NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Cookies Lack Integrity: Real-World Implications**

Speaker: Professor Haixin Duan
Tsinghua University, China

Date/Time: 30 May 2017, Tuesday, 02:00 PM to 03:30 PM

Venue: Executive Classroom, COM2-04-02

Chaired by: Dr Liang Zhenkai, Associate Professor, School of Computing
(liangzk@comp.nus.edu.sg)

Abstract:

A cookie can contain a "secure" flag, indicating that it should be only sent over an HTTPS connection. Yet there is no corresponding flag to indicate how a cookie was set: attackers who act as a man-in-the-middle even temporarily on an HTTP session can inject cookies which will be attached to subsequent HTTPS connections. Similar attacks can also be launched by a web attacker from a related domain. Although an acknowledged threat, it has not yet been studied thoroughly. This paper aims to fill this gap with an in-depth empirical assessment of cookie injection attacks. We find that cookie-related vulnerabilities are present in important sites (such as Google and Bank of America), and can be made worse by the implementation weaknesses we discovered in major web browsers (such as Chrome, Firefox, and Safari). Our successful attacks have included privacy violation, online victimization, and even financial loss and account hijacking. We also discuss mitigation strategies such as HSTS, possible browser changes, and present a proof-of-concept browser extension to provide better cookie isolation between HTTP and HTTPS, and between related domains.

Biodata:

Haixin Duan is a Professor at Tsinghua University, China, and a visiting scholar of ICSI at UC Berkeley. He is in charge of the Network and Information Security Lab, and the Security Response Team of China Education and Research Network (CCERT). His main research interest is network security, including DNS security, web security, intrusion detection and anonymous communication. He has been actively publishing in top system and network security journals and conferences (IEEE S&P, CCS, USENIX Security and NDSS), and serving as members of their technical program committees. One of his paper is awarded the Distinguished Paper in NDSS 2016. He is also the co-founder of the "Blue Lotus" CTF team. Prof. Duan obtained his B.S. from Harbin Institute of Technology, and Ph.D. from Tsinghua University.

His full publication list is at:
http://netsec.ccert.edu.cn/duanhx/?page_id=1307