

COMPUTER SCIENCE SEMINAR SERIES

Department of Computer Science
City University of Hong Kong
(Departmental Seminar 2006/2007 - No 59)

MiniSec and Message in a Bottle

Mr LUK Mark
PhD Candidate

Electrical and Computer Engineering Department
Carnegie Mellon University
USA

Date :

13 June 2007 (Wednesday)

Time :

2:00pm - 3:00pm (Refreshment will be served at 1:45pm)

Venue :

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

Abstract

MiniSec

Secure sensor network communication protocols need to provide three basic properties: data secrecy, authentication, and replay protection. Secure sensor network link layer protocols such as TinySec and ZigBee enjoy significant attention in the community. However, TinySec achieves low energy consumption by reducing the level of security provided. In contrast, ZigBee enjoys high security, but suffers from high energy consumption.

MiniSec is a secure network layer that obtains the best of both worlds: low energy consumption and high security. MiniSec has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication. The latter does not require per-sender state for replay protection and thus scales to large networks. We present a publicly available implementation of MiniSec for the Telos platform, and experimental results demonstrate our low energy utilization.

Message in a Bottle

Existing protocols for secure key establishment all rely on an unspecified mechanism for initially deploying secrets to sensor nodes. However, no commercially viable and secure mechanism exists for initial setup. Without a guarantee of secure key deployment, the traffic over a sensor network cannot be presumed secure.

To address this problem, we present a user-friendly protocol for the secure deployment of cryptographic keys in sensor networks. We propose a collection of five techniques to prevent an attacker from eavesdropping on key deployment. To demonstrate feasibility for real-world use, we implement our protocol on Telos motes and conduct a user study.

Biography

Mark Luk is a PhD candidate in Electrical and Computer Engineering at Carnegie Mellon University. He completed his Masters degree in Information Security at Carnegie Mellon University under Prof. Adrian Perrig. Prior to that, he received his Bachelors degree in Computer Science from University of California at Berkeley. His research interests revolve around sensor network security and systems security. More information about his research can be found at www.ece.cmu.edu/~mluk.

* * * * *

*In case of questions, please contact Dr Duncan Wong at Tel: 2788 8020, E-mail: duncan@cityu.edu.hk /
Dr Guoliang Xing at Tel: 2788 7525, E-mail: glxing@cs.cityu.edu.hk, or
visit the CS Departmental Seminar Web at <http://www.cs.cityu.edu.hk/>.*