NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title:	**Shreds: Fine-grained Execution Units with Private Memory (paper published in IEEE S&P 2016)**

Speaker:	Assistant Professor Long Lu Department of Computer Science Stony Brook University, USA
Date/Time:	28 June 2016, Tuesday, 10:30 AM to 12:00 PM
Venue:	Executive Classroom, COM2-04-02
Chaired by:	Dr Saxena, Prateek, Dean's Chair Assistant Professor, School of Computing (prateeks@comp.nus.edu.sg)

Abstract:

Once attackers have injected code into a victim program's address space, or found a memory disclosure vulnerability, all sensitive data and code inside that address space are subject to thefts or manipulation. Unfortunately, this broad type of attack is hard to prevent, even if software developers wish to cooperate, mostly because the conventional memory protection only works at process level and previously proposed in-process memory isolation methods are not practical for wide adoption.

We propose shreds, a set of OS-backed programming primitives that addresses developers' currently unmet needs for fine- grained, convenient, and efficient protection of sensitive memory content against in-process adversaries. A shred can be viewed as a flexibly defined segment of a thread execution (hence the name). Each shred is associated with a protected memory pool, which is accessible only to code running in the shred. Unlike previous works, shreds offer in-process private memory without relying on separate page tables, nested paging, or even modified hardware. Plus, shreds provide the essential data flow and control flow guarantees for running sensitive code. We have built the compiler toolchain and the OS module that together enable shreds on Linux. We demonstrated the usage of shreds and evaluated their performance using 5 non-trivial open source software, including OpenSSH and Lighttpd. The results show that shreds are fairly easy to use and incur low runtime overhead (4.67%).

Biodata:

Long Lu is an assistant professor of computer science at Stony Brook University. His research interest lies in the intersection of security, operating systems, and program analysis.

His recent work is focused on mobile platform and app security. He joined Stony Brook after he had obtained his Ph.D. from Georgia Tech in 2013. (more about his work can be found at www.longlu.org)