Ensuring Application Specific Security, Privacy and Performance Goals in RFID Systems

Farzana Rahman

Monday, December 03, 2012
9:00 a.m.
Cudahy 401

Committee
Dr. Dennis Brylow, Associate Professor
Department of Mathematics, Statistics, and Computer Science, Marquette University, WI, USA

Dr. Praveen Madiraju, Associate Professor
Department of Mathematics, Statistics, and Computer Science, Marquette University, WI, USA

Dr. Mohammad Zulkernine, Associate Professor
School of Computing, Queens University, Ontario, Canada

Dr. Rumi Ahmed Khan, Associate Professor
Florida State University, College of Medicine, Tallahassee, FL

Abstract
Radio Frequency IDentification (RFID) is an automatic identification technology that uses radio waves to identify objects such as products, animals or persons. Due to the constraints on memory, power, storage capacity, and amount of logic on RFID devices, traditional public key based strong security mechanisms are unsuitable for them. Usually, low cost authentication protocols are used to secure RFID systems. However, the generic authentication protocols provide relatively low performance for different types of RFID applications. In this dissertation, we identified that each RFID application has unique research challenges and different performance bottlenecks based on the characteristics of the system. One strategy is to devise security protocols such that application specific goals are met and system specific performance requirements are maximized.

This dissertation aims to address the problem of devising application specific security protocols for current and next generation RFID systems so that in each application area maximum performance can be achieved and system specific goals are met. In this dissertation, we propose four different authentication techniques for RFID technologies, providing solutions to the following research issues: 1) Detecting counterfeit as well as ensuring low response time in large scale RFID systems, 2) Preserving privacy and maintaining scalability in RFID based healthcare systems, 3) Ensuring security and survivability of Computational RFID (CRFID) networks, and 4) Detecting missing WISP tags efficiently in CRFID based critical systems. Since ensuring security is the common goal in most RFID systems, we propose authentication protocols that use low cost operations like hash functions, XOR operations and pseudorandom number generation to ensure security and other application specific goals. In this dissertation, we also present the evaluation results of our proposed methodologies.

Open to the Public