MAP-i
Programa Doutoral em Informática

Information Security in Healthcare

Unidade Curricular em Opção Temática e-Saúde
Thematic Option e-Health

April 21, 2009

Abstract

This document describes a Ph.D. level course *Information Security in Healthcare* a Thematic Option e-Health ("Unidade Curricular em Opção Temática e-Saúde") of the PhD program MAP-i, corresponding to a Curriculum Unit credited with 5 ECTS.

The course provides a complete analysis of Health Insurance Portability and Accountability Act (HIPPA) and the European legislation regarding information security of personal health records. Information security is usually defined by three main characteristics: confidentiality, integrity and availability. The course analyze the existing legislation HIPPA and EU identifying all three aspects and will describe some of the most prominent existing solutions that allow us to enforce current legislation.

Lecturing Team

U. Porto: Luís Antunes, Manuel Eduardo Correia

U. Minho: Henrique Santos

U. Aveiro: André Zúquete

---

1 Introduction

The Hippocratic oath incorporated the principle of medical confidentiality into doctors professional ethics.

> "All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."

In addition to the confidentiality of clinical information, this course cover also its integrity and availability. Integrity is a key point to the reliability and availability of the information as a support to the clinical decision. The widening use of healthcare information systems such as the Electronic Medical Record (EMR), which allows for the collection, extraction, management, sharing and searching of information, is increasing the need for information security.

Information security is usually defined by three main characteristics: confidentiality - the prevention of unauthorized disclosure of the information; integrity - the prevention of unauthorized modification of the information; availability - the prevention of unauthorized withholding of the information. Confidentiality is often used interchangeably with privacy but they are not exactly the same. Privacy is the right of an individual to not have their private information exposed (and this is usually enforceable by law), whilst confidentiality is limiting access to information to authorized individuals only.

The complexity of building secure information systems relates mainly to three fundamental and competing factors: the complexity of the security technology itself; the difficulty of classifying the information that is to be protected; and the use of the technology by humans (usually the most problematic factor). Other important but secondary competing factors are: protecting information from unauthorized access whilst needing to be able to access it for audit or law enforcement purposes; and making it easy for an authorized user to gain access to the information but complex for an unauthorized user to do the same.

With this unit we intend to provide a complete analysis of Health Insurance Portability and Accountability Act (HIPPA) and the European legislation regarding information security of personal health records. Information security is usually defined by three main characteristics: confidentiality, integrity and availability. The course analyzes the existing legislation HIPPA and EU identifying all these security aspects and will also present existing technical solutions that allow us to enforce current legislation. The unit will be self contained and only some basic knowledge of networks and programing is required, but even this will be subject to a short review whenever deemed necessary.

ACM Computing Classification System subjects covered:

- D.4 OPERATING SYSTEMS (C), D.4.6 Security and Protection (K.6.5).
- H. Information Systems, H.2 DATABASE MANAGEMENT (E.5), H.2.0 General - Security, integrity, and protection
- K.4 COMPUTERS AND SOCIETY, K.4.1 Public Policy Issues - Computer-related health issues, Ethics, Privacy

This unit proposed share some topics from the syllabus of the following courses in CMU (visited at 18/04/2009):

- CMU (USA). `http://cups.cs.cmu.edu/courses/privpolawtech-fa07/`.
- CM (USA) `http://privacy.cs.cmu.edu/courses/pad1/syllabus.html`.

2 Objectives

This OPT aims to provide a broad but rigorous and well founded perspective of information security in the medical fields, with special emphasis on clinical care and research. Explain legal and ethical issues surrounding privacy and security of patient medical information. Examine the basics of privacy, security and systems management in the health sector. Identify steps to ensure privacy and security in patient medical information and explore the usability of security systems in clinical settings and its relationship with patient empowerment and health self-management issues.

3 Learning Outcomes

The students should be able to:

- Identify sources of law and standards for EMR (such as European legislation and HIPPA) regarding health information security;
- Describe and plan the basic requirements enabling legal health records, namely confidentiality, integrity and availability. Ideally the students should also be able to specify and implement them;
- read and have a critical judgment over a information security product description or over a scientific working paper on the same subject.

4 Course Contents

As the main focus of this unit is a theoretical approach to cryptography we follow a well tested syllabus that can be found in similar courses in most Doctoral Programs in the main Universities.

- Introduction to information security.
  - Confidentiality, Integrity and availability.
  - Some recent studies regarding the Information Security of Personal Health Records (PHR) in Portugal.
- Legislation and Ethics
  - Health Insurance Portability and Accountability Act (HIPPA)
  - European Legislation.
  - Bio-ethics.
- Identity and Anonymity
  - The concept of Identity and Identification.
  - The roles of identification and anonymity.
  - Identification Cards. Advantages, difficulties and challenges.
  - Dangers of digital age identification.
  - Authorization without identification.
  - Anonymity Tools
  - Anonymity Enhancing Technologies: Union Routers and the TOR network.
- User centric Identity Management.
  - Historical Perspectives: From the user login to the provision and management of federated user identity systems.
  - The Role of federated identity management as an essential building block for the integration of disparage (medical) systems.
  - User centric identity management systems.
  - User centric identity management on clinical settings. Its role on privacy enhancement and self-health management mechanisms.

- Access Control Mechanisms
  - Access to Health Records: who should be granted access?
  - Identity Based Access Control.
  - Role Based Access Control.
  - Break the Glass
  - Biometric Systems
- Privacy.
  - The concept of Privacy.
  - The social value of Privacy.
  - A taxonomy of Privacy.
  - The future of Privacy.
  - Privacy enabling technologies.
- Information Security Management
  - ISO/IEC 27001
  - ISO 27799

5 Teaching Methods

- Lectures and invited lectures.
- Occasional tool demonstration and case study sessions.

