

CS4239 (2015/2016 Semester 1)




Week 1: 10 Aug 2015 - 14 Aug 2015

Introduction - what the module is about, discussing background for the module, specifically any systems background or mathematical background needed for the module. **Start** discussion on common software vulnerabilities

Lecture slides posted by Roland Yap.

Monday 10 August is a Public Holiday. The slides and video have been posted, and the students are encouraged to email lecturers to ask queries about the module if they want to decide whether to take the module or have other queries. Email of lecturers: ryap@comp.nus.edu.sg abhik@comp.nus.edu.sg

Learning Activities

1.1	 Files	prelim.pdf - Preliminaries
1.2	 Files	intro1.pdf - Introduction (part 1)
1.3	 Files	intro2.pdf - Introduction (part 2)
1.4	 Files	intro3.pdf - Introduction (Part 3)
1.5	 Multimedia	CS4239 Intro1
1.6	 Multimedia	CS4239 Intro2
1.7	 Multimedia	Intro3
1.8	 Multimedia	Intro3b

 Top

Week 2: 17 Aug 2015 - 21 Aug 2015

Lesson: Memory Errors - C & System Background

There will be an in-class quiz on C as well as the lecture

Lecturer: Roland Yap

Learning Activities

2.1	 Multimedia	CS4239 Week 2 Lecture
-----	--	-----------------------

 Top











Week 3: 24 Aug 2015 - 28 Aug 2015 : Memory Errors (continued)

Lesson: Spatial and Temporal Memory Errors

Lab: Buffer overflow examples and introduction to Black box fuzzing (Peach fuzzer) via detection of buffer overflows

Lecturer: Roland Yap






Learning Activities

3.1	 Multimedia	Week 2 Supplement
3.2	 Multimedia	Week 3 video - recorded during lecture
3.3	 Multimedia	Week 3 Remainder Lecture
3.4	 Weblink Victor van der Veen, Nitish dutt-Sharma, Lorenzo Cavallaro, Herbert Bos: Memory Errors: The Past, the Present, and the Future	
3.5	 Weblink	Úlfar Erlingsson, Yves Younan, Frank Piessens: Low-Level Software Security by Example
3.6	 Weblink	Laszlo Szekeres, Mathias Payer, Tao Wei, Dawn Song: SoK: Eternal War in Memory
3.7	 Weblink	SEI CERT C Coding Standard
3.8	 Weblink	Reference Book: Robert C. Seacord, Secure Coding in C and C++
3.9	 Files	CS4239Tutorial 1.pdf
3.10	 Files	CS4239_Software_Installation_Guide.pdf - CS4239_Software_Installation_Guide

[↑Top](#)**Week 4: 31 Aug 2015 - 04 Sep 2015 : Fuzzing Part 1****Lesson:** Fuzzing part I [mostly blackbox fuzzing plus measuring blackbox fuzzing]

READING: Fuzzing: the state of the art, technical report - provided in the following, see PDF file

*Lab: Black box fuzzing tool (Peachfuzzer)***Lecturer: Abhik Roychoudhury****Learning Activities**

4.1	 Files	Fuzzing_the_art_of_state.pdf
4.2	 Weblink	Optional reading - Sample of latest progress in fuzzing
4.3	 Files	6pp-BlackBoxFuzzing.pdf - Week 4 lecture
4.4	 Files	CS4239Tutorial 2.pdf - Tutorial 2 - Peach Fuzzer (continue)
4.5	 Multimedia	Black-box fuzzing

[↑Top](#)**Week 5: 07 Sep 2015 - 11 Sep 2015****Lesson:** Fuzzing part II (whitebox fuzzing)

READING: Directed Automated Random Testing paper, PLDI 2005

KLEE: Unassisted and Automatic Generation of High-Coverage Tests for Complex Systems Programs, OSDI 2008.

Taint based directed whitebox fuzzing, ICSE 2009

TaintScope: Checksum aware directed fuzzing, Oakland 2010.

