Security Analytics and Intelligence

Yeali S. Sun

Department of Information Management

National Taiwan University

Taipei, Taiwan

Abstracts:

Cyber criminals are more sophisticated and more determined than ever. Running security operations center is facing new challenges. Five main areas of capabilities are essential to the SOC operations for combating attacks and threats: effective detection, intelligent analysis, event reporting, forensics, and recovery. In this talk, I will present the two works that we currently focus on in building up a security analytics and intelligence platform. We consider an important and indispensable solution that is required and important to security management to escalate cyber defense is a platform equipped with a wide range of security analytics tools for choice and a security intelligence system. By taking advantage of cloud computing and big data technology, we are building a system that supports real-time, interactive, visualized communication map for effective security analysis. The system aims to process enormous volumes of data collected from various network traffic points to aid real-time interactive security incident analysis and forensics. We also research malware profiling and malware detection of embedded mobile system in cyber-physical systems. We extend the virtual machine introspection (VMI) techniques for Android system and develop VMI library to bridge the semantic gap between the virtual machine monitor, guest OS and the customized Java VM inside the Android to map low-level information. Moreover, we also look into adding taint analysis tool to the security analysis platform to identify the vulnerability in a host so to patch and to assess the scope of infection and harm.