

SEMINAR

Security analysis and new composition of broadcast authentication for wireless sensor networks

**by Taekyoung Kwon
Sejong University, Seoul, Korea**

**Friday, May 2nd, 2008
11:00 AM**

Science and Technology II, room 100A

Abstract

In this talk, I would like to present the recent result of security analysis and new composition of broadcast authentication for wireless sensor networks. Technological advancement in large scale distributed networking and small low-powered sensor devices has led to the development of wireless sensor networks in unattended and even hostile environments. Such networks may need broadcast authentication for allowing a based station to send commands and requests to distributed sensor nodes in an authentic manner. The well known broadcast authentication schemes based on the delayed exposure of one-way key chains are devised for efficiency in resource-limited sensor nodes. This talk firstly shows that such schemes with 64-bit key chains (desired for efficiency) disclose partial future keys through time memory data tradeoff techniques, and become severely less efficient in computation and buffer occupation for possible sleep modes, network failures, and idle sessions of networks. Secondly, a new scheme is presented for resolving those problems by composing two levels of chains that have distinct intervals and mutually authenticate each other. This allows the short key chains to continue indefinitely and efficiently for sensor nodes, and makes new interesting strategies and management methods possible. The talk will be given mostly in abstract but some concrete results will be shown.

Short bio:

(1988-1999) BS, MS, and Ph.D. in Computer Science, Yonsei University, Seoul, Korea.

(1999-2000) PostDoc at U.C. Berkeley - funded by KOSEF and Samsung Electronics.

(2001-present) Associate Professor in Computer Eng., Sejong University, Seoul, Korea

(2007-present) Visiting Research Associate at UMD. (working with Prof. Virgil Gligor)