

Achieving Information Security in the IoT-Based Nursing Information Systems: An Essential Challenge for the Future of Nursing Informatics

Battulle Prashansa Rao, MS

Co-presenters: Ketan Patil and Gunes Akif

Abstract

Problem Statement: Preserving the security of information stored and exchanged over the network is becoming a major challenge for the health information systems based on the Internet of Things (IoT). Therefore, achieving information security for these systems will be an essential topic for the future of nursing informatics. In this study, we tackled a problem of leveraging and improving the existing IT security standards and practices used in IoT-based healthcare information systems that will exchange data extensively over the network. **Methods:** To establish a framework and methodological focus, we carried out an extensive literature review of current information security standards. This framework was used to customize and adapt the security standards and guidelines of IoT information systems to be implemented in nursing informatics. To examine and validate the relevance of this framework, the identified standards and practices (e.g., static code analysis) were applied to a real life IoT-based healthcare information system. The identified security problems were used to prepare a prioritized test plan. This prioritization plan was then used to test the system using security testing techniques such as Uniform Resource Locator (URL) manipulation, Structured Query Language (SQL) Injection, Cross-site scripting (XSS), etc. **Results:** Based on our literature review, four major information security standards were identified and used to formulate a security framework. The analysis of the interconnected healthcare system based on this security framework revealed that the system implementation and adoption failed to follow security standards and best practices. Some of the implemented security standards lacked documentation of procedures and policies to be followed in case of emergencies. The overall set of security policies and standards followed were insufficient in protecting the system from attackers and malicious users. It was also found that the code base consists of various possible security vulnerabilities which can be exploited easily. Almost 1,000 security warnings were found using SCA tools which includes warnings of possible malicious code and SQL injection. Around 17% of the code depended on external system, which helps to interact and retrieve data from external repositories. This makes the existing IoT based healthcare information system vulnerable to more attacks. The prioritized security testing revealed that very little effort was applied by the source code vendor to ensure that the system was built securely, thus resulting in leaking of private and confidential data to attackers. During URL manipulation testing, around 1,600 URLs were found to be leaking highly sensitive data and allowed invalid access to the system; these can be considered major information security problems. **Significance:** Security of vital medical information is of utmost importance. Leveraging the existing information security standards and practices of IoT based nursing information systems provides useful and interesting insights to the executives and government officials responsible for implementing and managing these interconnected healthcare systems. This study demonstrates that improvement in established IT security guidelines can help decision makers and experienced professionals in effectively monitoring, identifying, and responding to challenges associated with security breaches in interconnected healthcare systems.