Defending End Users and Service Providers from Emerging Security Threats

Wei Meng
Chinese University of Hong Kong

2/28/2019 at 10:30 am
CoRE A 301

Abstract

The World Wide Web is the primary tool that billions of people use to interact over the Internet on a daily basis. The web makes available a large variety of important services and applications, such as search, social networking, banking and shopping. Because of their increasing importance to organizations, businesses and individual users, web applications have become the primary targets for attackers. For example, attackers target individual users by launching injection attacks and phishing attacks at the client side, and target enterprises and organizations by exploiting vulnerabilities at the server side.

In this talk, I will introduce two systems that I built to address two emerging threats against the end users and the service providers. First, I will present Observer, a browser-based analysis framework for systematically investigating click interception on the web. With Observer, we detected 437 malicious third-party scripts that intercept user clicks on over 600 websites with 43 million daily visits combined. Next, I will introduce Rampart, a system that protects the server end of web applications from CPU-exhaustion DoS attacks. Rampart is implemented as an extension to the PHP Zend engine, and thus can protect 83% of websites worldwide without requiring source code modification.

Bio

Wei Meng is an Assistant Professor in the Department of Computer Science and Engineering at the Chinese University of Hong Kong. He received his Ph.D. degree in Computer Science from the Georgia Institute of Technology in 2017 and his Bachelors degree in Computer Science from Tsinghua University in 2012. His research focuses on computer security and privacy. He is particularly interested in designing and building systems to protect end users and applications on the Internet. His research has been published at top

conferences such as USENIX Security, WWW, CCS, and NDSS. He currently leads the Computer Security Lab in the CSE department at CUHK.

Faculty Host: Sudarsun Kannan