The College of Graduate Studies and the College of Information Technology Cordially Invite You to a

Master Thesis Defense

Entitled

AUTHENTICATED KEY ESTABLISHMENT PROTOCOL FOR CONSTRAINED SMART HEALTHCARE SYSTEMS BASED ON PHYSICAL UNCLONABLE FUNCTION

by

Abdalla Saleh Elkushli

Faculty Advisor

Dr. Farag Sallabi, College of Information Technology

Date & Venue

1:30 pm
Monday, 18 April 2022
Room 1021 , E1 Building

Abstract

Smart healthcare systems are one of the critical applications of the internet of things. They benefit many categories of the population and provide significant improvement to healthcare services. Smart healthcare systems are also susceptible to many threats and exploits because they run without supervision for long periods of time and communicate via open channels. Moreover, in many implementations, healthcare sensor nodes are implanted or miniaturized and are resource-constrained. The potential risks on patients/individuals' life from the threats necessitate that securing the connections in these systems is of utmost importance. This thesis provides a solution to secure end-to-end communications in such systems by proposing an authenticated key establishment protocol. The main objective of the protocol is to examine how physical unclonable functions could be utilized as a lightweight root of trust. The protocol's design is based on rigid security requirements and inspired by the vulnerability of physical unclonable function to machine learning modeling attacks as well as the use of a ratchet technique. The proposed protocol verification and analysis revealed that it is a suitable candidate for resource-constrained smart healthcare systems. The proposed protocol's design also has an impact on other important aspects such as anonymity of sensor nodes and gateway-lose scenario.

Keywords: authenticated key establishment, perfect forward secrecy, PUF, root of trust, smart healthcare systems, resource-constrained.