CSCE 465 Computer & Network Security

Instructor: Dr. Guofei Gu
Spring 2015
http://courses.cse.tamu.edu/guofei/csce465/

Course Logistics and Topics
What is Security?

- [Informally] Security is the *prevention* of certain types of *intentional* actions from occurring
  - These potential actions are *threats*
  - Threats that are carried out are *attacks*
  - Intentional attacks are carried out by an *attacker*
  - Objects of attacks are *assets*
Goals of Security

Prevention
– Prevent attackers from violating security policy

Detection
– Detect attackers’ violation of security policy

Recovery
– Stop attack, assess and repair damage

Survivability
– Continue to function correctly even if attack succeeds

Components of Security

Confidentiality
– Keeping data and resources hidden/confidential

Integrity
– Preventing unauthorized changes to data or resources
  • Data integrity (integrity)
  • Origin integrity (authentication)

Availability
– Enabling access to data and resources
Why This Course?

- Increased volume of security incidents
- Security threats
  - Malware: Virus, worm, spyware
  - Spam
  - Botnet
  - DDoS attacks
  - Phishing
  - ...

- Why do you take this class? Your understanding and expectation?...

More Examples: Botnet
Denial of Service

Estonia recovers from massive denial-of-service attack

By Jeremy Kirk , IDG News Service , 05/17/2007

A spree of denial-of-service (DOS) attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, CSO for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restore service.

"Yes, it's a serious problem, but we are up and running," Aarelaid said.

Aarelaid said analysts have found postings on Web sites indicating Russian hackers may be involved in the attacks. However, analysis of the malicious traffic shows that computers from the United States, Canada, Brazil, Vietnam and others have been used in the attacks, he said.

Malware

Spyware:
It's not what every well-dressed spy is wearing
More...

- “Attack of the tweets: Major Twitter Flaw Exposed” – UK researcher says vulnerability in Twitter API lets an attacker take over a victim’s account – with a tweet. Aug 27, 2009 [Darkreading]
- Conficker worm
- Stuxnet botnet...
Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in information security.
  - Security goals and threats to networking infrastructure and applications.
  - Network security
  - System security
  - Introduction to cryptography.
- Be able to determine appropriate mechanisms for protecting computer & network systems.

Course Styles

- Descriptive: what is out there.
- Critical: what is wrong with ...
- Skill oriented: homework/labs.
  - Explore!
- Interactive: discussion and questions encouraged and considered in grade
  - Students are encouraged to present their findings
- Information sharing: home page, piazza and email
Course Outline

• Background
  – Confidentiality, integrity, availability
  – Security policies, security mechanisms, assurance

• Network and system security
  – Fundamental security theories, Access control
  – Program/software security
  – Malware
  – Vulnerability analysis
  – Firewalls
  – Intrusion detection

Course Outline - Cont’d

• Cryptography
  – Secret key cryptography
  – Hashes and message digests
  – Public key cryptography

• More
  – Authentication and security handshakes pitfalls
  – IP security
  – Web security
Prerequisites

- CSCE 313
- Programming experience in C/C++ is required
- Knowledge in data communication and networking is required
- Other basic knowledge: operating systems, discrete mathematics...
- The right motivations!

Textbooks and References

- 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)
- Reference text(s) and class notes - see web site.
Course Resources

- WWW page: [http://courses.cse.tamu.edu/guofei/csce465/](http://courses.cse.tamu.edu/guofei/csce465/)
  - For course materials, e.g., lecture slides, related homework supplements, class notes, tools, etc.
  - Will be updated frequently. So check frequently.
- Piazza webpage (for discussion, Q&A)
  - [https://piazza.com/class#spring2015/csce465](https://piazza.com/class#spring2015/csce465)
- eCampus webpage (for submission, grade distribution)
  - [http://ecampus.tamu.edu/](http://ecampus.tamu.edu/)
- Office hour: 3-5pm Wednesday or by appointment

- TA: Lei Xu (csce465@gmail.com), Office hour 2-3pm Tuesday or by appointment

Grading

- Grading: Assignments 50%, Midterm Exam 20%, Final Exam 25%, Course participation 5%
  - There will be some bonus points in homework/labs
- Assignments: Five homework assignments, each including paper-and-pencil questions and/or programming/lab problems.
- Grade scale: 90-100 = A, 80-89 = B, 70-79 = C, 60-69 = D, Below 60 = F
- Late homework will be accepted with a 20% reduction in grade for each day late by
- After grades distributed/returned, 1 week for regrading.
Homework & Labs

- You need both theory and practice
- Labs included in homework: (Tentative list)
  - Packet sniffering and spoofing
  - Buffer overflow
  - TCP/UDP attacks
  - Secret-key cryptography
  - ...
- Mechanism
  - Virtual machine & network
- Many labs are difficult and time-consuming (but very rewarding)
- All the work is individual, NO teams
- You are expected to explore issues beyond what’s included in lectures by yourselves
- By taking this course, you agree you will not misuse tools obtained in the labs

Optional Honors Project

- You form a team (up to 3) and conduct a project, in which you design/implement/evaluate some useful and new attack/defense/system/tool/service. Talk to me for details if interested.
- If you take this option, you do not need to do the fifth homework and do not need to take the final exam!
- There are bonus points for excellent project!
- The deadline to let me if you want to take this option: Feb. 17 (you have one month to think and form a team)
Ethics & Academic Integrity

- We will study/discuss threats and attacks in the class/lab. You should be fully aware of ethics when studying these techniques. If in any context you are not sure about where to draw the line, come talk to me first.
- The university, college, and department policies against academic dishonesty will be strictly enforced.
- "An Aggie does not lie, cheat, or steal or tolerate those who do."