CS6101 - Software Security & Analysis
Syllabus

Welcome! This module introduces you to the field of software security and analysis. You have 2 options to successfully complete this module.
1. *Do a small project with one of the faculty members.* Discuss with the faculty individually if you are keen on this option.
2. *Write paper summaries for any 6 papers in 2 focus areas listed below*.

Project Option

The goal is to get hands-on experience on security and analysis projects, potentially leading to a paper publication. Typically, you will work on a new idea in a team of atmost 2 first-year PhDs under the guidance of one faculty member. Expected workload is about 9 hours/week per person for a period of 5-6 weeks. Please discuss with individual faculty advisors about available projects, or even better, propose your own.

Paper Summary Option

You can pick *any 2 focus areas* listed below for paper reading based on your interest. **You must read a minimum of 6 papers from these 2 focus areas** by the end of the first half of the course. The papers are chosen to give a broad overview of the security and software analysis field. Please feel free to pick your own pace in reading the papers.

For each paper you read, please write a paper summary and email it to prateeks@comp.nus.edu.sg. **The email subject should start with "[CS6106-Summary]".** It should be **no more than 2 pages in PDF format** [10 pt, double-column, ACM conference style]. It should be *precise and well-articulated* and should answer the following questions**:**

- What problem is the paper claiming to solve, and what it actually achieves a solution to?
- Is the problem new to that sub-field? Is the problem interesting to you?
- What are the assumptions of the problem/solution? What is the threat model that this mechanism is trying to prevent? How practical or sound are these assumptions -- have they been empirically or theoretically validated?
- What do you like about this approach? What would you have done differently or better? In what ways would your solution be better?
- Does the technique achieve its goal, in general? Where will this technique fail -- theoretically and in practice?
- If you were the author of this paper, suggest three novel ideas for future papers that you would undertake as follow-on work? Spend 10-20 mins on any one: Sketch how you would implement it, and, what would be the "evaluation" section of that paper look like?

Academic Honesty: You can discuss the papers with other students. However, you must write up your paper summary independently. Be sure to cite any references you utilize in your writeup to avoid plagiarism, as required by the NUS academic honesty policy.

Focus Areas & Paper List

Here are the focus areas and the associated papers in each of the areas.
If you are specifically interested in issues on cloud security, you can treat the papers marked with cloud () as a separate focus area.

Attack Research

- Lest We Remember: Cold Boot Attacks on Encryption Keys
- Remote timing attacks are practical.
- Timing Analysis of Keystrokes and SSH Timing Attacks
- Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds 
- How to Break Anonymity of the Netflix Prize Dataset.

Software Security

- Beyond stack smashing: recent advances in exploiting buffer overruns
- On the Effectiveness of Address-Space Randomization
- Taint-Enhanced Policy Enforcement: A Practical Approach to Defeat a Wide Range of Attacks
- Control Flow Integrity
- Preventing Privilege Escalation
- Extensible security architectures for Java
- Efficient Software-Based Fault Isolation
- Return-Oriented Programming: Systems, Languages, and Applications
- NOZZLE: A Defense Against Heap-spraying Code Injection Attacks
- http://static.usenix.org/events/sec09/tech/slides/sotirov.pdf

OS Security, Malware & Trusted Computing

- An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants
- Architectural Support for Copy and Tamper Resistant Software
- Backtracking Intrusions
- Improving Host Security with System Call Policies
- StriderMonkeys
- Permission Re-Delegation: Attacks and Defenses
- Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis
- Terra: A Virtual Machine for Trusted Computing 
- Pioneer: Verifying Code Integrity and Enforcing Untampered Code Execution on Legacy Systems
- Process Out-Grafting: An Efficient “Out-of-VM” Approach for Fine-Grained Process Execution Monitoring
- Private Editing Using Untrusted Cloud Services 

Network Security & Intrusion Detection

- Inferring Internet Denial of Service Activity

- Bro: A System for Detecting Network Intruders in Real-Time
- Firewall Gateways, Chapter 3
- SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks 
- Anomaly Detection of Web-based Attacks
- The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection
- Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Off-line Intrusion Detection System Evaluation as Performed by Lincoln Laboratory
- Outside the Closed World: On Using Machine Learning For Network Intrusion Detection

Applied Cryptography & Protocol Security

- CryptDB: A Practical Encrypted Relational DBMS
- Why Cryptosystems Fail
- Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems
- Prudent engineering practice for cryptographic protocols
- Practical Techniques for Searches on Encrypted Data 
- A Semantic Model for Authentication Protocols
- Faster Secure Two-Party Computation Using Garbled Circuits

Web Security

- The Essence of Command Injection Attacks in Web Applications
- Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense
- Robust Defenses for Cross-Site Request Forgery
- BlackHat USA 2011: SSL And The Future Of Authenticity - YouTube
- DNS Cache Poisoning
- Protecting Browsers from DNS Rebinding Attacks
- SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks

Privacy & Anonymity

- Privacy, economics, and price discrimination on the internet
- What is privacy worth?
- Detecting and Defending Against Third-Party Tracking on the Web
- Privacy-enhancing technologies for the Internet
- Tor: The Second-Generation Onion Router
- Differential Privacy
- Privacy Integrated Queries 
- Airavat: Security and Privacy for MapReduce 

Software Analysis

- CCured: Type-Safe Retrofitting of Legacy Code
- EXE: Automatically Generating Inputs of Death
- Measuring Channel Capacity to Distinguish Undue Influence
- Mining Specifications of Malicious Behavior
- Detection of recurring software vulnerabilities.

- Verifying Client-Side Input Validation Functions Using String Analysis
- Strict Control Dependence and Its Effect on Dynamic Information Flow Analyses
- DARWIN: An Approach for Debugging Evolving Programs
- A Symbolic Execution Framework for JavaScript
- Efficient Malware Detection using Model-Checking.