

COMPUTER SCIENCE COLLOQUIUM

Department of Computer Science
City University of Hong Kong

Lightweight Secure Search Protocols for Low-cost RFID Systems

Dr GUAN Yong
Associate Professor
Department of Electrical and Computer Engineering
Iowa State University
USA

Date :

6 August 2009 (Thursday)

Time :

11:30am - 12:30pm (Refreshment will be served at 11:15am)

Venue :

CS Seminar Room, Room Y6405, 6th Floor, Yellow Zone, Academic Building,
City University of Hong Kong, Tat Chee Avenue, Kowloon Tong

Abstract

RFID technology can potentially be used in many applications. A typical RFID system involves a reader and a number of tags, which may range from the battery-powered tags that have Wi-Fi capabilities, to the low-cost tags that are constrained in computation capacities and hardware resources. Keeping RFID systems secure is crucial since RFID systems are vulnerable to a number of malicious attacks. As for low-cost RFID systems, security problems become much more challenging, because traditional security mechanisms are infeasible to be used on low-cost tags due to their resource constraints. Tag search is an important functionality that a RFID system should provide. In this research, we study how to secure tag search with a focus on low-cost RFID systems. Existing solutions are mostly based on hash functions and consume 8000 to 10000 gates, however, the low-cost tags can afford at most 2000 gates for secure features. In this work, we propose several lightweight secure search protocols based on Linear Feedback Shift Registers (LFSR) and Physically Unclonable Functions (PUF). Our protocols prevent adversaries from learning tag identity and impersonating RFID reader or tags. Experimental results show that our solutions have hundreds of nanoseconds processing time and require no more than 1400 hardware gates on tags.

Biography

Dr Yong Guan is an Associate Professor of Electrical and Computer Engineering at Iowa State University. He received his Ph.D. degree in Computer Science from Texas A&M University in 2002, MS and BS degrees in Computer Science from Peking University in 1996 and 1990, respectively. He has been working on networking and distributed systems, with focuses on security and privacy issues, including computer and network forensics, wireless and sensor network security, and privacy-enhancing technologies for the Internet. He is the leading PI for IARPA/DTO/ARDA-funded Network Attack Attribution Project and several NSF-funded security projects. His research have addressed issues in digital forensics, anonymity, secure network coding, key management, secure localization services, and intrusion and online fraud detection. He served as the general chair of 2008 IEEE Symposium on Security and Privacy (Oakland 2008, the top conference in security) and the vice program chair for ICDCS 2008 (Security and Privacy Area). Dr Guan has been recognized by various awards, including the Best Paper Award from the IEEE National Aerospace and Electronics Conference in 1998, the 2nd place graduate winner in the international ACM student research contest in 2002, NSF Career Award in 2007, ISU Award for Early Achievement in Research in 2007, the Litton Industries Professorship in 2007, and the Outstanding Community Service Award of IEEE Technical Committee on Security and Privacy, 2008.

* * * * *

*In case of questions, please contact Prof Weijia Jia at Tel: 2788 9701, E-mail: wei.jia@cityu.edu.hk,
or visit the CS Departmental Seminar Web at <http://www.cs.cityu.edu.hk/>.*