Session 5

Patient data, ethical, legal and security issues

Conclusions & Recommendations

David W Chadwick

Professor of Information Systems Security

University of Salford

Standardization in E-health

Presentations in Session

- Security needs for Telemedicine; Mr Ph. Feuerstein, Radiologie, CH de Mulhouse
- The use of X.509 in E-Healthcare; Mr D. Chadwick, Contributor to Q 9/17 on directory services & systems, ITU-T Study Group 17
- Security standards for health communication from ISO and CEN: Mr G. Klein, Convenor of ISO/TC 215/WG 4, and chairman of CEN/TC 251
- E-health legal issues; Mr B. Stanberry, EHTEL (NO SHOW)
- Standards for Confidentiality and Security in Health Care: Mr P. Waegemann, CEO, Medical Records Institute, Chair, ASTM Standards Committee E31 on Health Informatics; Chair, US TAG to ISO TC 215 on Health Informatics; Vice-Chair, Mobile Healthcare Alliance (MoHCA)

Standardization in E-health

Highlights from Presentation 1
"Security needs for Telemedicine"

- Expressed security requirements from a user's point of view, overviewing: confidentiality, authenticity, integrity, availability, auditability, anonymity and copyright protection
- Never underestimate the need for standardizing "manware" (by which the speaker meant user aspects of the system) as well as hardware and software
- Speaker would like a data transfer auto-destruction mechanism if someone attempts un-authorized access to data

Standardization in E-health

Highlights from Presentation 2
"The Use of X.509 in E-Healthcare"

- Speaker looked at how X.509 can be used for both strong authentication and strong authorisation
- It is still an issue how we authenticate patients electronically in a user acceptable manner, and how we allow an authorized relative to pick up an electronic prescription

Standardization in E-health

Highlights from Presentation 3

"Security standards for health communication from ISO and CEN"

- Gave an overview of health informatics standards, which are often based on technology standards from ITU-T, ISO and IETF, but..
- We don't only need standards for technologies, but also for trusted third party services, national and international agreements, and responsible users etc.
- A lot of standardisation work is needed in these softer areas, e.g. defining roles, security management procedures, policies for TTPs etc.

Standardization in E-health

Highlights from Presentation 4
"E-health legal issues"

- Original speaker did not show
- Substitute Martin Denz gave a short talk about EHTEL and EHTEL T6 working group for legal, security and privacy issues
- EHTEL objective is to promote the widespread use of telematics in E-health.
- Additional material can be obtained from www.ehtel.org (see written contributions on the final edition CDROM)

Standardization in E-health

Highlights from Presentation 5
"Standards for Confidentiality and Security in Health Care"

- A view from the US
- E-health is different from e-commerce - Bilateral agreements are not acceptable in e-health care
- More than 200 general electronic security standards, but none apply specifically to e-health
- Trust in e-healthcare data is an issue – at least 5% of health data on the Internet is wrong
- Mobile security is needed for palm devices
- Speaker presented seven levels of electronic signature – lowest is self generated, and strongest is PKI generated

Standardization in E-health

Overview of issues in the session

- Users and patients requirements are important, and should not be overlooked or under-estimated e.g. in the US a top down approach to providing mobile access to EHR failed for years, but now doctors are demanding patient records be downloadable to their palm pilots.
  - How do we authenticate professionals and patients in a way they can easily use and accept? Is PKI too difficult?
  - How do we allow patients to authorize others to access their medical data and prescriptions
  - How can patients know they can trust health information on the Internet
  - How can unauthorized users be prevented from access?

Standardization in E-health

Recommendations

- We need health specific security standards (which are usually built on existing technology standards such as SSL, X.509 etc.)
- We need softer standards as well as technology ones, for topics such as: security procedures, trusted third parties, defined roles (→*privilege attributes*), international agreements, long term archiving etc.

Standardization in E-health

Follow-up actions

Action Item	Lead	Other players	Prio
Privilege Management and Access Control	ITU-T SG 17 ISO TC 215 WG4	CEN TC 251 OASIS	High
Access Control Policies	OASIS	IETF GGF	Med
Standards for Privilege Attributes	Internet2		Med
Privilege Allocation Policies	ETSI		Med

Standardization in E-health

Conclusion

- There is still plenty of scope for international standardisation effort related to trust and security, not only in health specific technology related topics, but more importantly in the softer topics related to security management and international agreements

Standardization in E-health