Special Topics in Security and Privacy of Medical Information

Sujata Garera

Previous lecture
- Portable patient record systems
  - USB PHRs
  - Smart phone based systems

This lecture
- Share storage on smart phones
- Health monitoring systems
  - WAITER
  - AMON
  - Body sensor networks
Division of capabilities

Scenario 1

Scenario 2
Scenario 3

Storage - EMT share
- EMT share is encrypted on the phone
- Smart card could be used
  - What happens if credentials are stolen or lost?
  - Need a way to revoke access rights

Possible ways
- Public private key pair
  - A public private is assigned to each EMT by a Regional Health Organization (RHIO)
  - Public keys are made available over the internet and private key is programmed on EMT smart card
  - Software on phone encrypts the EMT share with each of these public keys
  - Revocation can be accomplished in a simple manner
    - How?
### Storage- EMT share

**Possible Ways**
- Same public key pair used by all EMTs in a given region
  - Key pair valid for one day and renewed next day
  - At end of day client software deletes the ciphertext for that day
    - Keys may be made available say 150 days in advance and client may update her ciphertexts of EMT shares every 100 days or every time the number of stored ciphertexts drops below 50
    - Don’t have to worry about revocation with this method

### Tradeoffs

**First option is convenient with respect to EMT operations**
- EMT doesn’t need update his smart card everyday

**Second more robust but doesn’t support EMT access auditing easily**

### Storage-BTG share

- BTG share must be stored encrypted on the phone
- Encrypted in a way that in an emergency, access to one user’s share should not allow you to access another user’s BTG share
- Have a central organization such as a RHIO manage these BTG access keys
**Storage-BTG share**

- Each user stores the phone’s public BTG key and an encryption of the BTG share with it.
- In case of emergency the private key is released.
- A new key pair is generated for the phone later on.

**Storage-Password share**

- Password derived key is used to encrypt one of the shares of the key $K_r$. 
  - Potential dictionary attacks are possible.
  - What is a dictionary attack?
  - Can increase the time to launch dictionary attacks.
  - Manber approach: Append the password with a secret randomly chosen salt.
  - System can find salt by linear search.
  - Time required to process a single password is negligible but processing many password possibilities is time consuming.

**Share updates**

- Shares need to be re-encrypted periodically especially EMT share.
- Shares are also stored encrypted under user credentials so that updates possible.
Open issues

- Biometric key generation
  - Authentication certainly exists: Classifeye
  - From pictures taken from the smart phone
  - Newer hardware may make this possible

- Granular access control
  - Allow user flexibility of revealing certain portion of her health records to certain health groups

Real time Monitoring Systems
Real time Monitoring systems

- **Goals**
  - Develop low cost methods for health care improvement using emerging mobile and pervasive computing
  - Sensors used should not affect the users behaviors or inconvenience a user
  - Low energy consumption
  - Process real time data at health facility
  - Detect emergency situations
  - Secure transmissions

- **WAITER**
  - Monitor user and issue alerts in emergency scenarios
  - Heart beat, motion, body temperature sensors used to collect users vital signs
  - Transmitted via Blue tooth
  - Mobile phone equipped with bluetooth receiver collects the data which is processed onsite
Lack of security
- Bluetooth
- Discoverable vs Non-discoverable
- Brute force
- Intelligent brute force
  - Nokia: Bluetooth address 11:11:11:50:11:11

Increasing security of this system
- Assignment
- Design a protocol
Realtime Monitoring Systems

- **AMON**
  - Advanced care and alert portable telemedical Monitor
  - Continuous medical monitoring for high risk cardiac/respiratory patients
  - Monitors multiple parameters
    - Many more compared to WAITER
  - Cellular connection to a telemedicine center

**AMON**

- **Features**
  - Multiparameter Monitoring
  - Activity Recognition
  - Online Analysis and Emergency Detection
  - Flexible Communication Interface
  - All-in-One Wrist-Worn System

**AMON**

- **System Overview**
Possible evaluations
- Everything normal
- One parameter out of range
- Multiple parameters out of range

Sensors

Communication
- SMS
  - Used for messages with small values such as BP results
- Virtual circuit switched channel established through a mobile phone link
  - Long messages such as ECG readings
- Internet based channel such as FTP/TCP-IP
  - More for future applications
AMON
- Telemedicine center

AMON
- Validation performed through user study
  - 70% found device comfortable
  - 10% female complained it was painful when BP taken
  - Gave them a feeling of security
  - Design required improvements
  - Sensor measurements were erroneous when signals could not be detected due to noise

AMON
- More advanced compared to WAITER
- Security aspects considered
- User study performed
- More portable and wearable
If patient identity concealed how is the information correlated to right patient record?

This lecture

- A wearable personal healthcare and emergency aid system
  - Wu et al.
- A Wearable multi-parameter medical monitoring and alert system
  - Anliker et al.