

# Internet Security [1]

## VU 184.216

### Introduction

Paolo Milani Comparetti

[pmilani@seclab.tuwien.ac.at](mailto:pmilani@seclab.tuwien.ac.at)

Clemens Kolbitsch

[ck@seclab.tuwien.ac.at](mailto:ck@seclab.tuwien.ac.at)

# Welcome to InetSec [1]

*Int. Secure Systems Lab  
Technical University Vienna*

- For those who are lost: You currently in the preparation 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.
  - Remember that breaking into other people's computer systems is illegal

# OK, but why learn security?

*Int. Secure Systems Lab  
Technical University Vienna*

- In computer science education, you learn to design and program code, but security education falls short.
  - Today, failing to protect yourself and not being security-aware can be very costly
- All programmers need to be aware of security
  - Simple programming mistakes lead to serious security problems
  - Number of security-related incidents on the Internet increasing fast
    - identity theft
    - "Aurora" attacks on google and 100s of other companies originating from china
- Even as an end-user, understanding security and privacy issues is increasingly useful

# Number of Reported Incidents

*Int. Secure Systems Lab  
Technical University Vienna*

<b>Year</b>	1988	1989
<b>Incidents</b>	6	132

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

<b>Year</b>	2000	2001	2002	2003
<b>Incidents</b>	21,756	52,658	82,094	137,529

- Statistics from [www.cert.org](http://www.cert.org)
  - Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, we stopped providing this statistic at the end of 2003.

# Some Interesting Numbers

*Int. Secure Systems Lab  
Technical University Vienna*

- Malware industry is worth 100 billion dollars per year
- 80-90% of the e-mail traffic out there is spam
- 50%-80% of computers connected to Internet infected with spyware
- A 26 year-old made 20 million dollars with spam before being caught
- phishing sites hosted by the RBN (Russian business network) made an estimated 150 million dollars with stolen bank credentials in 2006
  - source: Symantec Report on the Underground Economy (2008)
- Top rogue AV "affiliates" made over 300000\$ a month
  - source: Symantec Report on Rogue Security Software (2009)

# What we expect from you

*Int. Secure Systems Lab  
Technical University Vienna*

- 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
  - do not "help" your colleagues by giving them your solution (or posting your solution online!)

# Administrative Issues

*Int. Secure Systems Lab*  
*Technical University Vienna*

- Mode
  - Lectures (in English) until beginning of June
- regular security challenges (e.g., cracking web applications, security tools, stack-based buffer overflows)
  - each challenge is open for 1 or 2 weeks
  - **no deadline extensions**
- written final exam (late June)
- When and Where:
  - Wednesdays 12:00 (c.t.). Lecture lasts 1h 30.
  - EI 10
- Slides and News (please visit regularly!)
  - <http://www.seclab.tuwien.ac.at/inetsec/>

# Topics

*Int. Secure Systems Lab  
Technical University Vienna*

- Networking Basics
- TCP/IP Security (e.g., ARP spoofing, seq. number guessing,...)
- Web security and vulnerabilities (e.g., SQL injections, XSS,...)
- Internet Application security (e.g., DNS cache poisoning,...)
- Software testing (i.e., finding vulnerabilities)
- **Basic** cryptography
- Stack-based buffer overflows
- Language security (e.g: Java security)

# InetSec Lab

*Int. Secure Systems Lab  
Technical University Vienna*

- Assignments
  - Lab starts on 24.03.2010
  - 6 challenges
  - 5 points per challenge solved
  - **no points** for "partially solved" challenges
- 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 (registration starts on 04.03.2010 and continues until 31.03.2010)
  - check home page for details
- Submission
  - hard deadlines (with sufficient time)
  - automatic checking with immediate feedback

# Grading

- Each challenge (assignment) brings you 5 points
- The written exam has 50 possible points, total of 75 points for the course
- You need to have a total of **38** points to pass the course
  - Example: John Hacker solves 3 challenges, and gets 35 points in the written exam. John has  
 $3*5+35=50$  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 lose

# Challenges (tentative list)

*Int. Secure Systems Lab  
Technical University Vienna*

- Network security tools (e.g., nmap, tcpdump)
- Web security (2 challenges)
- Security-related programming assignment
- Cryptography
- 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	✗	✓
• Web security	✓	✓

# Who should do InetSec 2

*Int. Secure Systems Lab  
Technical University Vienna*

- People who would like to become “security gurus”.
  - We take part in a Capture the Flag hacking contest against other universities – lots of fun. (1st place in 2007, 2nd place in 2005 and 2009)
- 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, reverse engineering applications

# Your Roadmap to Enlightenment

---

<b>Requirement</b>	<b>Rating</b>
• InetSec 1, candidate	<i>Nobody</i>
• InetSec 1, pass	<i>Apprentice</i>
• InetSec 2, 6 solved challenges	<i>Stackmaster</i>
• InetSec 2, 7 solved challenges	<i>exploit Warlock</i>
• InetSec 2, 8 solved challenges	<i>Guru</i>
• InetSec 2, 8 solved challenges, CTF	<i>Master Guru</i>

# Inetsec Team

---

- Lecturers:
    - Paolo Milani Comparetti
    - Clemens Kolbitsch
  
  - Tutors:
    - Will be handling issues with the lab environment and challenges and answering questions in the TUWIS forum
    - Bernhard Miller (new tutor)
    - Markus Kammerstetter (former tutor, now advising)
-

---

Any Questions?

---

See you next week...

---

Now let's see what "real" hackers do...

---