

---

# Security and Privacy System Architecture for an e-Hospital Environment

---

Kathryn Garson, Carlisle Adams  
University of Ottawa

---

## Agenda

- Introduction
  - Hospital Environment
  - Privacy Goals
  - Encryption and Access Control
  - Authentication
  - Other Privacy Concerns
  - System Architecture
  - Conclusion
-

---

## Introduction

- Mobile Emergency Triage (MET) project
    - Software provides doctors with interactive decision support for triage and treatment of patients
    - To be used as a trial in Ottawa hospital
    - Wireless network allowing physicians to travel patient to patient with tablet PC
    - MET software pulls patient records from database
    - Sensitive data transmitted over wireless network, stored on servers and tablet PC
  
  - Need access control and encryption to protect sensitive information
- 

---

## Hospital Environment

- Highly sensitive data required in emergency situations
    - Cannot have security measures get in the way of physician's access to information
  
  - Patient records currently paper moving towards electronic
    - Each record consists of multiple documents
    - All will be available in electronic form
-

---

## Hospital Environment

- Current system in emergency department is read-only
    - Employees sign in with username and password (no restrictions)
    - High-traffic areas
    - Access depends on employee role and associated permissions
    - Only access from within hospital, remote log-in will not be a part of our trial
- 

---

## Privacy Goals

- Personal Information Protection and Electronic Documents Act (PIPEDA – Canada)
  - Personal Health Information Protection Act (PHIPA – Ontario)
    - Extends PIPEDA
  - Principle 7 of PIPEDA specifies safeguards to be used to protect sensitive data
-

---

## Privacy Goals

- Sensitive information should be protected by high level of security
  - Include technological methods such as passwords and encryption
  - Limit access on a 'need to know' basis
  - Medical records should be protected from loss, theft, unauthorized access, disclosure, copying, use, or modification
- 

---

## Privacy Goals

- **United States**
    - Title II of Health Insurance Portability and Accountability Act (HIPAA) has similar privacy standards
  - **Europe**
    - EU Data Protection Directive
  - **Our goal is to satisfy these privacy guidelines**
    - Provide encryption and access control
    - Use appropriate authentication method
    - Additional privacy need: automatic deletion of records
-

## Encryption and Access Control

- Network Encryption and Access Control
- Encryption Only
- Identity-Based Encryption
- Role-based Encryption
- Policy-Based Encryption

## Network Encryption and Access Control

- Wired Equivalency Privacy (WEP) Protocol not considered secure
- Virtual Private Network (VPN) using SSL
  - All communications between client and server are encrypted using a shared key
  - OpenVPN uses SSL technology and provides authentication, confidentiality, and data integrity
  - Physician's device and MET servers will have VPN software

## Network Encryption and Access Control

- Still need access control to manage access within network
- Role-Based Access Control (RBAC) systems work well in hospital environment
  - Permissions already based on employee role
  - Authenticate to system when asking for resources
- RBAC and VPN will provide security we need

## Encryption Only

- May be unnecessary to separate access control and encryption
- Traditional Public Key Cryptography
  - Each user has a private and public key
  - Keys managed by use of certificates
  - Encryptions are done for a particular user
  - Problems: cumbersome management of keys, cannot encrypt easily for multiple recipients
  - Would need to add access control methods to organize encryptions based on roles

---

## Identity-Based Encryption

- In Identity-based encryption, any string can be used as the public key
    - E.g. email address
    - Recipient authenticates to a trusted authority and receives the corresponding private key
  - Users don't need to manage their own keys
    - Public key is well-known and unique to that person, no certificate necessary
    - Private key is generated when user authenticates themselves
  - However, we still need to figure out how to encrypt for multiple recipients based on role
- 

---

## Role-Based Encryption

- Using a more general approach, encryption can be done on a role
    - Since any arbitrary string can be used as public key, can use a string such as “doctor”
    - Allows to encrypt a document with access control rules
  - However, we need to be able to express more complex rules
    - E.g. “a doctor or nurse can have read access”
-

## Policy-Based Encryption

- Document is encrypted under a policy, which is a combination of rules
  - Can be simple policies such as  
“<Doctor AND Write> OR <Nurse AND Read>
- User wishing to decrypt
  - Authenticates to a Trusted Authority
  - Receives a private key based on their role containing credentials
  - If their credentials satisfy policy rules, their key can decrypt document

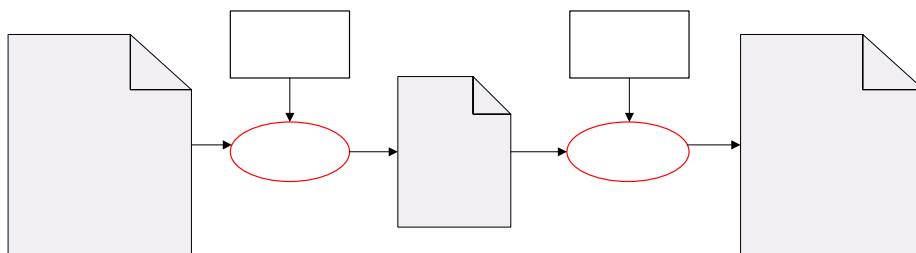
## Policy-Based Encryption

- Automated encryption process
  - Physicians and staff will not have to manage private keys
  - Authentication process allows to decrypt
  - Policies can be specified by document type
  - Staff entering/saving documents will not have to select which policy to encrypt under

