Privacy and Security Vulnerabilities in Health Care Infrastructure Mobile Technology

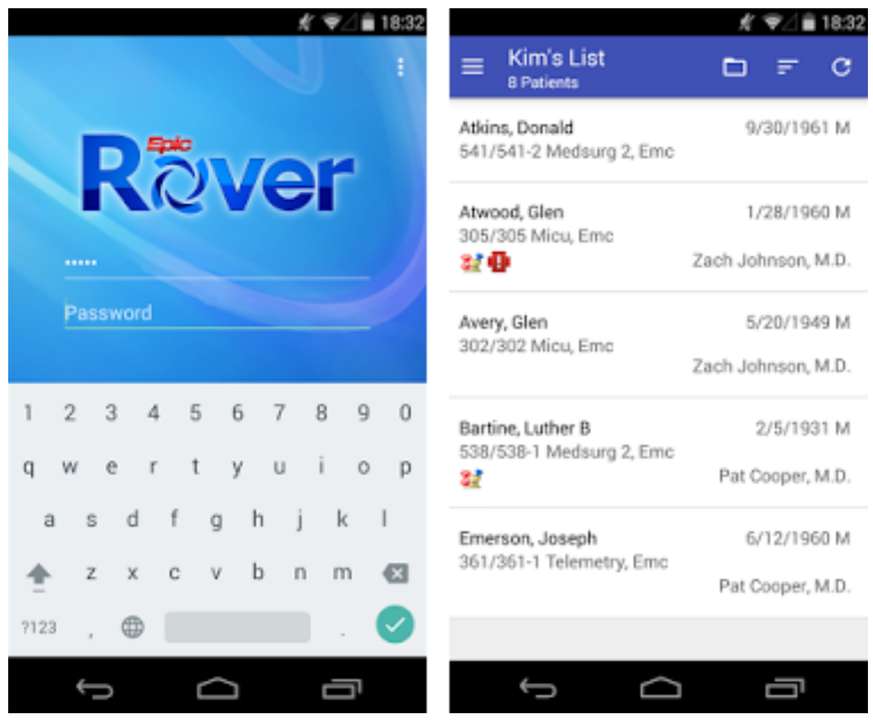
Dr. Sajedul Talukder
Edinboro University

Objective: Ensuring Privacy and Security Vulnerabilities in Health Care Infrastructure

Our Contributions::

1. Security Vulnerabilities and Countermeasures
2. Qualitative Risk Assessment Matrix

Epic Rover Mobile App



Research Findings

- **• Security Vulnerabilities and Countermeasures. This paper identifies common security threats and vulnerabilities to EPHI, and, develop and adopt appropriate mitigation to reduce risks and maintain compliance.**
- **• Qualitative Risk Assessment Matrix. This paper presents a qualitative risk assessment matrix developed by taking into account potential threats and vulnerabilities, the probability of their occurrence, the potential impact and severity if they were to occur, and the inherent risk by introducing mobile devices.**

Vulnerability	Description	Countermeasure
Outdated Software Version and Delay in Patching:	Not patching the OS or software on a regular basis leaves the system in a vulnerable state, and could allow new and identified threats to exploit the system's lack of updates. This increases the system's susceptibility to malware, and can result in the data being compromised.	Automatic updates, policies requiring patching when made available
Insufficient Authorization	Authorization procedures should be specifically defined for users in respect to their role in the organization, their status, and their department, to avoid users who aren't authorized to view personal data gaining access to it.	Two-factor authentication, access control lists, IDS/IPS
Improper use of Device	If a user carries out unacceptable behavior on a device containing EPHI, such as accessing untrustworthy sites, downloading media, or emailing personal information, they may not only put EPHI at risk, but also the network.	Acceptable Use Policy, system logs, training
Connection to Unsecure or Untrusted Network	If there is an incoming and outgoing of data over a network which has not been secured or verified using a trusted certificate, the data is exposed to invalid access and modification, especially without the use of cryptography.	Restrict devices to intranet connection, VPN, firewall, encryption
Jailbreaking	Rooting or jailbreaking a mobile device may leave it open to malicious attacks, as the encryption protection gets bypassed if the app is running on a rooted device.	Acceptable Use Policy, perform regular system test/analysis
Unattended Device	If a device containing EPHI is not properly monitored, it may be accessed or stolen by unauthorized users, exposing personal and confidential data.	Remote wiping, lock inactive devices, monitoring (cameras and logs)

Takeaway

According to the NIST Cyber Security Framework, steps to ensure compliance will promote the process of integration of mobile devices into our system and advise us to establish and enforce the appropriate policies and procedures to better secure the EPHI we make, store, view and distribute.

Conclusion

- ❑ We explore the information that the safety department wants to evaluate and fully analyze the vulnerable situations and risks posed by the usage of mobile apps within the medical community before this new technology is introduced, and propose risk management and mitigation strategies while ensuring compliance with regulatory requirements.

Interested in our research? Please visit our PENSLab:
http://penslab.cs.edinboro.edu/

PENSLAB Privacy ENhanced Security

EDINBORO UNIVERSITY