Lecture 1
Course Overview and Logistics

Zhiqiang Lin
Zhiqiang.lin@utdallas.edu
The University of Texas at Dallas

January 11th, 2016
Security
Security: The Goal

• [Informally] 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)

• This is **hard** because:
  – Computers can do a lot of damages super fast.
  – There are many places for things to go wrong.
  – Networks enable
    • Anonymous attacks from anywhere
    • Automated infection
    • Hostile code and hostile hosts
Basic Components (CIA) in Security

- **Confidentiality**
  - Keeping data and resources hidden
- **Integrity**
  - Data integrity (integrity)
  - Origin integrity (authentication)
- **Availability**
  - Enabling access to data and resources
Dangers

Damages of information
Disrupts of service
Theft of money
Theft of information
Loss of privacy

integrity
availability
secrecy/integrity
secrecy
secrecy
Vulnerabilities

• Bad (buggy or hostile) *programs*
• Bad (careless or hostile) *people* giving instructions to good programs
• Bad guy interfering with *communications*
Real-World Security

• It’s about value, locks, and punishment.
  – Locks good enough that bad guys don’t break in very often.
  – Police and courts good enough that bad guys that do break in get caught and punished often enough.

• Security is expensive—buy only what you need.
Why We Don’t Have “Real” Security

• A. People don’t buy it:
  – Danger is small, so it’s OK to buy features instead.
  – Security is expensive.
    • Configuring security is a lot of work.
    • Secure systems do less because they’re older.
  – Security is a pain.
    • It stops you from doing things.
    • Users have to authenticate themselves.

• B. Systems are complicated, so they have bugs.
Why Security Becomes Harder

- **Timesharing** brought the basic dilemma of security
- Each user wants a **private machine**, **isolated** from others, but users want to share **data, programs** and **resources**

1950 - 1964 (Multics) - 1982 (Internet) - 2016

- Security was by **physical isolation**
- You bring your data, control the machine, take everything away

- **The Internet**: Less isolation, more sharing
- More valuable stuff in the computers
What’s the State-of-the-Art

http://www.digitalattackmap.com/
Threats We Have Observed

- Virus/Malicious Software (1990s)
- Worms (2000s)
- Botnets (late 2000s)
- APTs, Insiders (2010s)
Who Are They?

- Cyber criminals
- State sponsored
- Attackers
- Insiders
- Script kiddies
- Hacktivists
The most powerful adversary

http://cyberwardesk.com/have-cyberattacks-become-nation-state-attacks/
Thai government websites hit by denial-of-service attack

BBC News - Oct 1, 2015
Several Thai government websites have been hit by a suspected distributed-denial-of-service (DDoS) attack, making them impossible

Nuclear power plants are at serious risk of cyber attacks

BT.com - Oct 6, 2015
Nuclear power plants across the world are not adequately prepared for the threat of “serious cyber attacks” from terrorist groups,

Canadian military seeks hackers to build exploits and defend...

International Business Times UK - Oct 7, 2015
"Cyberattacks on information technologies like personal computers... are usually result mostly in immaterial damages, like the loss,

3 nations tried cyberattacks on Hillary Clinton's private e.

CBS News - Oct 8, 2015
That means her server was possibly vulnerable to cyberattacks ... and the nature of the cyber intrusions

About 330,000 in state affected by cyberattack involving T

The Seattle Times - 22 hours ago
Nearly 330,000 Washington residents are among the 15 million people affected by the cyberattack on T-Mobile US data at credit-
services ...

Cyber attack puts T-Mobile customers at risk

The Turlock Journal - Oct 6, 2015
Defensive strategies

- Keep everybody out
  - Isolation

- Keep the bad guy out
  - Code signing, firewalls

- Let him in, but keep him from doing damage
  - Sandboxing, access control

- Catch him and prosecute him
  - Auditing, police
Elements of Security

Policy: *Specifying* security  
What is it supposed to do?

Mechanism: *Implementing* security  
How does it do it?

Assurance: *Correctness* of security  
Does it really work?
The Access Control Model

- Guards control access to valued resources.
Mechanisms—The Gold Standard

Authenticating principals
  – Mainly people, but also channels, servers, programs

Authorizing access.
  – Usually for groups of principals

Auditing

Assurance
  – Trusted computing base
# Computer and Network Security

<table>
<thead>
<tr>
<th>Software Security</th>
<th>Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Security</td>
<td>Cryptography</td>
</tr>
</tbody>
</table>
Agenda

• Course Introduction
• Course Topics
• Course Staff
• Course Mechanics
Course Topics

Computer and network security (CS4393)

- Software Security
  - Control Flow Hijack
  - Execution Safety
  - Information Flow
- Cryptography
  - Goals of Crypto
  - Stream Ciphers
  - Block Ciphers
  - Asymmetric Crypto
  - Authentication/Integrity
- OS Security
  - Common Defenses
  - Authorization
  - Security Architectures
- Network Security
  - Web Security
  - Denial of Service
  - Protocols
  - Intrusion Detection
Software Security
Control Flow Hijacks

Malicious Input

Buffer Overflow
Control Flow Hijacks

Shellcode (aka payload) + Padding &buf

Computation + Control

Allow attacker ability to run arbitrary code
- Install malware
- Steal secrets
- Send spam
Software Security

