👋 DUG#9 Closing Remarks 👋

Call for Participation (CFP) for Qubes OS Summit 2025 is open!

We are waiting for your submissions and suggestions for the talks.

List of suggested topics:

- Qubes OS related topics
- UI/UX
- Hardware
- Security features
- App qubes

Date & Venue

Once again Qubes OS 2025 Summit comes to the vibrant city of **Berlin from the 26th to the 28th of September**! This year event will take place in Ahoy Berlin, Wattstraße 11, 13355 Berlin.
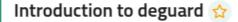
Conference format

Qubes OS 2025 Summit is all about flexibility and inclusiveness. We're seeking speakers who can **join us physically in Berlin or virtually from anywhere in the world**. This hybrid format ensures that the event will be live-streamed, allowing everyone to participate simultaneously, whether they're at the venue or online. Don't miss the chance to be part of this forward-looking conference!

Sponsorship

Empower the Qubes OS Summit 2025 with your sponsorship. Make an impact today - schedule a call or contact us via email at events@3mdeb.com.

Submit a proposal

Introduction to deguard ☆

03-20, 19:00–19:10 (UTC), Dasharo Developers vPub ❓

This talk will introduce the deguard utility, allowing to bypass Intel BootGuard and enabling coreboot development on previously locked down platforms.

Intel Boot Guard has long been a major roadblock for Coreboot development, effectively locking down newer platforms—except for vendors purchasing in bulk with Boot Guard disabled. This talk will explore how that landscape has shifted with Deguard, a tool leveraging a disclosed vulnerability (CVE-2017-5705).

Filip Lewiński
Junior Firmware Developer @ 3mdeb

Become your own UEFI Secure Boot CA - how to implement a secure signing infrastructure in your company. ☆

03-20, 20:00–20:10 (UTC), Dasharo Developers vPub ❓ 🎙

This demonstration is a proposal for implementing a self-hosted, highest-standard, secure infrastructure in your company responsible for maintaining your own UEFI Secure Boot keys for your industrial equipment's firmware. No bureaucracy, no months of waiting for signed binaries, pure operational approach.

See also: 📄 The slideshow (522.1 KB)

Kamil Aronowski

An enthusiast of reasonable security, and a contributor to the UEFI Shim review process.
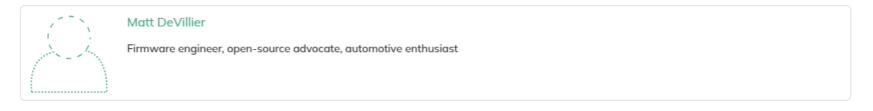
MrChromebox AMA about open source firmware

03-20, 21:00–21:20 (UTC), Dasharo Developers vPub ❓

Join us for a vPub talk with MrChromebox as he shares insights from his open-source firmware development journey. He'll discuss his background, the project's inception, and engage in an Ask Me Anything (AMA) session. Whether you're an enthusiast or a seasoned developer, this is an opportunity to ask questions and learn about innovations, challenges, and future directions in open-source firmware. Don't miss it!

Matt DeVillier

Firmware engineer, open-source advocate, automotive enthusiast

Zen1-4 of uCode Hacking ⭐

03-20, 22:00–22:20 (UTC), Dasharo Developers vPub ❓

What happens when you mix a few beers with microcode? Join us for a wild ride through the underbelly of CPUs, where we hack, jive, and sip on insights! We will explore the chaotic art of microcode hacking, uncovering vulnerabilities while cracking jokes and enjoying cold drinks. Embrace the chaos, unleash some Zen, and let's toast to breaking stuff in the name of security! Who knew low-level code could be this much fun? 🥂💻

Andrew Cooper

Hypervisor and kernel hacker. XenServer, upstream Xen maintainer and security team member.

DASHARO

- **Test:** Dive into our latest releases, test them out, and share your feedback. Your experiences refine our roadmap. 🧪

- **Choose:** Choose to be an active part of our community. Your engagement shapes Dasharo's evolution. 🛠️

- **Know:** Stay informed and share your knowledge. Together, we deepen our understanding and create a robust firmware solution. 🎓

Your Actions Matter 🌟 Thank You 🙏

- **Spread the Word**: Help more people discover, test, and choose Dasharo. 🗣️

- **Contribute**: Your code, documentation, and ideas are the building blocks of Dasharo's growth. 👩‍💻👨‍💻

- **Engage**: Join our discussions, forums, and DUG meetings. Every interaction enriches our community. 🤝

DUG wraps up…

..vPub kicks in. Same passion, less formal, more cypherpunk. Cheers to open firmware freedom!