Title: WarGames in Memory: Ending Control-Flow Hijack Attacks

Speaker: Assistant Professor Mathias Payer
Purdue University

Date/Time: 2 April 2014, Wednesday, 10:00 AM to 11:00 AM

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:

Memory corruption (e.g., buffer overflows, random writes, memory allocation bugs, or uncontrolled format strings) is one of the oldest and most exploited problems in computer science. These problems are here to stay as low-level languages like C or C++ continue to trade safety for potential performance. A small set of all proposed solutions (e.g., Address Space Layout Randomization, Data Execution Prevention, and stack canaries) is applied in practice but real exploits show that all currently deployed protections can be defeated.

The problems of current protection mechanisms call for novel approaches towards software protection that fulfill the following properties: low overhead for high security guarantees, no changes to the original source code, and compatibility to existing libraries and binaries (including a partial migration strategy).

We present a security policy that deterministically protects software against control-flow hijack attacks. Our mechanism uses both a user-space virtualization system (building on binary translation) to support legacy code and a compiler-based framework to enforce the integrity of all code pointers at runtime. Such a system controls the execution of all code in user-space, extracts information from all loaded components, and enforces a strong security policy for the executed software with low overhead. We show possible pitfalls and limitations and discuss future extensions and optimizations.

Biodata:

Mathias Payer will join as an Assistant Professor at Purdue University in summer '14 for system security. He is currently a post-doctoral researcher at UC Berkeley in Dawn Song's BitBlaze group. His research focus is in system security, runtime systems, user-space software-based fault isolation, binary translation/recompilation, and (application virtualization).
Mathias graduated from ETH with a Dr. sc. ETH in May 2012. The topic of his thesis focuses on the protection of binary-only code using binary translation and additional security guards. At UC Berkeley he continues this line of thought and broadens the evaluation of different security techniques and evaluates why individual solutions have failed where other, weaker solutions succeeded.