In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Randomness and Wireless Security

by

Professor Don Towsley
Distinguished Professor
Department of Computer Science
University of Massachusetts

Date	**:**	**24 Feb., 2012 (Fri.)**
Time	**:**	**10:30-11:30am**
Venue	**:**	**Room 833 Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

Abstract

The wireless media is a rich source of randomness. In this talk we focus on two problems in securing wireless communication. In the first part we describe a practical way to harness this randomness to provide and/or improve the security of wireless communications. We introduce the notion of "dynamic secrets", information shared by two parties, Alice and Bob, engaged in communication and not available to an adversary, Eve. The basic idea is to dynamically generate a series of secrets from inevitable transmission errors and other random factors present in wireless communications. These dynamic secrets exhibit interesting security properties and offer an alternative or complement to existing security protocols. As part of the talk we will present a simple algorithm for generating these secrets and using them to update a shared key.

In the second part of our talk we focus on the use of randomness so as to avoid detection of the communications. Here the challenge is for Alice to communicate with Bob without an adversary, Willie the warden ever realizing that the communication is taking place. Specifically, we show that Alice can send O(\sqrt{n}) bits to the Bob in n channel uses with probability of detection by the Willie less than \epsilon for any \epsilon > 0. Conversely, attempting to transmit more than O(\sqrt{n}) bits either results in detection by Willie with probability one or a non-zero probability of decoding error as n -> \infinity.

Biography

Don Towsley holds a B.A. in Physics (1971) and a Ph.D. in Computer Science (1975) from University of Texas. He is currently a Distinguished Professor at the University of Massachusetts in the Department of Computer Science. He has held visiting positions at numerous universities and research labs. His research interests include networks and performance evaluation.

He currently serves on the editorial boards of IEEE Journal on Selected Areas in Communications and previously served as Editor-in-Chief of IEEE/ACM Transactions on Networking and on numerous other editorial boards. He has served as Program Co-chair of several conferences.

He has received the 2007 IEEE Koji Kobayashi Award, several lifetime achievement awards, a 2008 SIGCOMM Test-of-Time Paper Award, the 1998 IEEE Communications Society William Bennett Best Paper Award, and numerous conference/workshop best paper and test of time awards. Last, he has been elected Fellow of both the ACM and IEEE.

**** ALL ARE WELCOME ****

Host: Professor Dah-Ming Chiu (Tel: 3943-8357, Email: dmchiu@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)