Current Approaches to Secure Health Information Systems are Not Sustainable: an Analysis

Vicky Liu, William Caelli, Lauren May, Peter Croll, Matt Henricksen

Institute of Security Information (ISI), Queensland University of Technology, Brisbane, Australia

Research Question

Are the current approaches to secure health information systems viable and sustainable?

Are there any cases related to health information privacy violations or weaknesses?

Privacy Invasion at Australia's Centrelink [1]

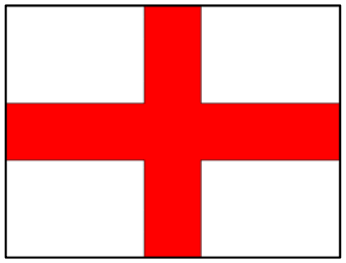
- Centrelink deploys spyware software to detect inappropriate access to client records
  - **790** cases of inappropriate access to client records since 2004
    - 19 staff were fired, 92 resigned,
    - More than 300 staff faced salary deductions or fines,
    - 46 were reprimanded, and
    - the remainder were demoted or warned.

Access control management issue

Inadequate Security Measures at UK's NHS System [2]

- 50 million patient records may be made accessible by 250,000 NHS staff
- To access patient records is on a "need-to-know" basis.
- Does not allow patients to selectively protect particular parts of their health information

Access control management issue



Security Weaknesses at HHS Information Systems [3]

- Significant security weaknesses, e.g.
  - network management, user rights and file permissions, and the auditing and monitoring of security related events
- The potential to expose clients' sensitive information to serious privacy invasions

Access control management issue

HHS : Health and Human Services

Access Controls

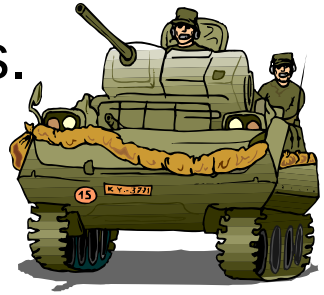
- A set of rules that specify which users can access what resources with which types of access restrictions
- **Applications**
  - Operating systems,
  - Network control systems, and
  - Database management systems
- **Access Models**
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Role-based Access control (RBAC)

Discretionary Access Control (DAC)

- Most mainstream operating systems are based on DAC
- DAC enforces security by ownership
- DAC allows the owner of information to grant access permissions to other users/programs at his/her discretion, for example, in Unix/Linux
  - chmod 777 spy
- It is vulnerable to “Trojan horse” attacks

Mandatory Access Control (MAC)

- MAC can be use to prevent some types of Trojan horse attacks.
- The traditional MAC was originally designed largely for a military environment based on the MLS hierarchical structure.
- MAC focuses on data confidentiality
- MAC can provide the ability to limit access to only legitimate users
- In MAC-based system, it is more difficult for an external adversary to tamper with audit systems.



Role-based Access control (RBAC)

- To simplify the management of authorisation
- Policy-independent and policy neutral i.e. not enforcing any particular protection policy
- RBAC does not efficiently support access policies in the way of general consent qualified by explicit denials

Health Informatics Access Control (HIAC)

Privacy

Security

Flexibility

Legal Compliance

HIAC {MAC, RBAC}

Health Informatics Access Control (HIAC)

- The HIAC system is necessarily MAC-based, incorporating RBAC properties.
- The HIAC profiling mechanism allows for health professionals to specify their requirements to a refined level of granularity.
- This degree of simultaneous control and flexibility is not achievable with either DAC or MAC individually.
- In a HIS environment, the flexibility feature is required to allow for emergency override.

References

[1] Leigh D and Evans R, Warning over privacy of 50m patient files, Guardian News and Media Limited, issued on 01/11/2006, http://society.guardian.co.uk/health/news/0,,1936403,00.html accessed 01/11/200

[2] Sharanahan D and Karvelas P, Welfare workers axed for spying, The Australian, issued on 23/08/2006, http://www.theaustralian.news.com.au/story/0,20867,20223075-601,00.html accessed 23/08/2006

[3] GAO, Information Security: Department of Health and Human Services Needs to Fully Implement Its Program. 2006 United States Government Accountability Office http://www.gao.gov/new.items/d06267.pdf accessed 20/11/2006

Vicky Liu, William Caelli, Lauren May, Peter Croll

Institute of Security Information (ISI)

Queensland University of Technology, Brisbane, Australia

v.liu@qut.edu.au, w.caelli@qut.edu.au, l.may@qut.edu.au, croll@qut.edu.au