Linux Security – Kernel Features and Attack Vectors

Seminar Sommersemester 2018 @ TUM

Sascha Wessel, January 30, 2018

Linux Security - Kernel Features and Attack Vectors

Seminar Sommersemester 2018

- Linux is a monolithic Unix-like kernel
- Linux is Open Source (GPLv2)
- Linux is widely used: embedded devices, wireless access points, smart TVs, mobile devices, desktop computers, servers, supercomputers, ...

-> Many attacks, (known) vulnerabilities, etc.

-> Many research papers to increase Linux security

-> Familiarize with the research topic...

Linux Security - Kernel Features and Attack Vectors

Themen

- OP-TEE (Trusted Execution Environment)
- Virtualization with KVM (QEMU)
- Sandboxing with seccomp and seccomp-bpf
- Isolation with namespaces and cgroups
- Container management (systemd, docker, CoreOS)
- Linux Security Modules: SELinux, etc.
- System call fuzzing (syzcaller)
- Linux driver fuzzing
- Side channels and countermeasures (cache-timing attacks, Meltdown, Spectre)
- Reproducible builds
- ...

Linux Security - Kernel Features and Attack Vectors

Inhalte – je nach Thema

- Beschreibung der Kernel Features und Funktionsweisen
- Involvierte Subsysteme? In welchen Dateien implementiert?
- Überblick wisssenschaftlicher Veröffentlichungen und Dokumentation
- Zusammenspiel Kernel Feature mit Userland
- Welche Tools verwenden das Kernel Feature? Verwenden sie es unterschiedlich?
- Mögliche Angriffsvektoren?
- Bekannte Schwachstellen? CVEs?
- Entwicklung der letzten Monate
- Ausblick der nächsten Entwicklungsschritte
- Evaluation (security, performance impact)
- ...

Linux Security - Kernel Features and Attack Vectors

Literatur

- Source Code @ GitHub – `https://github.com/torvalds/linux`
- Source Code @ Free Electrons – `https://elixir.free-electrons.com`
- LKML – `http://vger.kernel.org/vger-lists.html`
- LWN.net – `https://lwn.net`
- phoronix – `https://www.phoronix.com`
- `https://scholar.google.com/scholar?q=linux+security`
- ...

Linux Security - Kernel Features and Attack Vectors

Was wird erwartet?

- Grundlegende Programmierkenntnisse in C
- Eigenständige Literaturrecherche
- Erstellung einer Ausarbeitung (englisch) in LaTeX(10-15 Seiten LNCS)
- Erstellung von Slides (englisch)
- Präsentation (deutsch) 30 Minuten + 15 Minuten Diskussion
- Aktive Mitarbeit und Diskussion ist erwünscht

Linux Security - Kernel Features and Attack Vectors

Termine

Vorbesprechung

- Dienstag, 30.1.2018 um 11 Uhr im Raum 01.08.033

Zwischenevaluation

- Freitag, 04.05.2018, 12-14 Uhr im Raum 01.08.033

Vorträge

- Donnerstag, 12.07.2018, 09-18 Uhr im Raum 01.08.033
- Freitag, 13.07.2018, 09-18 Uhr im Raum 01.08.033

Anmeldung/Registrierung

TUM Matching System

- Registrierung vom 09.02.2018 bis 14.02.2018
- `http://docmatching.in.tum.de/index.php/schedule`

Contact Information

Sascha Wessel

Department Secure Operating Systems

Fraunhofer-Institute for
Applied and Integrated Security (AISEC)

Address: Parkring 4
85748 Garching (near Munich)
Germany
Internet: http://www.aisec.fraunhofer.de

Phone: +49 89 3229986-155
E-Mail: sascha.wessel@aisec.fraunhofer.de