• Recognize and exploit vulnerabilities
  – Buffer overflow
  – Format string
  – Gist of other control flow hijacks, e.g., integer overflow, heap overflow

• Understand defenses in theory and practice
  – ASLR
  – DEP
  – Canaries
  – Know the limitations!
Cryptography
Everyday Cryptography

- ATM’s
- On-line banking
- SSH
- Kerberos
Adversary Eve: A very clever person
Cryptography’s Goals:
- Data Privacy (Confidentiality)
- Data Integrity
- Data Authenticity

Adversary Eve: A very clever person
Alice

Public Channel

Adversary Eve:
A very clever person

Bob
Adversary Eve: A very clever person

Attacker’s Goals:
- Privacy (Confidentiality)
- Integrity
- Authenticity
Goals

• Understand and believe you should never, ever invent your own crypto algorithm

• Basic construction

• Basic pitfalls

• How they are used in our daily life
OS Security
OS Goals

• Know Lampson’s “gold” standard
  – Authorization
  – Authentication
  – Audit

• Know currently used security architectures
Network Security
Networking Goals

• Understand the common attacks in networking, and the importance of IDS

• Be able to recognize and perform basic web attacks

• State what a DDoS is, and how CDN’s mitigate their effect
Agenda

• Course Introduction
• Course Topics
• Course Staff
• Course Mechanics
About the Instructor

• Ph.D., Purdue

• Assistant Professor, UT Dallas, Since August 2011

• **Systems** Security:
  – Virtual Machine Introspection
  – Cloud VM Management

• **Software** Security
  – Binary code analysis
  – Dynamic decompilation
  – Binary code reuse

• Mobile device security
  – App. Analysis
  – New Attacks
About the Teaching Assistant

- TBA
Agenda

• Course Introduction
• Course Topics
• Course Staff
• Course Mechanics
Basics

• Pre-req:
  – Basic UNIX development (gcc, gdb, etc.)
  – Operating Systems Concepts
  – Programming experience in C/C++ or JAVA is required
  – Knowledge in data communication and networking is required
  – The right motivations!

• Read papers or book chapters posted before each lecture
  – Read
  – Underline
  – Question
  – Review
Textbooks and Lecture Notes

• Required textbooks
    • *This book contains computer security theory & technologies and will be used for the first half of the course*
    • This book is very comprehensive in crypto. I will follow it as much as possible for the second half of the course
  – Accessible online through campus library links (choose SAFARI database)

• Lecture notes and additional materials
  – see elearning
Workload

• 6 project (homework) assignments
  – “if we adopt a picture that ignores practice, our field (computing) will end up like the failed ‘new math’ of the 1960s--all concepts, no practice, lifeless; dead” -- Peter Denning
  – Tentative

<table>
<thead>
<tr>
<th>Project</th>
<th>TOPICS</th>
<th>Starting Date</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project-1</td>
<td>Basic Software Security</td>
<td>01-19</td>
<td>02-01</td>
</tr>
<tr>
<td>Project-2</td>
<td>Advanced Software Security</td>
<td>02-02</td>
<td>02-15</td>
</tr>
<tr>
<td>Project-3</td>
<td>Secret Key Encryption</td>
<td>02-16</td>
<td>03-01</td>
</tr>
<tr>
<td>Project-4</td>
<td>One way hash function and MAC</td>
<td>03-02</td>
<td>03-15</td>
</tr>
<tr>
<td>Project-5</td>
<td>Public Key Cryptograph and Authentication</td>
<td>03-30</td>
<td>04-12</td>
</tr>
<tr>
<td>Project-6</td>
<td>Web Security</td>
<td>04-13</td>
<td>04-27</td>
</tr>
</tbody>
</table>
Grading

• Composition:
  – 55% Class Project and Homework (combined)
    • There might be bonus points
  – 15% Midterm
  – 25% Final
    • Comprehensive, with an emphasis on the second half of the semester
  – 5% Class Participation
    • Actively asking questions
    • (Nearly) no absence
      – Students can have at most 2 absences without reasons
Grading

A: [92-100]
A-: [90-92)
B+: [88-90)
B: [82-88)
B-: [80-82)
C+: [78-80)
C: [72-78)
C-: [70-72)
D+: [68-70)
D: [62-68)
D-: [60-62)
F: [0-60)
Other Policies

• **Late Policy**
  – All late submissions will automatically lose 10 points per delayed day.
  – *Suppose Project-A has 100 points, then you have 10 days to reach 0 points*

• **Collaboration Policy**
  – Students are encouraged to collaborate, particularly on the discussion on the course project.
  – *Project needs to be done independently.*

• **Cheating Policy**
  – Immediately reported
ETHICS!

• Obey the law
• Do not be a nuisance
• Don’t cheat, copy others work, let others copy, etc.
Survey

• Know you better
  – What's your career plan?
  – What you mostly want to learn from this class?
  – Programming languages you are familiar with
  – Your course prerequisites
  – Your brief introduction to the instructor

• This Survey will be available on elearning
  – due on January 15, 2016 11:59:00 PM CST
Questions