Wireless Security and Health Care Information Systems

Vladimir Oleshchuk
Faculty of Engineering and Science
Agder University College
Grimstad, Norway

Outline

- Wireless communication: (dis)advantages.
- Wire(less) (un)security
- Healthcare information systems
- Wireless healthcare information systems
- Security of wireless healthcare information systems

Advantages of Wireless Communications

- Freedom of mobility: "Access to any application from any device on any network".
- Reasons to use wireless communications:
  - Improve productivity: real-time access and faster distribution important business information
  - Growing mobility customers and employees
  - Improved customer service (fast response increase customer satisfaction)
  - Competitive advantage (contact with customers, partners, suppliers and employees)
- Major benefit (for healthcare sector):
  - Streamlining doctor/patient relationship
  - Patient data can be updated in real-time y doctor
  - Online track of medication prescriptions and billing information

Disadvantages of Wireless Communications

- Wireless networks are vulnerable to attack
- Threats
  - Uncontrolled terrain:
    - (anonymous, uncontrolled coverage area between end points);
  - Eavesdropping:
    - (gather information about who use the network, what is accessible, equipment capability, coverage area, etc.)
  - Communication jamming (DoS):
    - Client jamming, base station jamming etc.

Wireless Threats (cont.)

- Injection and modification of data
  - Connection hijacking
  - Man-in-the-middle attacks
- Rouge client (mimic client identity)
- Rouge network access points (attacker set up a rouge access points to impersonate a network resource)
- Client-to-client attacks (get sensitive information to access other resources)

Security Vulnerability and Risks

- Exposed access points (APs):
  - WLAN radiates data that may exceed the area physically controlled by enterprise
- Service Set Identifier (SSID) used for authorization:
  - Compromised, default password etc.
- Invisible WLAN access points:
  - Ad hoc networks establishment between devices with built-in WLAN cards or unauthorized APs
- Overlapping spectral footprints
  - Accidental or intentional networks overlapping
- MAC used as identifier
- Lack of flood protection
- Client platform security vulnerabilities

Security protection levels:

- Hardware protection should be
  - (authentication, authorization and encryption) integrated into hardware.
- Wireless security policy:
  - developing and enforcing a strong wireless security policy based on sound risk analysis
- Monitoring and Intrusion detection
  - Discovering wireless vulnerabilities, detection intruders and attacks
- Virtual private networks
  - Install VPN client software on all wireless available PC

Security Considerations for Wireless Devices

- Security of wireless devices impacts the security of entire network
  - Physical security
  - Information leakage

Some suggestions to information leakage threats

- Laptops:
  - Pay attention to storage of passwords and keys (f.ex., some wireless cards store WEP keys in registry in cleartext).
  - Use host-based IDS, personal firewalls.
- PDAs:
  - Minimize storage of data that PDA access
  - Do not rely on client-side security (compromised sensitive data in PDA can be compromise the whole application; PDA-based encryption mechanisms have been found to be vulnerable)
- Wireless infrastructure (APs, bridges, etc.)
  - Use secure protocols to access infrastructure (SSH, SSL, SNMPv3 etc.)
  - Disable insecure protocols (HTTP, SNMPv1)
  - Improve physical security
- Mobile phones
  - Similar to PDAs and laptops
  - Encrypt sensitive information before sending (f. ex., use WTLS while using WAP)

Info security in the health care system

- The range of technical and procedural mechanisms that aim to preserve confidentiality, restricting information access and modification to authorized users for authorized purposes.
- The goal is to insure the accuracy and timely availability of data for the legitimate users
  - Electronic healthcare records can be protected by applications and servers that incorporate authenticated, authorized and audited access control.
  - Encryption can protect the integrity of data while in transit.
  - User authentication and screen locks can prevent improper access and accidental disclosure.
  - Enterprise security policies consistent with emerging recommendations can help ensure that appropriate technical, administrative and procedural measures are employed to protect patient data.
  - Legislative and regulatory measures can provide guidelines for protection of electronic health information and provide punitive damages for violations.

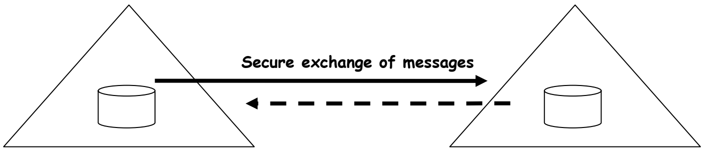
Norwegian laws and regulations

In Norway, there are strict regulations with respect to the security required when medical information is electronically processed:

1. Helseregisterloven (**Health Act**) §§ 5 and 6 give the necessary legal background for allowing medical electronic health records.
2. Security requirements for these records is in Helseregisterloven §36 regulated by The **Personal Data Act** (Personopplysningsloven) and the corresponding regulations.
3. These regulations require the responsible enterprise to perform a Vulnerability Assessment in order to decide both the security needed, if the security established is good enough and possible need for improved security measures.
4. The Norwegian Data Inspectorate (Datatilsynet) gives more detailed guidance (reference model, encryption strength etc.), and recommendations to indicate the minimum need of security for information like medical health records.

Exchange of medical information

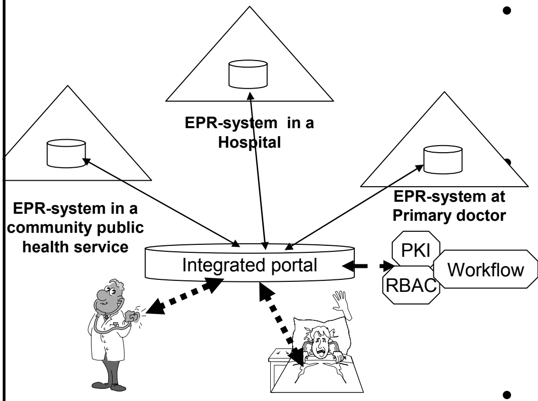
- In Norway health services are organized in hierarchic pyramids reporting to a Managing Director.
- It is established solutions for secure exchange of messages between different Health Services using XML, Digital Certificates and 128 bit DES encryption.
- A Primary Doctor are not allowed to log into an EPR-system at a hospital because he is not administrative reporting to the hospitals Managing Director and thus not covered by the hospitals responsibility for the information security management system (ISMS).


Secure exchange of messages

EPR-system in a Hospital

EPR-system at Primary doctor

Example: Access to the patient's EPR


EPR-system in a Hospital
EPR-system in a community public health service
EPR-system at Primary doctor
Integrated portal
PKI
RBAC
Workflow

- Patient may need a limited access to the electronic patient records (EPR).
- Health services should be able to share information.
- It must be possible to give input of biomedical recordings.
- Should be able to control access (deny) to EPR.

Risk management

- Risk management includes examination of three factors:
  - Assets (patient and business information, critical data etc.)
  - Threats (dissatisfied patients,)
  - Vulnerabilities

Plans

- Use cases and possible future scenarios for using healthcare information systems.
- Security analysis of existing solutions and make risk assessments future scenarios.
- Risk assessment of using wireless communication (vulnerabilities, threats, etc.)
- Development of new secure solutions for wireless healthcare information systems.