Fraunhofer AISEC

Fraunhofer Institute for Applied and Integrated Security AISEC

Seminar: Keeping out Cheats, Viruses and other unwanted programs on Xbox, Switch, iOS, Windows, Linux & co

Fraunhofer AISEC, Department Secure Operating Systems

Why „keep something out“?

- Virus / Malware
  - Protect the user against a system compromise, or limit the impact.
  - Provide trust for the user
- Cheating
  - Protect the game against modifications from the user.
  - Provide trust to other connected peers.
- DRM
  - Protect the media player against data extraction.
  - Provide trust to the content distributor.
- and many more…

- Zero Trust / Device Posture Rating
  - No single purpose or requirement, but a framework to define trust requirements – which can include system trust.
  - Provide a basis (e.g. measurements, or security guarantees) for trust evaluation

Seminar Topics

- System Integrity Attacks and Defenses on Commercial-Off-The-Shelve Hardware (COTS)
  - XBOX, Switch: consoles in general - iOS, Android: mobile platforms - Windows, Linux, MacOS: desktop / server platforms
  - Bring you own topic (discuss with us beforehand - Linux distro xy is not a topic)

In Scope:

- Each student will be assigned one platform / ecosystem. You should:
  - Make yourself familiar with the general **system security architecture** of your platform.
  - Systemize **defensive** mechanisms and explain why they are necessary based on their respective **attacks or bypasses.**
  - Lay-out mechanisms to prove the systems integrity to third party (attestation) – if your platform supports it.
  - Using your observation, evaluate / **rate the current state** of the system security.
- Concrete topic and scope for each paper will be assigned based on the course occupancy and students' preferences and individual background.

Out of Scope:

- Any behavioural analysis or similar.
- Signature databases, threat intelligence and metadata services in general.
- Advanced-Persistent-Threats (APTs) and other black magic.
- Actual malware development.

Target audience

- Requirements:
  - IT-Sicherheit (IN0042)
  - Einführung in die Rechnerarchitektur (IN0004)
  - Grundlagenpraktikum: Rechnerarchitektur (IN0005)
  - Grundlagen Betriebssysteme und Systemsoftware (IN0009)
- Optional, but we absolutely recommend at least one of the following:
  - Background in cheat engineering / malware development / CTF / binary exploitation
  - Background in system administration / sysop / dev-[sec-]op / MDM
  - Background in platform firmware or kernel development/ security
- You need a hacker's mindset for this course.
  - Sources are not solely academical (technical documentation, security writeups / talks etc.)
  - Features may be fully undocumented, only available in code / code-samples.
  - Platforms can be designed to intentionally hide their security architecture.

At a glance

Key Facts & Figures

- This course includes **platform** and systems security. You may be programming, but only if you need to validate some API etc. It is not mandatory or expected.
- Kick-Off: 17.04. 14:00 – 18:00; physical attendance is mandatory.
- Outline submission on 20.05.2024 23:59 Anywhere on Earth (= 21.05.2023 13:59 Munich Time)[1], 5 weeks after kickoff
- Paper submission on 22.07.2024 23:59 Anywhere on Earth (= 23.07.2024 13:59 Munich Time)[2], 9 weeks after outline
- Presentation slots:
  - Times TBA, most likely in the week from August 5th (depends on exams of participants)
  - Location TBD, but most likely at Fraunhofer AISEC (Campus Garching)
  - In person attendance is mandatory.
- This seminar allows up to 7 students maximum and needs at least 3 students to take place.
- Always communicate with all course organizers: sos-seminar-sose-25-organizers@aisec.fraunhofer.de

[1]: https://www.timeanddate.com/worldclock/converter.html?iso=20250521T115900&p1=tz_aoe&p2=168
[2]: https://www.timeanddate.com/worldclock/converter.html?iso=20250723T115900&p1=tz_aoe&p2=168

At a glance

Key Facts & Figures (con't)

- Individual assignment
- Improving scientific writing skills in TeX (8-10 pages, ACM template)[1]
- Presenting a scientific topic (in German/English):
  - 30 minutes + 15 minutes discussion.
- Enhancing knowledge in systems security

- Grading:
  - 30 + 15 minutes discussion.
  - Scientific paper: 50% (Content, Style, Effort, Grasp)
  - Presentation: 40% (Content, Lecture Style, Understandability)
  - Active participation/discussion: 10%

[1]: Will be provided to you at the kickoff meeting.

Topic Application

How to get your topic

If you were not at the preliminary meeting, please contact the organizers sos-seminar-sose-25-organizers@aisec.fraunhofer.de .

Contact

Albert Stark, Katharina Bogad
Secure Operating Systems
Tel. +49 89 3229986-{1020,167,1046}
{firstname}.{lastname}@aisec.fraunhofer.de

Fraunhofer AISEC
Lichtenbergstr. 11
85748 Garching near Munich
Germany
www.aisec.fraunhofer.de

Fraunhofer
AISEC

Fraunhofer Institute for Applied
and Integrated Security AISEC