2017Fall:Software Security

Lecture 1 : Introduction to the course

Bing Mao

maobing@nju.edu.cn

Department of Computer Science

Outline

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.

Course Overview
Description

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

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

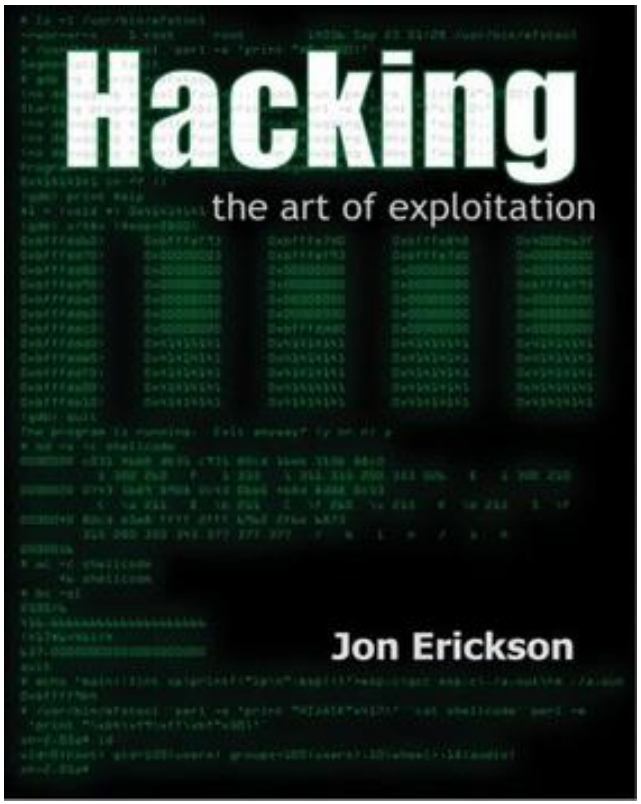
Text Books

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



Text Books

3. Related paper for after-class

- To be determined.

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**
  - Vulnerabilitiy discovery
- **Summary**
  - Software security and program analysis

Prerequisites

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

Tentative Course Project

- StackOverflow Attack
- ROP Attack
- Taint

Teaching Assistant
Contact Information

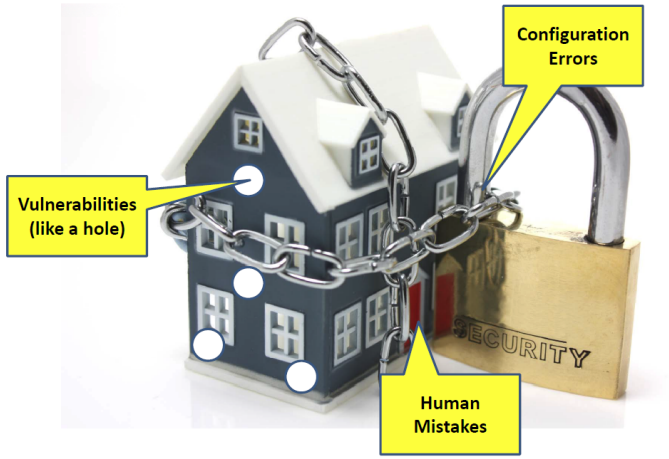
- Weiping Zhou
  - 1377203152@qq.com
- Zhilong Wang
  - 2395845334@qq.com

Course Group

- QQ group:641654480

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/

What's the Reality Today?

What's the Reality Today?

