Internet Security [1]

VU 184.216

Engin Kirda	engin@infosys.tuwien.ac.at
Christopher Kruegel	chris@auto.tuwien.ac.at

Welcome to InetSec [1]

- For those who are lost: You currently in the brief introduction lecture to the *Internet Security* VU ☺
  - This is an introductory course that aims to make you “security-aware”.
  - So far, as a computer scientist, you have learned to write code and build applications… we show you how to break them ☺
  - Our aim is to help you learn typical and common security mistakes (i.e., vulnerabilities) by cracking applications.
  - Mind you, hacking is illegal and you are solely responsible for how you use what you learn.

OK, but why learn security?

- In computer science education, you learn to design and program code, but security education falls short.
  - Simple programming mistakes lead to serious security problems.
  - Today, failing to protect yourself and not being security-aware can be very costly.
  - Number of security-related incidents on the Internet increasing fast (e.g., look at recent worms on MS systems).
  - Recently, a person in Sweden got falsely accused of doing illegal things because his computer was hacked.
  - Do you want people to hurt your privacy by looking at your documents and e-mails and have “fun“?

Number of Reported Incidents

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

www.cert.org

What we expect from you

- Technical interest for security issues
  - (There are other courses you can do at the TU so you don't have to do this one ;-))
- Programming knowledge and experience (HTML, simple Javascript, SQL, Java, C…)
- Patience (security exercises aren't like Hollywood scenes ☺)
- Copying code and solutions, or hacking the lab system is **not** allowed.

Administrative Issues

- Mode
  - Lectures (in English) until June
  - regular security challenges (e.g., cracking web applications, phishing, code cracking, security tools, stack-based buffer overflows)
  - written final exam (end of June – tentative date)
- When and Where
  - Tuesdays 2pm. - 3pm
  - Freihaus Hörsaal 6
- Slides and News (please visit regularly!)
  - http://www.infosys.tuwien.ac.at/Teaching/Courses/InetSec/

Lecture - InetSec 1

Topics we will discuss

1. TCP/IP Security (e.g., ARP spoofing, seq. number guessing)
2. Web security and vulnerabilities (e.g., SQL injections, XSS)
3. Internet Application security (e.g., FTP bounce attack)
4. Simple cryptography (e.g., RSA)
5. Architectural principles
6. Stack-based buffer overflows
7. Software testing (i.e., finding vulnerabilities)
8. Operational practices
9. Miscellaneous topics of choice (e.g., firewalls, honeypots)

InetSec Lab

- Assignments
  - Lab starts after the Easter holidays
  - 6 challenges
  - no immediate credit assigned but… (explained in the next slide)
- Environment
  - assignments should be mostly solved at home / any computer with Internet connection
  - small “hacking” network, which is remotely accessible via ssh (Linux)
  - accounts can be obtained over the web (details will be announced in the coming weeks)
  - check home page for details
- Submission
  - hard deadlines (with sufficient time)
  - automatic checking with immediate feedback is planned

Grading for the lab

- You start with **-25** points, each challenge (assignment) brings you **5** points
- The written exam has **100** possible points
- You need to have **50** points to pass the course
- Example: John Hacker solves 3 challenges, and gets 70 points in the written exam. John has
  - ***-25+3*5+70=60*** points
- Hence, if you solve 5 challenges, you will get the maximum amount of points for the lab part of the course… 6 challenges gives you a +5 bonus
  - The less you solve, the more you loose

InetSec Lab

Challenges (tentative)

1. Security tools (e.g., nmap, tcpdump)
2. Cross Site Scripting
3. SQL Injections
4. Phishing
5. Code cracking (cryptography)
6. Stack-based buffer overflow (advanced in comparison to other challenges)

InetSec 1 and InetSec 2

	InetSec 1	InetSec 2
Unix Security	✗	✓
Windows Security	✗	✓
Buffer Overflows	✓	✓
Internet Application Security	✓	✗
Cryptography	✓	✗
Race Conditions	✗	✓
Reverse Engineering	✗	✓
Viruses and Worms	✗	✓
Wireless Security	✓	✗
Firewall and Intrusion Detection	✓	✗

Who should do InetSec 2

- People who would like become “security gurus”.
  - We take part in a Capture the Flag hacking contest against other universities – lots of fun. (3rd place last semester)
- People who are hard-core technical (i.e., C and Linux should not be a problem for you)
- You should be interested in solving technical problems
- People who have time
  - You get the chance to solve security challenges such as writing a virus, spoofing UDP packets, reverse engineering applications

Your Roadmap to Enlightenment

Requirement	**Rating**
InetSec 1, candidate	*Nobody*
InetSec 1, pass	*Apprentice*
InetSec 2, 6 solved challenges	*Generalist*
InetSec 2, 7 solved challenges	*Expert*
InetSec 2, 8 solved challenges	*Guru*
InetSec 2, 8 solved challenges, CTF	*Master Guru*

Goodbye

That‘s it… see you next week!