“Learning from Rootkits”
- Safe Place to stand for a Runtime Monitoring/Attestation System -

*SPRING 5: SIDAR Graduierten-Workshop über Reaktive Sicherheit*

Patrick Stewin, 7. July 2010, Bonn, Germany
patrickx@sec.t-labs.tu-berlin.de
Agenda

- Introduction
- Motivation
- Challenges
- Analysis x86 Platform
- Challenges for Attackers/Rootkits
- Important Related Work
- Conclusion and Further Research
Introduction

- **Rootkit evaluation:**
  - Originally placed in user space with root privileges to hide it
  - Rootkits moved from user space to kernel space and beyond!
  - Goal: somehow isolate rootkit from host platform using platform's stealth capabilities

- **Stealth – Isolation**

- Can we use stealth/isolation capabilities of x86 platforms to improve security properties?
Motivation

- Why to improve computer platform security properties?
- Example: Time-Of-Check-Time-Of-Use (TOCTOU) problem
  - Cf. Trusted Computing Group (TCG) attestation model
    - Chain of Trust starting at Root of Trust for Measurement (RTM)
      - Derives and stores fingerprint of software before software gets execution control
      - TOC: once, just before execution
      - No statement about runtime behavior (cf., e.g., buffer overflow attacks)

---

Patrick Stewin - SPRING 5: “Learning from Rootkits”
Goals

- Understand isolated execution environments to:
  
  i. Develop countermeasures against powerful and stealthy rootkits

  ii. Use them to enhance platform's security properties
Challenges

- Research mainly done on rootkits
- Monitor needs safe place to stand: “Learning from Rootkits”
  - Understand properties of rootkit environments
  - Related to Trusted Computing Base
- Monitor environment must be *bullet proof*
  - Rootkit environments are not!
- Measurement strategy
  - How, when and what to measure?
Analysis of x86 Platform

- **Protected Mode**

  Rings for Domain Isolation

  - User mode rootkits
  - Kernel mode rootkits

  - Ring 3 (user mode)
  - Services
  - Drivers
  - Ring 0 (kernel mode)

Patrick Stewin - SPRING 5: “Learning from Rootkits”
Analysis of x86 Platform

- **HW Virtualization Extensions:**
  E.g. OS Isolation

  - Ring 3 (user mode)
  - Ring 0 (kernel mode)
  - “Ring -1” (hypervisor)

  **Virtual machine based rootkits**
Analysis of x86 Platform

- **System Management Mode (SMM):** Special Processor Mode

  - Ring 3 (user mode)
  - Ring 0 (kernel mode)
  - “Ring -1” (hypervisor)
    - “Ring -2” (SMM)

  SMM based rootkits
Analysis of x86 Platform

- **Intel Active Management Technology (iAMT):**

  - Ring 3 (user mode)
  - Ring 0 (kernel mode)
  - "Ring -1" (hypervisor)
  - "Ring -2" (SMM)
  - "Ring -3" (AMT)

  AMT based rootkits
## Challenges for Attackers/Rootkits

<table>
<thead>
<tr>
<th>Hardware</th>
<th>iAMT (Ring -3)</th>
<th>SMM (Ring -2)</th>
<th>Firmware</th>
<th>VMM (Ring -1)</th>
<th>Kernel-mode (Ring 0)</th>
<th>User-mode (Ring 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infiltration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain</td>
<td>cooperation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail/ Download</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Vulnerability</td>
<td>exploitabe until publicly known</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Collection

<table>
<thead>
<tr>
<th>Isolation</th>
<th>DeepWatch</th>
<th>DeepWatch</th>
<th>VM introspection</th>
<th>intrusion detection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>antivirus</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>hardware discrepancies</td>
<td>behavior blocking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>kernel hook</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Red Pill</td>
<td>integrity checks</td>
</tr>
<tr>
<td>Amount of Data</td>
<td>FW measurement</td>
<td></td>
<td></td>
<td>performance loss</td>
</tr>
</tbody>
</table>

### Exfiltration

<table>
<thead>
<tr>
<th>Outbound Channel/ Traffic</th>
<th>router firewall</th>
<th>router/ personal firewall</th>
</tr>
</thead>
</table>

**Monitor is trustworthy**

**Could be used to attack monitor**
Important Related Work


Conclusion and Further Research

- Modern x86 platforms have very powerful stealth capabilities (stealthier than root in user mode)
  - Cf. kernel mode, VMBR, SMM, iAMT
- Basis for monitor environment

**Further Research:**
- Countermeasures against rootkits (e.g., ring -3 rootkits)
- Measurement strategy (cf. TOCTOU example)
  - When and what to measure?
    - Depends on use cases!
  - Which “ring”?
- Develop runtime monitoring/attestation system according to measurement strategy
Thank you!

Questions?