NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **A Next-generation Secure Internet Architecture for the 21st Century**

Speaker: Professor Adrian Perrig
Department of Computer Science
ETH Zurich, Switzerland

Date/Time: 9 November 2016, Wednesday, 11:00 AM to 12:30 PM

Venue: Executive Classroom, COM2-04-02

Chaired by: Dr Kang Minsuk, Assistant Professor, School of Computing
(kangms@comp.nus.edu.sg)

Abstract:

The Internet has been successful beyond even the most optimistic expectations. It permeates and intertwines with almost all aspects of our society and economy. The success of the Internet has created a dependency on communication as many of the processes underpinning the foundations of modern society would grind to a halt should communication become unavailable. However, much to our dismay, the current state of safety and availability of the Internet is far from commensurate given its importance.

Although we cannot conclusively determine what the impact of a 1-day or 1-week outage of Internet connectivity on our society would be, anecdotal evidence indicates that even short outages have a profound negative impact on society, businesses, and government. Unfortunately, the Internet has not been designed for high availability in the face of malicious actions by adversaries. Recent patches to improve Internet security and availability have been constrained by the current Internet architecture, business models, and legal aspects. Moreover, there are fundamental design decisions of the current Internet that inherently complicate secure operation.

Given the diverse nature of constituents in today's Internet, another important challenge is how to scale authentication of entities (e.g., AS ownership for routing, name servers for DNS, or domains for TLS) to a global environment. Currently prevalent PKI models (monopoly and oligarchy) do not scale globally because mutually distrusting entities cannot agree on a single trust root, and because everyday users cannot evaluate the trustworthiness of each of the many root CAs in their browsers.

To address these issues, we propose SCION, a next-generation Internet architecture that is secure, available, and offers privacy by design; that provides incentives for a transition to the new architecture; and that considers economic and policy issues at the design stage. We have

implemented SCION and deployed it in the production networks of 2 ISPs.

Biodata:

Adrian Perrig is a Professor at the Department of Computer Science at ETH Zurich, Switzerland, where he leads the network security group. He is also a Distinguished Fellow at CyLab, and an Adjunct Professor of Electrical and Computer Engineering, and Engineering and Public Policy at Carnegie Mellon University. From 2002 to 2012, he was a Professor of Electrical and Computer Engineering, Engineering and Public Policy, and Computer Science (courtesy) at Carnegie Mellon University; from 2007 to 2012, he also served as the technical director for Carnegie Mellon's Cybersecurity Laboratory (CyLab). He earned his Ph.D. degree in Computer Science from Carnegie Mellon University under the guidance of J.D. Tygar, and spent three years during his Ph.D. degree at the University of California at Berkeley. He received his B.Sc. degree in Computer Engineering from EPFL. Adrian's research revolves around building secure systems -- in particular his group is working on the SCION secure future Internet architecture.