Securing the Linux Kernel - Security Features and Attack Vectors

Bachelor/Master Seminar SoSe 2020
Barbora Hrdá and Monika Huber
January 28, 2020
Securing the Linux Kernel

Topic Suggestions

- (Security Issues in) Hardware Virtualization
- Privilege Escalation
- Isolation with Namespaces and Cgroups
- Sandboxing with seccomp
- Security Enhanced Linux (SELinux)
- AppArmor
- Full Disk Encryption
- Integrity Management Architecture using Secure Boot as an example
- Spectre
- Meltdown

Students are welcome to suggest own topics.
Securing the Linux Kernel

Prerequisites

- IN0009 Grundlagen: Betriebssysteme und Systemsoftware
- IN0004 Einführung in die Rechnerarchitektur
- Preferable: IN2209 IT Sicherheit
- Interest in the Linux operating system and security topics
Securing the Linux Kernel

Objectives

- Understand Linux Kernel security mechanisms and attack vectors.
- Preparing and writing a scientific paper in LaTeX (in English, 8-10 pages, LNCS).
- Presenting a scientific topic (in German/English): 30 minutes + 15 minutes discussion.
- Active participation.
Securing the Linux Kernel

Grading

- Scientific paper: 40% (Content, Style, Effort, Grasp)
- Presentation: 40% (Content, Lecture Style, Understandability)
- Presentation Slides: 10% (Content, Style)
- Active participation: 10%
Securing the Linux Kernel

Registration

- Send us an email with your top 3 desired topics.
- You can add a letter of motivation to emphasize your top choice.
- Register in the Matching system on time.
- We’ll assign topics to students with your input.
## Securing the Linux Kernel

### Time Table

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.01.</td>
<td>Preliminary meeting (today)</td>
</tr>
<tr>
<td>12.02</td>
<td>Deadline for registration in matching system and email with desired topics</td>
</tr>
<tr>
<td>03.03, 10:00-11:00</td>
<td>Kickoff meeting(^1) with topic distribution</td>
</tr>
<tr>
<td>20.04</td>
<td>Deadline for deregistration (afterwards: 5.0!)</td>
</tr>
<tr>
<td>04.05, 23:59</td>
<td>Deadline for submission of table of contents (ToC)</td>
</tr>
<tr>
<td>06.05, - 20.05</td>
<td>Individual meetings(^1) to discuss ToC</td>
</tr>
<tr>
<td>17.06, 23:59</td>
<td>Deadline for submission of paper</td>
</tr>
<tr>
<td>24.06, 23:59</td>
<td>Deadline for submission of presentation slides</td>
</tr>
<tr>
<td>01.07, 10:00-12:00</td>
<td>Presentation meetings(^1)</td>
</tr>
<tr>
<td>02.07, 13:00-16:00</td>
<td>(attendance compulsory!)</td>
</tr>
<tr>
<td>08.07, 10:00-12:00</td>
<td></td>
</tr>
<tr>
<td>09.07, 13:00-16:00</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\)All seminar meetings will be held at Fraunhofer AISEC
Contact Information

Barbora Hrdá and Monika Huber

Department Secure Operating Systems
Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Lichtenbergstr. 11
85748 Garching (near Munich)
Germany

Internet: http://www.aisec.fraunhofer.de

Phone: +49 89 3229986-167 (Barbora) or
+49 89 3229986-148 (Monika)

E-Mail: barbora.hrda@aisec.fraunhofer.de or
monika.huber@aisec.fraunhofer.de