## Policy-Based Encryption

- Encryption system by Molva & Bagga
- Consider a policy stating “an employee with the role of doctor or nurse can read a document”  
pol = <Doctor, role> OR <Nurse, role>  
act = read  
doc = document
- The document is encrypted  
temp = PolEnc(doc, pol)
- A person can decrypt if their credentials satisfy the policy  
cred = (alice:doctor)  
doc = PolDec(temp, pol, cred)

## Policy-Based Encryption



## Policy-Based Encryption

- Encryption in their system
  - Each conjunction is assigned a mask
  - Each disjunction is assigned a key
  - Each key is encrypted by each mask
  - User who satisfies one conjunction will be able to decrypt
  
- Our goal is to extend their work
  - Want to include multiple actions
  - Want to add key revocation

## Policy-Based Encryption

- Multiple actions
  - What if a doctor is allowed to modify a document, while a nurse can only read
  - Keep track of which conjunction in policy was satisfied
    - E.g. <Doctor, role> AND <Write, action>
  - Trap call to OS, if write action requested, and conjunction with was satisfied, open document in write mode
  
- Policies can contain action elements
  - Corresponding keys will contain requested action as well

## Policy-Based Encryption

- Key revocation
  - What if an ex-employee kept the decryption key, need to change key in current use
  - Add a time period to policy
  - Can only decrypt if decryption key was generated/retrieved during that time period
  
- Example
  - pol = <Doctor, role>AND<01/25/2008-02/25/2008, time>

## Policy-Based Encryption

- Updates to policies and keys should not interrupt system usage
  - Can update documents in batches
  - Any document currently opened will be saved encrypted under new policy
  - Any person wishing to decrypt a document under new policy will be issued a corresponding updated key
  - Anyone who saved old keys will not be able to decrypt new documents

## Policy-Based Encryption

- Provides both encryption and access control
  - Documents are encrypted for storage and all transmissions
  - Policy determines who can decrypt to have access
- Policy can be based on document type
  - Allows for small number of policies to manage
  - Allows for encryption to be done automatically
- Small number of decryption keys based on roles

## Authentication

- Security of encryption system relies on strong authentication
- Username and password most common
  - Users choose weak passwords
  - Imposing restrictions makes it hard to remember
- Two-factor authentication
  - Provides better security
  - Staff won't have to remember hard passwords

---

## Authentication

- Fingerprint Biometrics
    - Tablet PC to be used in trial has fingerprint reader
    - Some problems, including doctors wearing gloves
    - After discussing with doctors, agreed this was not an option
  
  - RFID Reader
    - Employee badges have a barcode
    - Can scan badge barcode
    - Second-factor of 'something you have'
    - Need to include a backup method for when someone forgets their badge for the day
- 

---

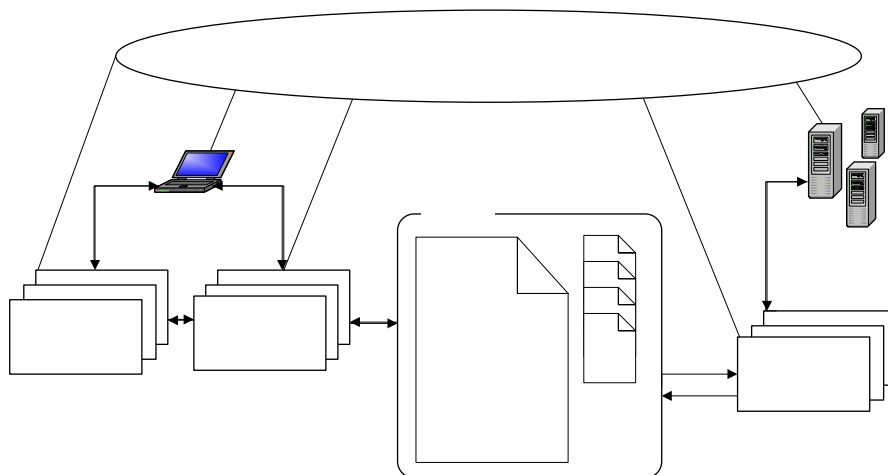
## Other Privacy Concerns

- Audit logs
    - Track user activity on system
    - Log on/off, records requested, records modified
  
  - Integrity mechanisms
    - Protect data from unauthorized modification
    - Message Authentication Code (MAC) to be able to verify integrity of records
  
  - Automatic deletion of files
    - Preventing records from leaving hospital
    - Security measure asked for by hospital staff
-

## System Architecture

- MET system is multi-agent
  - Information agents, task agents, interface agents
- Blackboard central temporary storage area
  - Agents pull/push information from/to the blackboard
- Integrating security functionality
  - As encryption agents
    - Problem in organizing agents in this way, encryption and decryption agents needed at blackboard, databases, and tablet PC, will be accessed by all agents
  - Security as a set of services
    - All agents have access to set of encryption services

## System Architecture



## Conclusion

- Policy-based encryption
  - Extensions to existing system
- Authentication mechanisms
  - Employee badge with a barcode
- Additional security needs
  - Audit logs, integrity mechanisms, deletion of files
- Integrating security into multi-agent system

## Questions