Lab: Answer questions on black-box fuzzing, specifically related to the first assignment

Supplementary Lecture: Primer to C (this does cover parts of C relevant to common security problems/bugs)

Lecturer: Abhik Roychoudhury

(Roland Yap [weekend C lecture to help students with C background])

Learning Activities

5.1		Weblink	Directed Automated Random Testing, PLDI 2005
5.2		Weblink	https://www.doc.ic.ac.uk/~cristic/papers/klee-osdi-08.pdf
5.3		Weblink	Greybox fuzzing - BuzzFuzz
5.4		Files	WhiteBoxFuzz-6pp.pdf - Week 5 lecture
5.5		Weblink	Taintscope paper
5.6		Multimedia	Whitebox Fuzzing
5.7		Files	c-part1.pdf - C Primer (Part 1)
5.8		Files	c-part2.pdf - C Primer (Part 2)
5.9		Web Lecture	Makeup Lecture - C Primer

[↑Top](#)

Week 6: 14 Sep 2015 - 18 Sep 2015

Lesson: Taint Propagation and related issues

Static analysis - an introduction. Static dependency analysis.

Static analysis for detection of software vulnerabilities - Discussion of static and dynamic taint analysis.
(to recommend related papers - can read Dytan paper from ISSTA 2007, and the references within).

READING: All you Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask), Oakland 2010 [basic reading]

Three other weblinks appear below, along with this one.




Lab: (i) Finish discussions on fuzzing






[15 September: Assignment 1 is due for online submission, checked by Thuan Pham/Abhik Roychoudhury, see CS4239_Assignment_1.pdf]

(ii) Introduce Static analysis tool (Clang checker) to be used for second assignment

Lecturer: Abhik Roychoudhury

Learning Activities

6.1		Weblink	Application of taint analysis for device drivers - SOSP 2009 paper
6.2		Weblink	Dynamic taint analysis tool - ISSTA 2007 paper
6.3		Weblink	Oakland 10 survey paper on Taint analysis




6.4		Weblink	Taintscope paper
6.5		Files	Taint-6pp.pdf - Week 6 Lecture
6.6		Multimedia	Week 6 lecture - Taint propagation
6.7		Files	CS4239_Assignment_1.pdf
6.8		Files	CS4239Tutorial 3.pdf - Tutorial 3 - Introduction to Static Analysis

[↑Top](#)**Week 7: 28 Sep 2015 - 02 Oct 2015****Midterm Examination**

Lab: Details of Clang checker for second programming assignment; also discuss the second assignment itself.

Lecturer: Roland Yap

Learning Activities

7.1		Files	CS4239Tutorial 4.pdf - Tutorial 4 - Understanding taint analysis in Clang Analyzer and writing new Clang checker
7.2		Multimedia	Memory Error Defences
7.3		Files	memdef.pdf - Defences Against Memory Errors

[↑Top](#)**Week 8: 05 Oct 2015 - 09 Oct 2015**







Lesson: Error Localization and Patching of programs (Error localization was covered in this lecture)


Readings : see weblinks below - the readings for patching will be more relevant for week 10 since week 8 was used for error localization.

Lab: Answer questions on Clang checker

Lecturer: Abhik Roychoudhury

Learning Activities

8.1		Weblink	Cause Clue Clauses
8.2		Weblink	Debugging Linux Code
8.3		Weblink	Patching/repair - ICSE 2013 paper
8.4		Weblink	Regression Debugging - FSE09
8.5		Weblink	SOSP 2009 paper on patching
8.6		Weblink	Windows Error Reporting, SOSP 2009 paper

8.7  Files CS4239ErrorLocalize.pdf - Week 8 lecture

8.8  Multimedia Week 8 lecture

 Top

Week 9: 12 Oct 2015 - 16 Oct 2015

Lesson: Software model checking for vulnerability detection.

READING: "A Survey of Automated Techniques for Formal Software Verification" by Vijay D'Silva et. al in TCAD 2008

There's Plenty of Room at the Bottom: Analyzing and Verifying Machine Code, CAV 2010.

Plus some basic material on model checking to be posted.







