THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Department of Computing
電子計算學系

Research Seminar

TLS Interception Mechanisms, Motivations and Lessons Learned

Dr Xavier de Carné de Carnavalet
Research Assistant Professor
Department of Computing
The Hong Kong Polytechnic University
Hong Kong

Date : 18 December 2020 (Friday)
Time : 11:00 a.m. - 12:00 noon

▶ Abstract

TLS is an end-to-end network protocol designed to provide confidentiality and integrity guarantees that improve end-user security and privacy. While TLS helps defend against pervasive surveillance of intercepted unencrypted traffic, it also hinders several common beneficial operations typically performed by middleboxes on the network traffic. This issue has resulted in some parties proposing various methods that "bypass" the confidentiality goals of TLS by playing with keys and certificates essentially in a man-in-the-middle solution, and leads to new proposals that extend the protocol to accommodate third parties, delegation schemes to trusted middleboxes, and fine-grained control and verification mechanisms. In this talk, we will first review the use cases for access to plaintext traffic despite the use of TLS, including the industry point of view. Then, we will explore the panorama of techniques and proposals by which TLS no longer delivers end-to-end security, and by which the notion of an "end" changes. In particular, we will discuss two very different approaches, mcTLS and delegated credentials, and make observations useful for researchers to understand what makes a technical proposal successful in the real world.

▶ About the Speaker

Dr Xavier de Carné de Carnavalet is a newly appointed Research Assistant Professor in the Department of Computing at PolyU. He obtained his Ph.D. from Concordia University, Canada, and was a postdoctoral fellow in the Department of Computing at Carleton University. He earned an M.A.Sc. from Concordia University and a Dipl-Ing./M.Sc. from École Supérieure d'Informatique Électronique Automatique (ESIEA) of Paris, France. His research targets real-world security and privacy problems that affect the public at large. One of the major directions of his research is to measure and improve user privacy and security from threats posed by software, web technologies and services. He has made contributions in the fields of passwords and authentication, reproducible builds, and secure communication interception, and published at top-tier venues such as NDSS, TISSEC, and TIFS. His work received several awards including the prestigious NSERC Vanier Canada Graduate Scholarship.

ALL are welcome!

Enquiries : Professor George Baciu
Email : csgeorge@polyu.edu.hk
Tel : 2766 7272

We drive innovation through
SMART COMPUTING