NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Observer-Resistant Password Systems: How hard to make them both usable and secure?**

Speaker: Dr Shujun Li
Deputy Director of the Surrey Centre for Cyber Security (SCCS)

Date/Time: 25 April 2017, Tuesday, 02:00 PM to 03:30 PM

Venue: Video Conference Room, COM1-02-13

Chaired by: Dr Chang Ee Chien, Associate Professor, School of Computing (changec@comp.nus.edu.sg)

Abstract:

Observer-resistant password systems (ORPSs, also known as human authentication against observers or leakage-resilient password systems) have been studied since the early 1990s in both cryptography and computer security contexts, but until today a both secure and usable ORPS remains an open question to the research community. The concept of ORPS can be used to cover a large family of attacks against password-based human authentication systems such as shoulder surfers, hidden cameras, man-in-the-middle, keyloggers and malware. A key assumption of ORPS is that human users must respond to authentication challenges without using any computational devices. In other words, the threat model behind ORPSs assumes that other than the human user's brain, nothing is trusted. The main security requirement is to avoid disclosure of the shared secret between the human user and the verifier (i.e., password) even after a practically large number of authentication sessions observed by an untrusted party.

According to Yan et al.'s NDSS 2012 paper which reviews research efforts on this topic for over two decades, it has been clear that no existing systems meet both security and usability requirements although many meet one well. In this talk, the speaker will introduce his research on ORPSs since the early 2000s, highlighting a number of key findings such as human behavioural based timing attack reported at SOUPS 2011 and some theoretical work reported at NDSS 2013 and IEEETIFS 2015. He will contextualise some part of his talk using a particular design of ORPS called Foxtail, one of those ORPSs whose implementations were shown to have a relatively better balance between security and usability. Known rules about designing ORPSs and future research directions will also be discussed. He will also introduce an ongoing Singapore-UK project with Singapore Management University related to ORPSs, which is about using cognitive modelling to automate security evaluation of user authentication systems against human behaviour based attacks.

At the beginning of his talk, the speaker will also introduce ongoing research activities and research projects at the Surrey Centre for Cyber Security (SCCS) of the University of Surrey, UK. He will list some ways to collaborate with cyber security researchers in Singapore.

Biodata:

Dr Shujun Li is a Deputy Director of the Surrey Centre for Cyber Security (SCCS), leading its cross-cutting research theme "Human Factors" and contributing to several other research themes especially "Privacy and Authentication" and "Multimedia Security and Forensics". He joined the University of Surrey in 2011 and is currently a Reader (Associate Professor) at Surrey's Department of Computer Science. His main research interests are mostly around interdiscplinary topics covering several different areas including cyber security (including privacy), human factors (including human-computer interface), digital forensics and cybercrime, multimedia computing, cognitive science, and applications of artificial intelligence. He has been working on a number intredisciplinary research projects as the principal investigator (PI) including one on applications of cognitive modelling in cyber security (COMMANDO-HUMANS), one on human-assisted machine learning for data loss prevention (H-DLP), and one on better approaches to understanding and influencing human behaviours for reducing human-related risks (ACCEPT). Trained as an electronic engineer and currently working at a Computer Science department, Dr Li is actively working with researchers from other disciplines especially Electronic Engineering, Psychology, Sociology and Business. Dr Li is a Senior Member of IEEE, a Professional Member of ACM, and a Global Member of the Internet Society. From 2009-2011 he was a member of MPEG (ISO/IEC JCT 1/SC 29/WG 11), and in 2012 was awarded an ISO/IEC Certificate of Appreciation for being the lead editor of ISO/IEC 23001-4:2011 "Information technology - MPEG systems technologies - Part 4: Codec configuration representation", the 2nd edition of the MPEG RVC standard. Dr Li has published around 100 publications at international conferences and journals, and his work has attracted over 5000 citations (Google Scholar). He is the co-editor of the Handbook of Digital Forensics of Multimedia Data and Devices, published by Wiley in 2015. He is currently on the editorial boards of 5 international journals and was serving on the orgnising and technical program committes of many conferences and workshops. He has two cyber security related patent applications pending, and is working very closely with industry and governmental organisations for his research. Although not a mathematician or a theoretical computer scientist, his current Erdos Number is 3 through at least two different routes.