

2017Fall:Software Security

Lecture 1 : Introduction to the course

Bing Mao

maobing@nju.edu.cn

Department of Computer Science



Outline

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Course Overview

This course is to examine various software vulnerabilities, review the literature how this problem was addressed, and discuss practical techniques and tools in fighting these threats.



Software Security

3 **Course Overview**

Description

Goal

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

Dept. of Computer Science,
Nanjing University

Course Overview

Description

- ▶ Graduate and postgraduate level
- ▶ Research oriented(not hacking)
- ▶ Software security class

Software Security

4

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

Dept. of Computer Science,
Nanjing University

Course Overview

Goal

- ▶ Understand the low-level details of real software implementations
- ▶ Be familiar with state of the art software vulnerabilities
- ▶ Attacks and defense related to software security
- ▶ Automated program analysis for the reverse engineering of binary code

Software Security

Course Overview

Description

Goal

5

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security
Background
Root Cause of the Security
Problems
Vulnerability Exploits
Reference

Dept. of Computer Science,
Nanjing University

Text Books

There are three main parts of the text books:

1. Computer Systems: A Programmer's Perspective (CSAPP)



Software Security

Course Overview

Description

Goal

6

Text Books

Content

Prerequisites

Tentative Course
Project

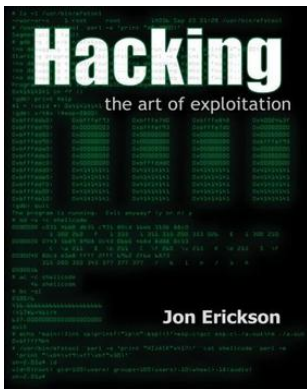
Teaching Assistant
Contact Information

Introduction to
Software Security
Background
Root Cause of the Security
Problems
Vulnerability Exploits
Reference

Dept. of Computer Science,
Nanjing University

Text Books

2. Hacking: The Art of Exploitation



Software Security

Course Overview

Description

Goal

7

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

Dept. of Computer Science,
Nanjing University

20

3. Related paper for after-class

- To be determined.

Software Security

Course Overview

Description

Goal

8

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

Content

- ▶ **Introduction**
- ▶ **Basic computer system knowledge**
- ▶ **Control Flow Hijacks**
 - ▶ Buffer Overflow
- ▶ **Practical Control Flow Defense**
- ▶ **Memory exploit**
 - ▶ ROP
- ▶ **Control Flow Integrity**
- ▶ **Program Analysis**
 - ▶ Program Representation
- ▶ **Dynamic Analysis**
 - ▶ Binary Instrumentation
- ▶ **Static Analysis**
 - ▶ LLVM(optional)
- ▶ **Symbolic Execution**
 - ▶ Vulnerability discovery
- ▶ **Summary**
 - ▶ Software security and program analysis

Software Security

Course Overview

Description

Goal

Text Books

9

Content

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security
Background
Root Cause of the Security
Problems
Vulnerability Exploits
Reference

Dept. of Computer Science,
Nanjing University

20

Prerequisites

- ▶ The basic knowledge of computer architecture
- ▶ ELF
- ▶ Stack Heap
- ▶ Assembly code(Intel x86)
- ▶ Computer Security basics
- ▶ C/C++ Programming in UNIX

Software Security

Course Overview

Description

Goal

Text Books

Content

10 Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

Dept. of Computer Science,
Nanjing University

Tentative Course Project

- ▶ StackOverflow Attack
- ▶ ROP Attack
- ▶ Taint

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

11

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Teaching Assistant

Contact Information

- ▶ Weiping Zhou
 - ▶ 1377203152@qq.com
- ▶ Zhilong Wang
 - ▶ 2395845334@qq.com

Course Group

- ▶ QQ group:641654480



Software Security2017

扫一扫二维码，加入该群。

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

12

Contact Information

Introduction to Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

20

Introduction to Software Security

Background

Computer security, also known as cybersecurity or IT security, is the “...protection of information systems from **theft** (secrecy/confidentiality) or **damage** (integrity) to the hardware, the software, and to the information on them, ...”—Gasser, Morrie (1988)



<http://www.securitygem.com/top-home-security-reviews/>

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

13

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Introduction to Software Security

Background

What's the Reality Today?

