Intrusion Detection and Malware Analysis
Course Introduction / Overview of Security Threats

Pavel Laskov
Wilhelm Schickard Institute for Computer Science
IT in a modern society

- Major growth factor
- Social phenomenon
- Critical infrastructure
Morris worm (1988)

- Written by a Cornell graduate student Robert Morris Jr, (now associate professor at MIT).
- Exploited multiple vulnerabilities in UNIX (sendmail, finger, rsh).
- Multiple infection resulted in severe denial of service.
- Infected 6,000 computers (from 60,000 then connected to Internet).
- Estimated damage: $10-100M.
ILOVEYOU worm (2000)

- First mass-mailer worm
- Used social engineering to activate a VBS script.
- Infected about 50M computers.
- Caused shutdown of email at Pentagon, CIA and British Parliament for cleanup.
- Estimated damage: $5.5B.
What can go wrong?

SQL Slammer worm (2003)

- “Flash” worm: infected most of the vulnerable systems within 10 minutes.
- Used a buffer overflow in a MS SQL server patched 6 months (!) earlier.
- Caused a major disruption of Internet traffic due to routing problems.
Samy worm (2007)

- Infected more than 1M users in MySpace within 20 hours.
- Used sophisticated cross-site-scripting for propagation.
- Forced MySpace to close the site for cleanup.
What can go terribly wrong?
Stuxnet: a new era in malware history

The real-world implications of Stuxnet are beyond any threat we have seen in the past. Despite the exciting challenge in reverse engineering Stuxnet and understanding its purpose, Stuxnet is the type of threat we hope to never see again.

W32.Stuxnet Dossier, Symantec
Key features of Stuxnet

- A first virus/worm to target industrial control systems
- Highly versatile propagation mechanisms:
  - USB drives
  - LAN
  - Exploitation of WinCC database server
  - Infection of PCS7 project files
  - Peer-to-peer update mechanisms
- Use of 4 previously unknown vulnerabilities
- Highly professional code, extensive hiding mechanisms
- Command-and-Control functionality
Architecture of SCADA systems
Some tricks from Stuxnet’s repertoire

Removable disk infection

- **Win2k, XP:** Autorun.inf

- **Vista, Windows 7:** specially crafted .lnk files start an exploit stored on a removable drive when its content is viewed
Infection of PCS7 project files

- PCS7 project files have extension .s7p and store management information about the system configuration.
- A specially crafted .s7p file will cause a Simatic manager to search for and load a certain DLL library (name not disclosed).
- A malicious variant of this DLL is placed by Stuxnet in a special directory where it will be loaded from unless found in 4 other system-default locations.
What can go wrong: lessons learned

- The key source of security problems is unpatched vulnerabilities.
- Current detection tools are useless unless regularly updated.
- Human error can lead to serious security breeches; further exploited by social engineering.
Key IT security mechanisms

Prevention
Detection
Reaction
Technical challenges

- Prevention mechanisms are sufficient only if they are correctly implemented.
- Detection mechanisms have to deal with huge variability of attacks and potentially unknown ones.
- Detection mechanisms must be able to withstand evasion and denial-of-service attacks.
- Reaction mechanisms must be timely and accurate and cause no disruption of normal functionality.
Non-technical challenges

- Organized crime: hacking previously done for fun is now done for profit.
- Incompetence and naivity of end users: what do they want to steal from *me*?
- Costs: investment in security is always lost money.
- Slow incident response: no matter what happened to my business it’s none of the business for my competitor.
Top security threats

- Remote exploits
- Web application attacks: SQL injection, cross-site scripting
- Spyware / Keyloggers
- Botnets
- Customized attacks / social engineering
Earning money with security violations

Study by T. Holz, M. Engelberth and F. Freiling at the University of Mannheim in April – October 2008.

Methodology: recovery of stolen credentials from dropzones.

Malware:
- Limbo/Nethell: keylogger, infection via drive-by-download
- ZeuS/Zbot: keylogger, infection via spam attachments
Study by T. Holz, M. Engelberth and F. Freiling at the University of Mannheim in April - October 2008.

Methodology: recovery of stolen credentials from dropzones.

Malware:
- Limbo/Nethell: keylogger, infection via drive-by-download
- ZeuS/Zbot: keylogger, infection via spam attachments
Impersonation attacks using keyloggers

- A keylogger is installed on a user machine by some attack vector.
- Keylogger downloads configuration data from a dropzone.
- Keylogger monitors keystrokes during access to specific websites and uploads them to a dropzone.
- Attacker retrieves credentials from a dropzone and sells it.
Analysis methodology

- Collect malware samples from honeypots and spam-traps.
- Execute malware samples in a specially instrumented sandbox, record and analyze outgoing communication.
- Contact a dropzone and download log files.
- Assess market value of stolen credentials using well-known estimates.
<table>
<thead>
<tr>
<th>Credentials</th>
<th>Amount</th>
<th>Price range</th>
<th>Average value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank accounts</td>
<td>10,775</td>
<td>$10 - 1000</td>
<td>$5,387,500</td>
</tr>
<tr>
<td>Credit cards</td>
<td>5,682</td>
<td>$0.40 - 20</td>
<td>$56,820</td>
</tr>
<tr>
<td>Social network IDs</td>
<td>78,359</td>
<td>$1 - 15</td>
<td>$587,162</td>
</tr>
<tr>
<td>Auction accounts</td>
<td>7,105</td>
<td>$1-8</td>
<td>$28,420</td>
</tr>
<tr>
<td>Email passwords</td>
<td>149,458</td>
<td>$4-30</td>
<td>$2,540,786</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>224,485</strong></td>
<td></td>
<td><strong>$8,600,688</strong></td>
</tr>
</tbody>
</table>
What will you learn?

- Main attack mechanisms
  - network, host and web application attacks
- Detection of malicious network traffic
  - network audit tools
  - feature extraction algorithms
  - detection algorithms
  - some response mechanisms
- Detection and analysis of malicious software
  - Malware types and their functionality
  - Malware collection, monitoring and analysis
Course administration

- **Lectures:**
  - Fri, 10:00–12:00 (ct), F122

- **Formalities:**
  - Credit hours (diploma): 2 SWS (lectures) + 1 SWS (exercises)
  - Credit points (master): 4 LP (lectures + exercises)

- **Exams and grading:**
  - diploma: oral exam by appointment, separate Übungsschein for exercises (with a grade)
  - master: written exam at the end of semester (70%), exercise grades (30%)

- **Course web page:**
  http://www.ra.cs.uni-tuebingen.de/lehre/ws10/intrusion_det.html
Homework assignments and exercises

Meetings:
- Mon, 14:00 (ct) – 16:00, A301
- First meeting: 25.10

2 individual homework assignments
3 assignments as a mini-project (in groups of 3-4 students)
Final assignment: live IDS competition

Evaluation and grades:
- all assignments are equally weighted
- the competition winner receives 20% bonus.
Edward Amoroso. 
*Intrusion Detection.*

John Aycock. 
*Computer Viruses and Malware.*
Springer Verlag, 2006.

Carl Endorf, Eugene Schultz, and Jim Mellander. 
*Intrusion Detection & Prevention.*

Stephen Northcutt and Judy Novak. 
*Network Intrusion Detection.*

Peter Szor. 
*The Art of Computer Virus Research and Defense.*
First and foremost: hunting hackers is fun!
It’s a major challenge: hackers are quite savvy!
It may get quite practical: modern IT-security needs intrusion detection!