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
What can go wrong?

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 wrong?

Integral Energy virus outbreak (2009)

- 1000 desktop computers in the Australian electricity supplier Integral Energy were infected by a Virut virus.
- Allegedly, operator consoles were also infected and quickly switched to Linux (?!).
- Power distribution network controlled by Solaris machines was not affected.
What can go wrong: personal experience
What can go wrong: personal experience
Hallo Pavel Laskov,

um 99downloads.de jetzt zu nutzen, müssen Sie nur noch Ihre Anmeldung aktivieren. Bitte rufen Sie dazu folgenden Link auf:

Jetzt hier klicken: http://www.99downloads.de/login.html?login=28785855949c355e8d0de7

(Sollte die Adresse nicht als Link dargestellt werden, kopieren Sie sie bitte vollständig in die Adresszeile Ihres Browsers.)

-----------------------------

Ihre Zugangsdaten für weitere Zugriffe:

Link: http://www.99downloads.de/login.html
Username: BEL103342
Passwort: Anb26PVI

-----------------------------

Ihr 99downloads.de-Team

kellers Premium Media Limited,
Nutzerservice
What can go wrong: personal experience

Sehr geehrter Pavel Laskov,


Da Sie nicht von Ihrem Widerrufsrecht Gebrauch gemacht haben, erlauben wir uns die Rechnungsstellung für die bereit gestellte und erbrachte Dienstleistung für die vereinbarte Vertragslaufzeit von 12 Monaten.

Teilnahme bei www.99downloads.de für 12 Monate - 60,00 Euro

Bitte geben Sie bei der Zahlung folgende Informationen an:

Ihre Kundenummer: BEL103342
Ihre Rechnungsnummer: 990103342

Bitte überweisen Sie den Rechnungsbetrag von 60,00 Euro bis zum 29.03.2009 auf unsere nachstehend angegebene Bankverbindung.

Kontoinhaber: Belleros Premium Media Limited
Kontonummer: 32 25 612 00
Bankleitzahl: 200 400 00
Bankinstitut: Commerzbank AG

Bei EU-Überweisungen:
Iban: DE89200400000322561200
Swift/Bic: COBADEHHCCX

Verwendungsbezeichnung: Rechnung, BEL103342, Kunde BEL103342
What can go wrong: personal experience

Zahlungserinnerung Kunde BEL103342 - 99downloads.de

From: Belleros Premium Media Limited <Mahnabteilung@99downloads.de>
To: pavel.laskov@first.fraunhofer.de
Date: 2009-03-28 10:36
Attachments: Zahlungserinnerung.pdf

Sehr geehrte/r Pavel Laskov,


Mit Zugang dieser Mahnung befinden Sie sich gem. § 286ff. BGB im Verzug. Uns steht damit die sofortige Erhebung einer Leistungsklage oder alternativ die Beantragung eines Mahnbescheides und die damit einhergehende Eröffnung eines Mahnverfahrens durch unsere Rechtsanwälte zu.

Teilnahme bei www.99downloads.de für 12 Monate - 60,00 Euro

Bitte geben Sie bei Zahlung folgende Informationen an:

Ihre Kundennummer: BEL103342
Ihre Rechnungsnummer: 990103342

Bitte überweisen Sie den Rechnungsbetrag von 60,00 Euro bis zum 05.04.2009 auf unsere nachstehend angegebene Bankverbindung:

Kontoinhaber: Belleros Premium Media Limited
Kontonummer: 12 25 612 00
Banklautzahl: 700 400 00
What can go wrong: personal experience

Dringende Nachricht - Letzte Mahnung Kunde BEL103342 - 99download.de

From: Belleros Premium Media Limited <Mahnabteilung@99download.de>
To: pavel.laskov@first.fraunhofer.de
Date: Sunday 12:01:15
Attachments: Letzte_Mahnung.pdf

Letzte Mahnung wegen Forderung aus Dienstleistungsvertrag

Sehr geehrte/r Pavel Laskov,

sie haben sich nachweislich am 20.03.2009 unter Angabe Ihrer IP-Adresse 134.2.172.155
und folgender persönlicher Daten bei unserem Projekt www.99downloads.de angemeldet:

Name, Vorname: Laskov Pavel
Strasse, Hausnummer: Kapellenweg 11
PLz, Stadt: 72070 Tuebingen
Email-Adresse: pavel.laskov@first.fraunhofer.de
Geburtsdatum: 24.05.1976


Wir empfehlen Ihnen daher, den Mahnbetrag umgehend auszugleichen, um weitere Kosten zu vermeiden. Die entstehenden Mehrkosten hätten Sie zusätzlich zu tragen.

Teilnahme bei www.99downloads.de für 12 Monate
---------------------------------------------
Teilnahmegebühr: 60,00 Euro
Verzugsprämie/Mahnkosten: 3,00 Euro
Gesamtbetrag: 63,00 Euro
Sehr geehrte[r] Pavel Laskov,


Wir haben unserer Mandantin nunmehr empfohlen, das gerichtliche Verfahren zur Titulierung der Forderung unter Aktenzeichen 1136812 einzuleiten.

Unsere Prozessabteilung wird im Falle der erfolgreichen Titulierung der Forderung die Pfändung von Bankkonten sowie die Pfändung von Lohn und Gehalt bei Ihrem Arbeitgeber erwerben.

Letztlich außergerichtlich weisen wir darauf hin, das unsere Mandatschaft nicht auf die Ihnen bekannte Forderung verzichtet und sich vorbehalten, alle rechtlichen Möglichkeiten der Beilegung dieser Forderung in Anspruch zu nehmen.

Um diese für beide Seiten unangenehme und insbesondere für Ihre Seite mit Kosten verbundene weitere Bearbeitung der Forderungssache zu vermeiden, geben wir Ihnen letztmals die Möglichkeit, die Forderung in Höhe von 110,29 Euro, bis spätestens 05.08.2009 auf unser Konto

Kontoverbindung: Postbank AG
Konto Nr.: 93 12 09
BLZ: 20010020

Bei EU-Überweisungen: IBAN: DE17200100200000931209 - BIC: PBNKDEFF
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
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
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.
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/ws09/intrusion_det.html](http://www.ra.cs.uni-tuebingen.de/lehre/ws09/intrusion_det.html)
Homework assignments and exercises

- Meetings:
  - Mon, 16:00 (ct) –18:00, A301
  - First meeting: 02.11

- 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.


Take-home message

- 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!