Security Analysis of Emerging Remote Obstetrics Monitoring Systems

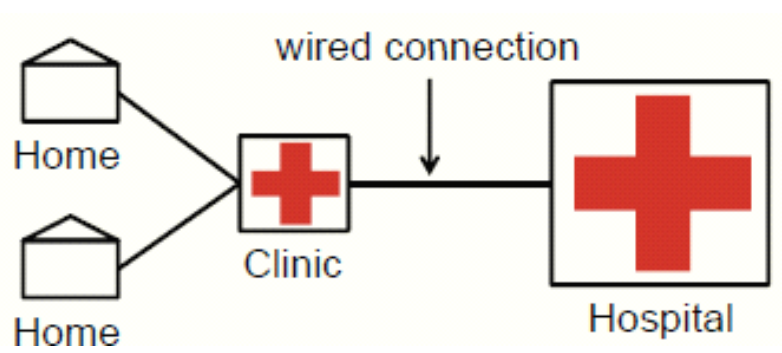
C. C. Tan*, L. Bai^, D. S. Mastrogiannis', J. Wu*

*Dept. of Computer and Information Sciences, Temple University
^ Dept. of Electrical and Computer Engineering , Temple University
'Dept. of Obstetrics, Gynecology & Reproductive Sciences, Temple University School of Medicine

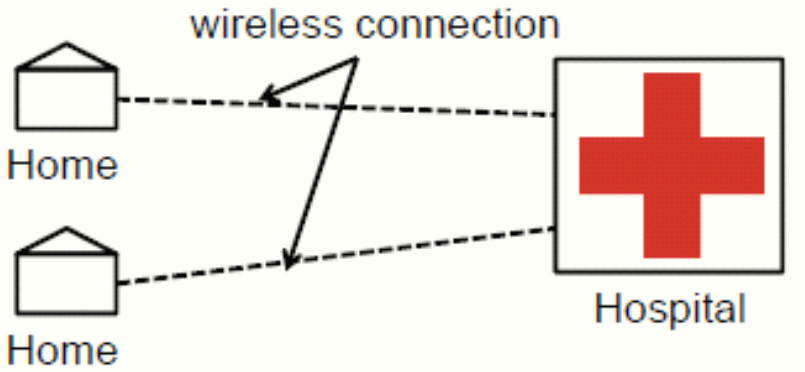
Introduction

- Electronic fetal monitoring is a common medical procedure in America
- Used in approximately 85% of births.
- Patient needs to travel to hospital for monitoring by trained personnel
- A burden for patients living in remote areas.
- Expensive (travel costs, waiting time, hospital resources, etc.)

Introduction



- Traditional telemedicine
- Use networking technologies to do monitoring at remotely, i.e. at a clinic.



- Emerging systems
- Use wireless, mobile, and sensor technologies to do monitoring at home.

Traditional vs Emerging Systems

- In traditional systems
  - Standard hospital monitoring equipment is used
  - Trained medical professionals operating the equipment
- In emerging systems
  - Off-the-shelf equipment is used, e.g. smartphones
  - Patient herself will be operating the monitoring equipment.

Traditional vs Emerging Systems

	Traditional systems	Emerging systems
Treatment location	Clinic	Home
Personnel	Medically trained staff	Non-medical personnel
Hardware	Medical grade	Off-the-shelf

- Differences make it necessary to revisit security for emerging systems.

