University of Victoria | Graduate Studies

Notice of the Final Oral Examination for the Degree of Doctor of Philosophy

of

MOHAMMED MUJIB ALSHAHRANI

MEng (Dalhousie University, 2013)
BSc (University of Saudi Arabia, 2009)

“Secure and Lightweight Authentication Schemes for Internet of Things (IoT)”

Department of Electrical and Computer Engineering

Wednesday, October 16, 2019
9:00 A.M.
Clearihue Building
Room B007

Supervisory Committee:
Dr. Issa Traore, Department of Electrical and Computer Engineering, University of Victoria (Supervisor)
Dr. Fayez Gebali, Department of Electrical and Computer Engineering, UVic (Member)
Dr. Hausi Müller, Department of Computer Science, UVic (Outside Member)

External Examiner:
Dr. Alireza Sadeghian, Department of Computer Science, Ryerson University

Chair of Oral Examination:
Dr. George Tzanetakis, Department of Computer Science, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

IoT platforms face huge challenges in deploying robust authentication mechanisms due to the fact that edge devices and resource-constrained devices may not have enough compute and storage capability to deploy and run existing mechanisms, which involve in general complex computations. Moreover, establishing end-to-end device authentication in the Internet of Things (IoT) networks is challenging because of the heterogeneous nature of IoT devices. One of the well-known challenges confronting the IoT infrastructure is related to authentication. Many IoT devices rely on weak authentication schemes, which has led in the last few years to several successful and widely publicized hacking incidents. According to the ISO/IEC 27002 standard, authentication is the process of determining whether something is, in fact, what it is declared to be. Authentication is considered the main gate to protect IoT networks from various security threats; determining who the entity is (authentication) is of high importance to establish a secure session between IoT devices. In this thesis, I identified gaps in the literature and investigated new authentication schemes and security mechanisms to improve IoT security and privacy against common attacks such as replay and impersonation. IoT security and privacy are enhanced by introducing a new lightweight mutual authentication and key exchange protocol for IoT based on dynamic identity and cumulative chained-hash. Nodes can anonymously and mutually authenticate and establish a session with the controller node using dynamic identities and temporary symmetric keys in an unlinkable and untraceable manner. Moreover, the enforcement of security policies between nodes is guaranteed by setting up virtual domain segregation and restricting nodes capabilities of sending and receiving data to or from other nodes. Cumulative chained-has his introduced as a way to ensure the identity of the sender (through challenge-response). Additionally, we introduce a new anonymous device-to-device mutual authentication and key exchange protocol based on the ZigBee technique. The proposed protocol relies on symmetric encryption and counter and enables IoT devices to authenticate in the network and agree on a shared secret session key when communicating with each other via a trusted intermediary (home controller). To achieve perfect forward secrecy, the session keys are changed frequently after every communication session. The proposed scheme achieves secure, anonymous authentication with the unlinkability and untraceability of IoT devices' transactions.

The security of the protocols is evaluated and simulated using three different methods: informal analysis, formal analysis using the Burrows–Abadi–Needham logic (BAN), and model-checking using the automated validation of Internet security protocols and applications (AVISPA) toolkit. The overhead and efficiency of the proposed schemes are analyzed and compared with other related schemes.