Securing the Linux Kernel - Security Features and Attack Vectors

Bachelor/Master Seminar SoSe 2020

Barbora Hrdá and Monika Huber

March 3, 2020

Fraunhofer AISEC

Securing the Linux Kernel

Topic Distribution

Topic	Student
(Security Issues in) Hardware Virtualization	Samuel Hopstock
Privilege Escalation	Markus Budeus
Isolation with Namespaces and Cgroups	Mathis Engelbart
Sandboxing with seccomp	Mete Polat
Security Enhanced Linux (SELinux)	Benjamin Orthen
AppArmor	Sebastian Warter
Full Disk Encryption I: Comparison of LUKS and Bitlocker	David Maul
Full Disk Encryption II: Full Disk Encryption on Android	Jan Schopohl
Integrity Management and Secure Boot	Julian Scheipl
Spectre	Samy El Deib
Meltdown	FabianÜhrer
Linux Audit Framework	Philipp Friese

Securing the Linux Kernel

Orientation Questions for Security Features

- Goal: What asset is protected with this security measure?
- Functionality: How does the mechanism achieve its intended goal?
  Where in the system does it take effect?
- Usage: Which tools use this mechanism and how do they do it?
  What (popular) implementations are there?
  What must be considered during use?
- Security Evaluation: How successfully does it achieve its goal?
  What are limitations or weaknesses of the mechanism?
  Are attacks against this feature known (and can they be mitigated)?
- Related Topics: Are there other ways of achieving the same goals?
  Can similar concepts be used to achieve different goals?
- Outlook: Are there current developments?
  Are further improvements or changes to be expected?

Securing the Linux Kernel

Orientation Questions for Attack Vectors

- Goal: What asset is targeted with this attack?
- Functionality: How does the mechanism achieve its intended goal? What fault in the system does it exploit?
- Security Evaluation: Which security features are circumvented? What impact did the attack have? Who was affected by it? How hard is it to mitigate the effects?
- Countermeasures: How can the attack be prevented? What security features were developed to mitigate it?
- Related Topics: Are there similar attacks?
- Outlook: Is the attack still relevant nowadays?

Securing the Linux Kernel

Starting Point

- (Security Issues in) Hardware Virtualization: `https://dl.acm.org/doi/10.1145/2480741.2480757`
- Privilege Escalation: `https://ieeexplore.ieee.org/document/8443329`
- Isolation with Namespaces and Cgroups: `https://ieeexplore.ieee.org/document/8693491`
- Sandboxing with seccomp: `https://ieeexplore.ieee.org/document/7560422`
- Security Enhanced Linux (SELinux): `https://selinuxproject.org`
- AppArmor: `https://gitlab.com/apparmor`

Securing the Linux Kernel

Starting Point II

- Full Disk Encryption I - Comparison of LUKS and Bitlocker:
  `https://eprint.iacr.org/2016/274.pdf`
  Full Disk Encryption II - Full Disk Encryption on Android:
  `https://pdfs.semanticscholar.org/e8cc/ca4394e1f4728f35af4cf077f3d5f3a77c4f.pdf`
- Integrity Management and Secure Boot:
  `https://ieeexplore.ieee.org/document/8804799`
- Spectre: `https://spectreattack.com/spectre.pdf`
- Meltdown: `https://meltdownattack.com/meltdown.pdf`
- Linux Audit Framework: `https://github.com/linux-audit`

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).
  LaTeX-Template for Paper: `ftp://ftp.springernature.com/cs-proceeding/llncs/llncs2e.zip`
- 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

Time Table

03.03. 10:00-11:00	Kickoff meeting with topic distribution[1] (today)
20.04.	Deadline for deregistration (afterwards: 5.0!)
04.05. 23:59	Deadline for submission of table of contents (ToC)
06.05. - 20.05.	Individual meetings[1] to discuss ToC
17.06. 23:59	Deadline for submission of paper
24.06. 23:59	Deadline for submission of presentation slides
01.07. 10:00-**13:00**[2]	
02.07 13:00-16:00	Presentation meetings[1]
08.07. 10:00-**13:00**[2]	(attendance compulsory!)
09.07 13:00-16:00	

[1] All seminar meetings will be held at Fraunhofer AISEC

[2] The meeting time was extended to fit the higher number of student (12 instead of 10)

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

Fraunhofer AISEC