

NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Randomness, Everlasting Security, and Undetectability**

Speaker: Professor Don Towsley
 Department of Computer Science
 University of Massachusetts

Date/Time: 22 January 2015, Thursday, 10:00 AM to 12:00 PM

Venue: Executive Classroom, COM2-04-02

Chaired by: Dr Tay Yong Chiang, Professor, School of Computing
 (tayyc@comp.nus.edu.sg)

Abstract:

Security and privacy are fundamental concerns in today's world. These concerns have become particularly prominent with the revelations of Edward Snowden of the awareness that the US National Security Agency has regarding our daily communications. These revelations have shown traditional security techniques to be vulnerable and calling into question whether or not security and privacy can be provided. In this talk we investigate how randomness in the environment can be used to provide everlasting security and undetectability (privacy) in wireless communications. In the first part of the talk we describe a practical way to harness this randomness to provide and improve 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 randomness present in the in wireless environment. Dynamic secrets exhibit interesting security properties and offer a robust alternative to cryptographic security protocols. We present a simple algorithm for generating these secrets and using them to ensure secrecy.

In some situations, Alice and Bob may want not only to secure their communications but to keep them private. In the second part of our talk we focus on the use of randomness to conceal their 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 establish that Alice can send $O(t^{1/2})$ bits (and no more) to Bob in time t over a variety of wireless and optical channels. Moreover, we report experimental results that corroborate the theory.

Biodata:

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 as a Co-Editor-in-Chief of ACM Transactions on Modeling and Performance Evaluation of Computer Systems (TOMPECS) and previously as Editor-in-Chief of IEEE/ACM Transactions on Networking, and on numerous editorial boards. He has served as Program Co-chair of several conferences including INFOCOM 2009.

He has received numerous awards including the 2007 IEEE Koji Kobayashi Award, and numerous paper awards including a 2008 ACM SIGCOMM Test-of-Time Paper Award and the 2012 ACM SIGMETRICS Test-of-Time Award. Last, he has been elected Fellow of both the ACM and IEEE.