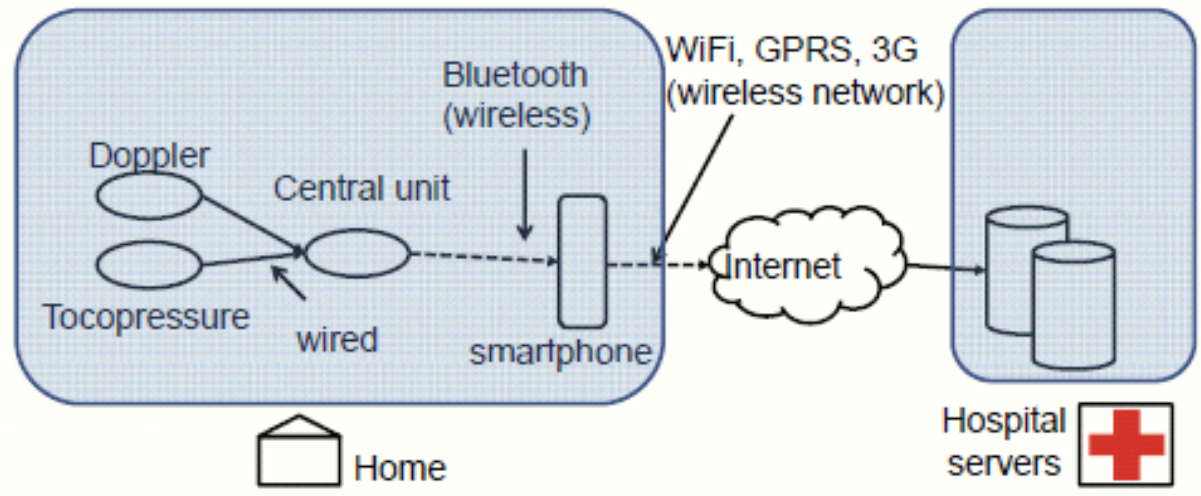
Key Differences

- The monitoring is no longer restricted to a clinic, but the user's home.
- Cannot assume home-based systems have a higher level of security protections. A password protection mechanism and management will need to be in place.
- No medical professionals to operate monitoring device in home-based systems. This may require a redesign of the user interface
- Smartphones are multi-purpose devices which are open to greater security risks, like viruses.

Our contributions

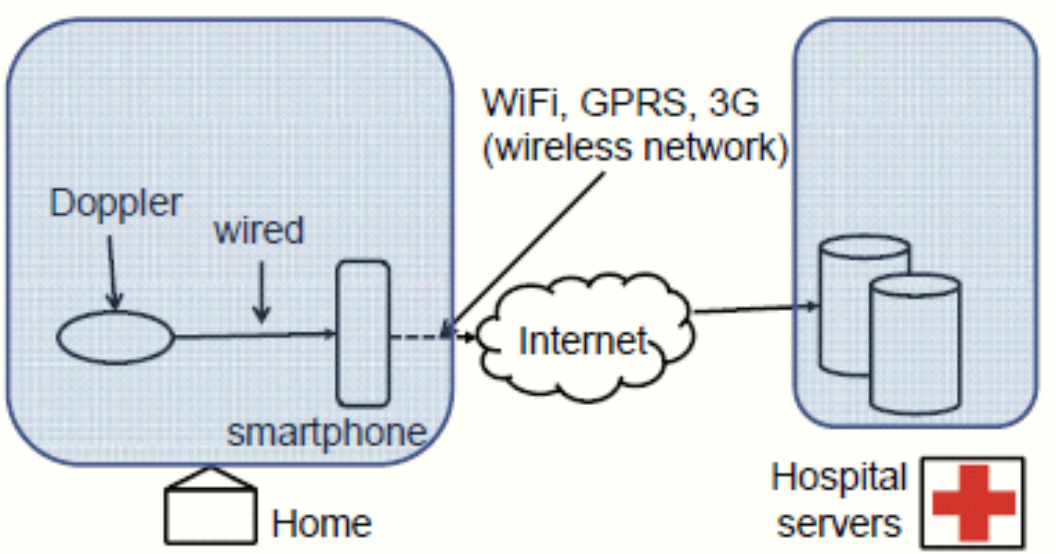
- Compare the security of two recently proposed systems against the HIPAA guidelines.
- Provide an overview of relevant security requirements needed for remote monitoring systems based on the HIPAA Security Rule.
- Suggest potential security vulnerabilities, and possible enhancements.

