computer
- Java applet (JDK 1.1)
- Users authenticated using password and token
- No keyboard input
- No saves to disk
- Keys, certificates stored on floppy disk; inserted when needed
Sample Screens
Project Status

• Phase 1:
  – Architecture and Design
  – Build Model
  – Test in Simulation Environment

• Phase 2:
  – Build Interface to UCSD
  – Deploy with Providers by 3rd quarter 1998; patients by 1st quarter 1999
  – Measure Results
Observations

• “Pure LBAC” is not an appropriate access model for healthcare -- but it is useful in implementing a more suitable model, RBAC.
• LBAC is useful in providing containment, thus increasing system robustness.
  – Both hierarchical levels and vertical compartments can be identified.
For more information re PCASSO ...

PRINCIPAL INVESTIGATORS

Dixie B. Baker, Ph.D.                          Dan Masys, M.D.
Chief Technology Officer                    Director of Biomedical Informatics
Commercial Health Care Group               School of Medicine
Science Applications International Corporation
(310) 615-0305, Ext. 13                     University of California, San Diego
Dixie.B.Baker@cpmx.saic.com                 (619) 534-4194

DEVELOPMENT TEAM

Robert Barnhart                               Rochelle Kline-Casey
Teresa Buss                                    Gary Meyer
Don Decoteau                                    Brad Witt

http://medicine.ucsd.edu/pcassoo