**COLLOQUIUM**

Department of Computer Science and Engineering

University of South Carolina

**Instant and Bug-Free Patch Generation for Fixing Heap Vulnerabilities**

**Qiang Zeng**

Date: **November 29, 2017**

Time: **10:00-11:00am**

Place: **Storey Innovation Center, Room 2277**

# Abstract

Patching is one of the most important measures to continuously uphold security throughout the life of a software system. Patch generation and deployment are probably the most critical tasks in the process of patching. However, patch generation is typically a lengthy procedure (according to Symantec, it takes an average of 28 days to release a patch for fixing a critical security bug); and patch deployment risks system stability due to new bugs contained in patches. From the perspective of speeding up patch generation and avoiding bugs in patches, we examine the notorious heap vulnerabilities, including heap buffer overflows (such as Heartbleed), uninitialized-read, use-after-free, and double-free, and explore the following two important but less-investigated problems: (1) How fast can heap patches be generated? (2) How to ensure zero bugs in the generated patches? While quick patch generation and bug-free patches are two naturally desired goals, they contradict each other in practice. Rushed patch generation tends to introduce bugs, while creating a quality patch requires significant time for debugging, testing, and even system redesign. Thus, how to achieve the two inherently contradictory goals simultaneously has been challenging. Inspired by “targeted therapy”, a cancer treatment that precisely recognizes and kills cancer cells, we propose Targeted Heap Therapy to pinpoint and treat vulnerable buffers, which are buffers that can be exploited to launch attacks, with instantly generated bug-free patches. This talk will also present some of the important problems and future prospects on Internet of Things security as well as our ongoing work on these problems.

**Dr. Qiang Zeng** is a Tenure-Track Assistant Professor in the Department of Computer & Information Sciences at Temple University. He received his Ph.D. in Computer Science and Engineering from the Pennsylvania State University. He has rich industry experience and has worked in the IBM T.J. Watson Research Center, the NEC Lab America, Symantec and Yahoo. Dr. Zeng’s main research interest is Systems and Software Security. He currently works on Mobile Security, IoT Security, and deep learning for solving security problems. He has published papers in PLDI, NDSS, MobiSys, CGO, DSN and TKDE.