6 Student Assessment

Research assignments. A large emphasis will be placed on research and communication skills, which will be taught throughout the course.

7 Lecturing Team

Short Bio of the lecturing team, attach follows the CVs.

- Luís Antunes (Coordinator) is an Assistant Professor affiliated with the Computer Science Faculty of the University of Porto, his main research interests are computational complexity, cryptography and access control. He is the principal investigator of some projects financed by the Portuguese science foundation. He has supervised one PhD student with success and is the supervisor of three others. One of the PhDs is working on new access control models for an Health Care institution, these is a joint supervision with David Chadwick from University of Kent. Additionally he is one of the founders and the coordinator of the first Health Informatics master course in Portugal.

- Manuel Eduardo Correia (Co-Coordinator) is an Assistant Professor affiliated with the Computer Science Faculty of the University of Porto, his main research interests are, theoretical and practical security aspects of systems and network administration, support infrastructures and security for scalable web services, automatic detection of network intrusions based on bio-inspired unsupervised learning mechanisms and large scale federated user-centric digital identity mechanisms for the Internet. He is currently supervising a Phd student on bio-inspired intrusion detection systems and has supervised with success and is currently supervising several master thesis in the area of systems security, identity provisioning and network administration.

- André Zúquete is an Assistant Professor affiliated with the University of Aveiro, his main research interests are security in distributed systems, with particular focus on authentication architectures, mobility with security and anonymity. He his researcher of Institute of Electronics and Telematics Engineering of Aveiro (IEETA) and collaborator of the Telecommunications Institute (IT), both at Aveiro. He participates in several national and international projects, such as PANORAMA QREN and SWIFT STREP. He is the supervisor of four PhD students. One of the PhDs is working on harmonization of authorization policies among distinct e-Government services.

- Henrique M. Dinis Santos received his first degree in Electric and Electronic Engineering, by the University of Coimbra, Portugal, in 1984. In 1996 he got his PhD in Computer Engineering, at the University of the Minho, Portugal. Currently he is an Associate Professor at the Information Technology and Communications group, at the University of Minho, being responsible for several graduate and postgraduate

courses, as well as the supervision of several final year projects and dissertations. He is also the president of the ALGORITMI Research Centre, at the University of Minho, and president of a national Technical Committee (CT 136) related with the information system security standards. During the second semester of 1990, under an ERASMUS program, he was teaching at the University of Bristol, United Kingdom, where it was recognized as University Academic staff.

References

[1] Julian Ashbourn. *Biometrics: advanced identity verification.* Springer-Verlag, London, UK, 2000.

[2] Lorrie Faith Cranor and Simson Garfinkel, editors. *Security and Usability - Designing Secure Systems that People can use.* O'REILLY, 2005.

[3] Filipa Falcão Reis and Manuel E. Correia. Public awareness concerning online privacy rights: Attitudes and perceptions of vulnerability among the youth. In *"EU Kids Online" Conference*, London School of Economics and Political Science, London., June 2009. London School of Economics and Political Science, London.

[4] Filipa Falcão Reis, Altamiro Costa-Pereira, and Manuel E. Correia. Access and privacy rights using web security standards to increase patient empowerment. *Studies in Health Technology and Informatics*, 137(Volume 137):275–285, June 2008.

[5] A Ferreira, R Cruz-Correia, L Antunes, P Farinha, E Oliveira-Palhares, D W Chadwick, and A Costa-Pereira. How to break access control in a controlled manner. *Computer-Based Medical Systems, IEEE Symposium on*, 0:847–854, 2006.

[6] Ana Ferreira, Lus Barreto, Pedro Brandao, Ricardo Correia, Susana Sargento, and Luis Antunes. *Accessing an existing virtual electronic patient record with a secure wireless architecture*, chapter II. Mobile Health Solutions for Biomedical Applications. IGI global, Medical Information Science Reference, April 2009.

[7] Ana Ferreira, Ricardo Cruz-Correia, Luis Antunes, and David Chadwick. Access control: how can it improve patients' healthcare? *Studies in Health Technology and Informatics*, 127, June 2007.

[8] Jim Harper. *Identity Crisis - How identification is Overused and Misunderstood.* CATO Institute, Washington DC., 2006.

[9] A. K. Jain, A. Ross, and S. Pankanti. Biometrics: A tool for information security. *Ieee Transactions on Information Forensics and Security*, 1(2):125–143, 2006. ISI Document Delivery No.: 163FY.

[10] A. K. Jain, Bolle Ruud, and Pankanti Sharath. *Biometrics: Personal Identification in Networked Society*. Springer-Verlag New York, Inc., 2005. 1207058.

[11] A. J. Palmer. Criteria to evaluate automated personal identification mechanisms. *Computers & Security*, 27(7-8):260–284, 2008.

[12] Kenneth Revett, Hamid Jahankhani, Sérgio Tenreiro Magalhães, and Henrique M. D. Santos. *A Survey of User Authentication Based on Mouse Dynamics*, volume 12 of *Communications in Computer and Information Science*. Springer Berlin Heidelberg, 2008.

[13] Ricardo Santos, Manuel E. Correia, and Luís Antunes. Use of a government issued digital identification card to secure interoperable health information systems. In *ICCST 2008, The 42nd International Carnahan Conference on Security Technology*, Prague, Czech Republic, October 2008.

[14] Daniel J. Solove. *Understanding Privacy*. Harvard University Press, 2008.