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。

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

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

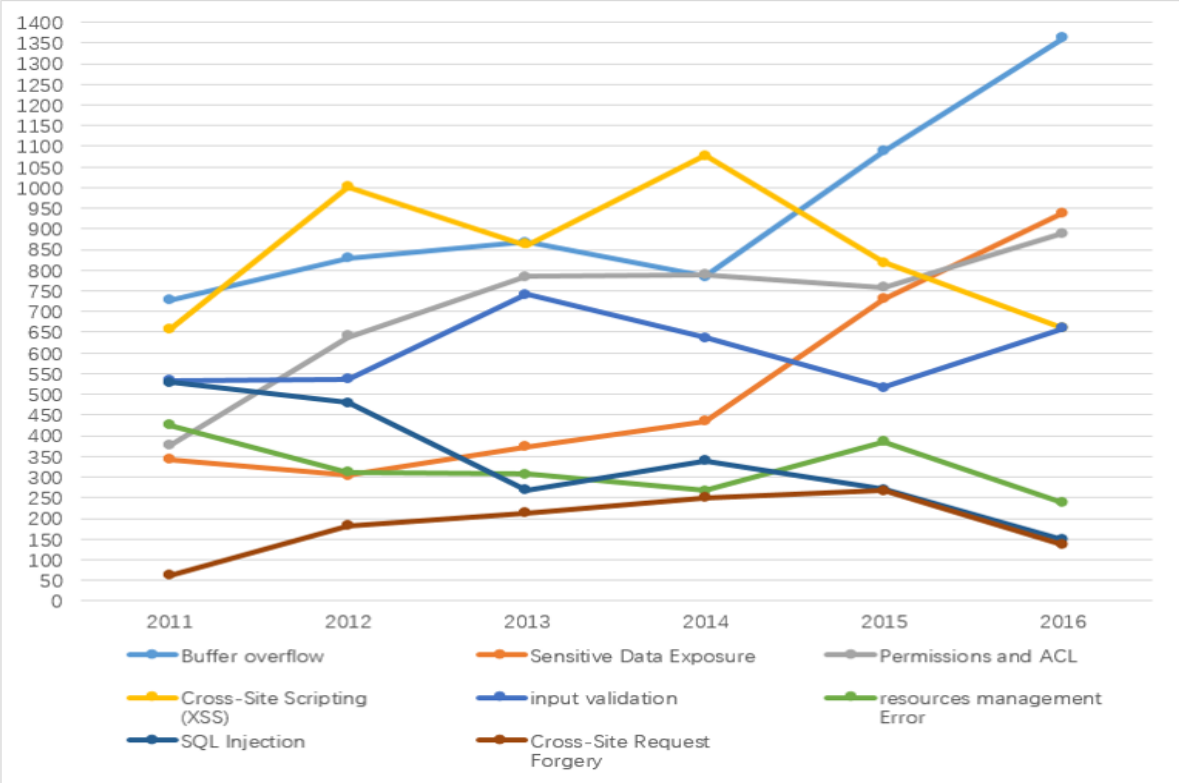
安全预警：Xshell 5官方版本被植入后门，更新即中招（国内已有用户受影响）

2017年8月14日发布

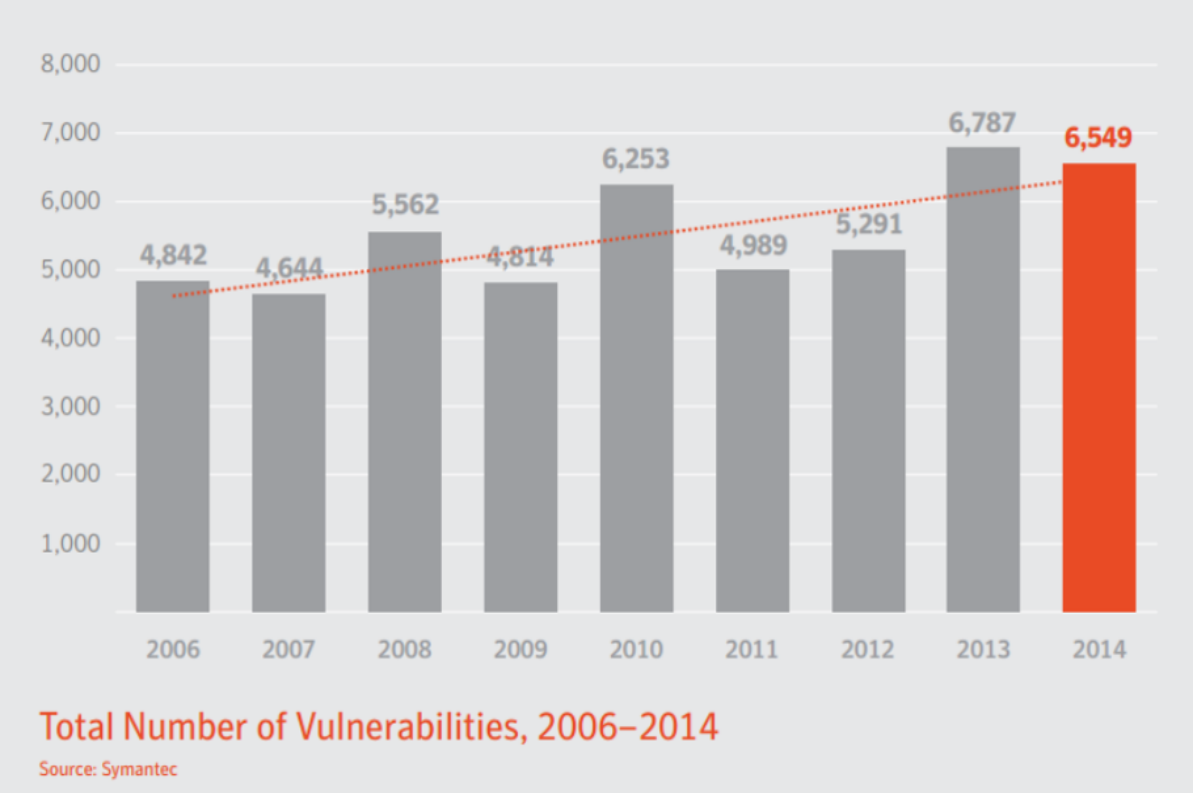
Who are the Bad Guys?

How Many Vulnerabilities?

How Many Vulnerabilities?



How Many Vulnerabilities?



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

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

Reference

- gdb
- objdump
- IDA pro