Transactions of the International Conference on Health Information Technology Advancement

Center for Health Information Technology Advancement

10-2013

Challenges of Mobile Healthcare Application Security

Alan Rea
Western Michigan University, rea@wmich.edu

Challenges of Mobile Healthcare Application Security

Alan Rea
1903 West Michigan Ave.
BIS Dept., Haworth College of Business
Western Michigan University
Kalamazoo, MI 49008-5412
rea@wmich.edu 269.387.1444

Abstract: Healthcare information technology has overcome many of the Web application security challenges in the past decade. We can now access information more securely and incidents of unintentional data loss are on the decline. However, more must be done to ensure the confidentiality, integrity, and availability of mobile applications in the healthcare field. Whether it is physicians using iPads to access treatment histories or patients managing healthcare options via smart phones, the proposed CAP framework (checks, assurances, protection) adds additional security and privacy layers to our modern mobile medical needs.

INTRODUCTION

The security of Healthcare information is paramount to the success of HIT systems. Over the past decade, we have seen an increase in both research and practical application that takes into account the importance of secure transactions, information exchange, and protection of data within Healthcare systems. There is still much work ahead of us, but it is clear that more healthcare professionals realize the need for secure information exchange as the profession moves from paper to electrons.

The Challenge

Application developers and practitioners have made great strides in creating usable and secure systems that can be used to facilitate healthcare data exchange whether it be patient records, prescriptions, lab tests, or other routine daily operational data within the context of application and web centric systems. We see this best illustrated in systems and software such as EPIC (EPIC, 2013).
However, computing systems and how we use them are once again experiencing a shift. More users are now accessing, creating, and consuming information via mobile devices (Fidelman, 2012). Whether it is the teenager updating Facebook via her smart phone, or a store manager checking inventory via his tablet, more people are using always-on, connected mobile devices for play, work, research, and sensitive personal transactions.

There is much literature that looks at creating and maintaining protected transactions between mobile agents. Whether we examine the types of attacks on or among mobile agents (Jansen, 2000), the guiding principles to protect them (Burkle, Hertle, Muller, & Wieser, 2009), or the trust required to ensure sensitive transactions (Pfitzmann, Pfitzmann, Schunter, & Waidner, 1997), we need to create a framework of security checks, trust assurances, and transaction protections before permitting the exchange of sensitive information. The CAP framework (checks, assurances, protections) will ensure secure interactions among mobile applications no matter what the specific platform.

CAP Framework Solution

In order to be an all-inclusive security framework malleable to the various types of attacks in order to protect transaction, as well as anticipate new attack vectors, the CAP must maintain three security tenets of confidentiality, integrity, and availability**:**

- Confidentiality: All data flow and stored information must be protected against those who should not have access. This includes strong authentication protocols and strong data encryption both during exchange and storage of data.
- Integrity: All data must be trustworthy and any changes to the data must be valid according to set parameters. This includes concepts such as data and source integrity.
- Availability: All data within an information system needs to accessible when it is accessed. No matter how secure an information system, it should allow authorized users to access information and supporting system frameworks need to ensure that the information is always obtainable. This includes databases, servers, networks, and all parts of the information system to include mobile devices that are accessing it from external networks.

Since we are dealing with mobile transaction between software agents (e.g., server and mobile client) we must also add additional layers to support CIA, as well as transactional security and trust. These additional layers address weaknesses or gaps in the existing standards:

- Authenticity: Although CIA addresses confidentiality, in a mobile solution the communicating components (e.g., mobile device and server) need to authenticate against each other in addition to user authentication. We can address this somewhat with SSL and shared certificates, but with sensitive information we need to ensure that the participants are who they say they are. Too often certificate spoofing can result in compromised systems (Fisher, 2012) so more needs to be in place.
- Assurance: After we authenticate mobile agents and servers, we need to assure secure transactions and communications. In mobile environments, a user may move between networks in a short period of time. The system must constantly check for a secure connection before transmitting the next burst of data.
- Reliability: We must also take into account the reliability of the mobile platforms and applications (i.e., "apps") that users employ to access sensitive personal information. Without constant validation, viruses can infect apps and still maintain a coherent, healthy app signature thereby impacting data and system CIA.

By combining the standard CIA requirements with the additional components of authenticity, assurance, reliability (CIA3R) we create a multi-layered secure transactional communication that assures trusting interaction and exchange of information via mobile platforms.

FUTURE RESEARCH AND CONCLUSION

The proposed CAP framework is only one proposed solution to safeguard mobile healthcare information access and storage. More research and testing will be done within this framework which will result in developed prototypes that can be tested using, at first, sample data and later real time interactions. Additional research is needed refine the CIA3R layers before implementing them in CAP as well.

Without additional research in the area of mobile apps and healthcare information access, we will see more data leakage as more users rely on mobile devices.

WORKS CITED

Burkle, J., Hertle, A., Muller, W., & Wieser, M. (2009). Evaluating the security of mobile application platforms. *Autonomous Agent, Multi-Agent Systems*, 395-311.

EPIC. (2013, September 8). *Mobile Applications and Portals*. Retrieved September 8, 2013, from EPIC: http://www.epic.com/software-phr.php

Fidelman, M. (2012, May 2). *The Latest Infographics: Mobile Business Statistics For 2012*. Retrieved September Sunday, 2013, from Forbes: http://www.forbes.com/sites/markfidelman/2012/05/02/the-latest-infographics-mobile-business-statistics-for-2012/

Fisher, D. (2012, October 31). *Final Report on Diginotar Hack Shows Total Compromise of CA Servers*. Retrieved September 8, 2013, from threatpost: http://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170

Jansen, W. (2000). Countermeasures for mobile agent security. *Computer Communications*, 1667-1676.

Pfitzmann, A., Pfitzmann, B., Schunter, M., & Waidner, M. (1997). Trusting Mobile User Devices and Security Modules. *Computer*, 61-67.