Lab: (i) Final questions on second assignment

(due on 15 October, checked by Thuan Pham / Abhik Roychoudhury, see Assignment_2.pdf)

(ii) Basic introduction to LLVM

Lecturer: Guest Lecture by Cho Chia Yuan DSO (invited by Abhik Roychoudhury)

Learning Activities

- | | | | |
|-----|---|------------|---|
| 9.1 |  | Weblink | Binary code model checking - CAV 2010 |
| 9.2 |  | Weblink | A Survey of Automated Techniques for Formal Software Verification |
| 9.3 |  | Files | CS4239_Assignment_2.pdf - Description for the Lab assignment 2 |
| 9.4 |  | Files | LLVM_TUTORIAL.pdf - Week 9 tutorial on LLVM |
| 9.5 |  | Files | CS4239ModelChecking.pdf - Week 9 lecture |
| 9.6 |  | Multimedia | Model Check |

 Top

Week 10: 19 Oct 2015 - 23 Oct 2015

Part 1: Finish the discussions on software patching (from week 8)

Part 2: Lesson: Perspective on various testing and analysis methods for vulnerability detection

A perspective about various testing and analysis techniques for vulnerability detection

(a) static analysis and abstract interpretation

(b) symbolic execution and fuzzing

(c) software model checking










READING: Check the weblinks against this lecture.

Lab: (i) Discuss the third assignment

(ii) KLEE for whitebox fuzzing

Lecturer: Abhik Roychoudhury

Learning Activities

10.1		Weblink	Buffer over-run analysis, NDSS 2000 paper
10.2		Weblink	MOPS checker, CCS 2002 paper
10.3		Weblink	String vulnerabilities, USENIX 2001 (less major reading)
10.4		Files	CS4239Patch-6pp.pdf - week 10 lecture (part 1)
10.5		Files	CS4239Perspective-6pp.pdf - Week 10 lecture (part 2)
10.6		Weblink	Patching/repair - ICSE 2013 paper
10.7		Weblink	SOSP 2009 paper on patching
10.8		Multimedia	19Oct15
10.9		Files	KLEE_TUTORIAL.pdf - Week 10 tutorial on KLEE

[↑Top](#)




Week 11: 26 Oct 2015 - 30 Oct 2015

Lesson: Arithmetic Vulnerabilities (part 1)

Lab: Discuss third assignment in details

Lecturer: Roland Yap

Learning Activities

11.1		Files	arithmetic.pdf - Dealing with Arithmetic
11.2		Multimedia	Arithmetic (Part 1)
11.3		Files	KLEE_BUCKETING_TUTORIAL.pdf - Week 11 tutorial on tests bucketing techniques

[↑Top](#)









Week 12: 02 Nov 2015 - 06 Nov 2015

Lesson: Arithmetic (Part 2) Operating Systems








Lab: SMT Lib format, Answer questions on whitebox fuzzing

Lecturer: Roland Yap


Learning Activities

12.1	 Files	UNDERSTANDING_SMT_LIB_FORMULA.pdf - Week 12 tutorial on SMT-LIB formula
12.2	 Files	arithmetic.pdf - Dealing with Arithmetic
12.3	 Files	os.pdf - Operating Systems Issues
12.4	 Weblink	Exploiting unix file-system races via algorithmic complexity attacks
12.5	 Weblink	Secure Programming HOWTO
12.6	 Weblink	BlackHat 2015: Stagefright: Scary Code in the Heart of Android
12.7	 Weblink	Slides for the Blackhat 2015 Stagefright talk
12.8	 Multimedia	Arithmetic (Part 2) + OS (Part 1)

[↑Top](#)**Week 13: 09 Nov 2015 - 13 Nov 2015**Lesson: Privileges and Sandboxing, Cryptography Issues, Software Architecture and DesignLab: Survey taken by students (**attendance is compulsory**)**Lecturer:** Roland Yap**Learning Activities**

13.1	 Files	os.pdf - Operating Systems Issues
13.2	 Files	various.pdf - Various Final Topics
13.3	 Weblink	GNU LibC Setuid Program Example
13.4	 Weblink	How to write a setuid program, Matt Bishop
13.5	 Weblink	Privilege Separation
13.6	 Weblink	M.S. Dittmer and M.V. Tripunitara., The UNIX Process Identity Crisis: A Standards-Driven Approach to Setuid, CCS, 2014
13.7	 Multimedia	Last Lecture: OS, Privileges, etc.

[↑Top](#)**Reading Week: 14 Nov 2015 - 20 Nov 2015****Assignment 3 due on 15 Nov 2015, checked by Thuan Pham / Abhik Roychoudhury --- see Assignment_3.pdf****Learning Activities**

R.1	 Files	CS4239_Assignment_3.pdf - Description for 3rd lab assignment on white-box fuzzing
-----	---	---

[↑Top](#)

Examination Week: 21 Nov 2015 - 05 Dec 2015

FINAL EXAM

 [Top](#)