System I



- Devices are connected to a central unit via wired connections which filter out errors and forward collected data to the gateway device through Bluetooth.
- The gateway device transmits the data to the hospital's server using SFTP.

System II



- Smartphone processes the data and transmits it back to the hospital server using GSM or GPRS and informs the patient and the professonal when the transmission is completed.
- HTTPS protocol is used to encrypt the data

HIPAA requirements

- **Access control** – system needs to regulate access to the data by authorized personnel or programs. The system may need to include a feature to perform encryption/decryption of data and session control.
- **Audit control** – system needs to implement a mechanism to record and examine the activities of the system.
- **Integrity** – system needs to incorporate mechanisms to both protect the stored data, as well verify that the stored data has not been tampered with.

HIPAA requirements

- **Person/Entity authentication** – requires system to verify that the identity of the entity accessing the data is correct.
- **Transmission security** – requires system to prevent unauthorized access of the data during transmission over the network. This includes encryption of data during transit and determines if data has been modified during transit.
- **Device and media controls** – requires procedures to ensure the data be safely deleted when the user is no longer using the system, or when the system is re-issued to a different user.

Adversary Model

- Assumptions:
  - Adversary has knowledge of monitoring systems
  - Adversary has access to any hardware necessary to communicate with the monitoring system.
  - Excludes denial-of-service attacks, such as wireless jamming which can prevent any communications between monitoring systems and the hospital servers.
  - All data is to be stored into the hospital's servers, restricting the discussion to attacks on the monitoring system itself.

Analysis

- **Access Control –** data from the sensors are transmitted to the smartphone from the central unit using Bluetooth which ensures that the data reaches the smartphone securely. Since most smartphones have a password feature, we can assume that only authorized personnel can have access to the password, and thus the data.
- **Audit control** – both systems perform some data processing on the data collected by the Doppler device, but neither system appears to implement any system to record the operations of the sensing device or the smartphone. As such, there does not appear to be possible to perform any diagonsis of system activities.

Analysis

- **Integrity** – System I uses SFTP to transfer the data form phone to the hospital's servers. SFTP provides integrity protection during data transfer but does not notify any party in the event of network failure. System II uses HTTPS to transfer data from phone to hospital's servers. HTTPS is built on top of TLC which provider integrity protection and incorporates a user feedback mechanism.
- **Person/Entity authentication** – Both systems use the password feature of the smartphone to satisfy person authentication requrements. However, neither system appears to perform any entity authentication and so the hopsital does not know whether the data is collected using a valid device or not.

Analysis

- **Transmission security** – Both Systems I and II uses standard secure data transmission protocols to transmit data form the device to the hospital. Therefor, both system provide transmission security.
- **Device/Media controls** – Neither system details the procedures for device and media controls. However, since both systems uses a removable storage in the form of a microSD card, existing hospital policies on device and media controls can be extended to meet this requirement.

Security Recommendations

- Restrict smartphone capabilities by removing unnecessary applications
- Preventing the user from installing new applications

Security Recommendations

- User and device authentication are necessary to provide integrity protections.
- At minimum, the system should authenticate the smartphone before allowing the data to be stored into the hospital server.

Security Recommendations

- Improve user feedback process in the data transfer process and the data collection process.
- Emerging systems should also consider including automatic diagnostic software that tries to determine whether the collected data is indeed correct.

Security Recommendations

- Possible to avoidance of encryption within the smartphone because the data is already encrypted during transmission.
- Simplifies the overall system design and increases the ease of handling an emergency situation where data needs to be accessed immediately.

Conclusion

- Emerging remote obstetrics monitoring systems have the potential to lower the cost of providing quality obstetrics care by using commercial components.
- This comes with additional security risks that are absent from traditional remote monitoring systems.
- Our analysis of two recent system designs suggest that additional security protections besides simply securing the data transmission is necessary to meet HIPAA requirements.