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

14

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

20

Introduction to Software Security

Background

What's the Reality Today?



Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

14

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

Introduction to Software Security

Background

What's the Reality Today?



震网 (Stuxnet) 病毒于2010年6月首次被检测出来, 是第一个专门定向攻击真实世界中基础 (能源) 设施的“蠕虫”病毒, 比如核电站, 水坝, 国家电网。互联网安全专家对此表示担心。

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

14

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Introduction to Software Security

Background

What's the Reality Today?



震网 (Stuxnet) 病毒于2010年6月首次被检测出来, 是第一个专门定向攻击真实世界中基础(能源)设施的“蠕虫”病毒, 比如核电站, 水坝, 国家电网。互联网安全专家对此表示担心。



被植入后门到Xshell版本中

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

14

20

Introduction to Software Security

Background

What's the Reality Today?



震网 (Stuxnet) 病毒于2010年6月首次被检测出来, 是第一个专门定向攻击真实世界中基础 (能源) 设施的“蠕虫”病毒, 比如核电站, 水坝, 国家电网。互联网安全专家对此表示担心。



被植入后门的Xshell版本

安全预警: Xshell 5官方版本被植入后门, 更新即中招 (国内已有用户受影响)

2017年8月14日发布

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

14

20

Introduction to Software Security

Background

Who are the Bad Guys?



Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

15

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Introduction to Software Security

Root Cause of the Security Problems

How Many Vulnerabilities?

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

16

Root Cause of the Security Problems

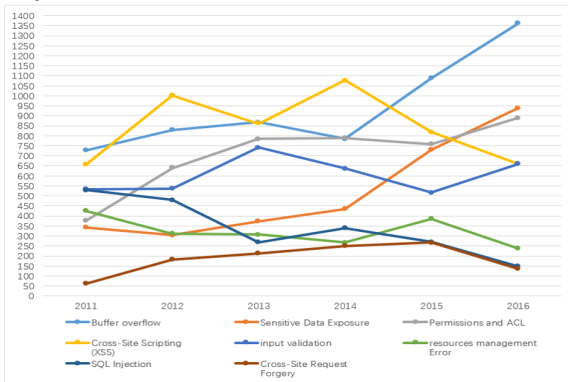
Vulnerability Exploits

Reference

Introduction to Software Security

Root Cause of the Security Problems

How Many Vulnerabilities?



Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

Reference

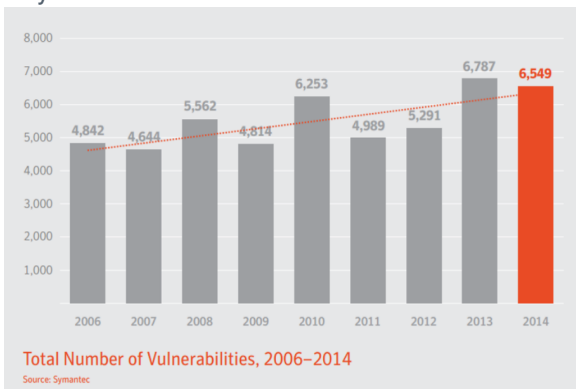
16

20

Introduction to Software Security

Root Cause of the Security Problems

How Many Vulnerabilities?



Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

17

Root Cause of the Security Problems

Vulnerability Exploits

Reference

Bugs, Vulnerabilities, and Exploits

- ▶ A bug is a place where real execution behavior may deviate from expected behavior
- ▶ A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (NIST's definition)
- ▶ An exploit is an input that gives an attacker an advantage

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

18

Vulnerability Exploits

Reference

Introduction to Software Security

Vulnerability Exploits

How Vulnerabilities are Exploited

Attack Method	Objective
Control flow hijacks	Gain control of the instruction pointer eip
Denial of service	Cause program to crash or stop servicing clients
Information Disclosure	Leak private information

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Reference

19

20

Introduction to Software Security

Reference

Reference

- ▶ gdb
- ▶ objdump
- ▶ IDA pro

Software Security

Course Overview

Description

Goal

Text Books

Content

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

20

Reference

20

Dept. of Computer Science,
Nanjing University