SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
Faculty of Engineering
Website: https://www.eng.nus.edu.sg/ece/

Area: Communications & Networks

Host: Prof Lim Teng Joon

TOPIC	**:**	**TLS Beyond the Browser: Combining End Host and Network Data to Understand Application Behavior**
SPEAKER	**:**	**Dr Blake Anderson,** **Cisco Networks**
DATE	**:**	**19 November 2019, Tuesday**
TIME	**:**	**10am to 11am**
VENUE	**:**	**E5-02-32, Engineering Block E5, Faculty of Engineering, NUS**

ABSTRACT

The Transport Layer Security (TLS) protocol has evolved in response to different attacks and is increasingly relied on to secure Internet communications. Web browsers have led the adoption of newer and more secure cryptographic algorithms and protocol versions, and thus improved the security of the TLS ecosystem. Other application categories, however, are increasingly using TLS, but too often are relying on obsolete and insecure protocol options.

To understand in detail what applications are using TLS, and how they are using it, we developed a novel system for obtaining process information from end hosts and fusing it with network data to produce a TLS fingerprint knowledge base. This data has a rich set of context for each fingerprint, is representative of enterprise TLS deployments, and is automatically updated from ongoing data collection. Our dataset is based on 471 million endpoint-labeled and 8 billion unlabeled TLS sessions obtained from enterprise edge networks in five countries, plus millions of sessions from a malware analysis sandbox. We actively maintain an open source dataset that, at 4,500+ fingerprints and counting, is both the largest and most informative ever published. In this paper, we use the knowledge base to identify trends in enterprise TLS applications beyond the browser: application categories such as storage, communication, system, and email. We identify a rise in the use of TLS by non-browser applications and a corresponding decline in the fraction of sessions using version 1.3. Finally, we highlight the shortcomings of naively applying TLS fingerprinting to detect malware, and we present recent trends in malware's use of TLS such as the adoption of cipher suite randomization.

BIOGRAPHY

Blake Anderson currently works as a Senior Technical Leader in Cisco's Advanced Security Research team. Since starting at Cisco in early 2015, he has participated in and led projects aimed at improving (encrypted) network traffic analysis, which has resulted in open source projects, academic publications, and patents. He and his collaborators published the initial research that eventually became Cisco's Encrypted Traffic Analytics (ETA) solution. Before Cisco, Blake received his PhD in machine learning/security from the University of New Mexico and worked at Los Alamos National Laboratory as a staff scientist.