The Year in Embedded Security

Marta Rybczynska

The Year in Embedded Security

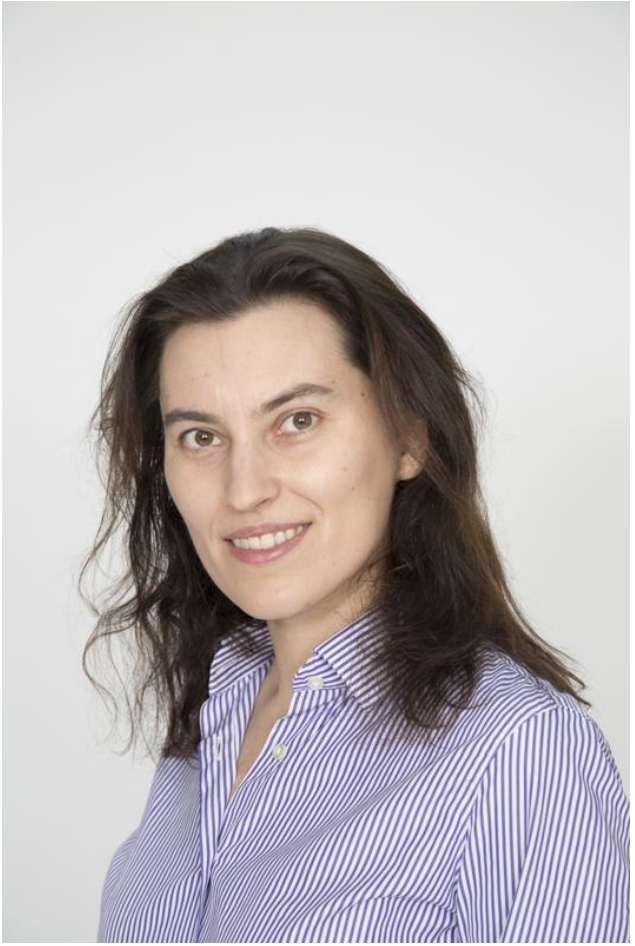
YGREKY

- Regulation
  - CRA & friends -> 1,5 years from now
- Cryptography
  - Post-quantum getting real
- Tools
  - AI and AI-assisted development, hardening improvements
- Dependencies and SBOMs
  - Bootloader security
- Vulnerabilities

Who is Marta Rybczynska?

YGREKY

- PhD in Telecommunications
  - Network security/anonymity systems
- Open source/embedded developer/architect
  - 20+ years in open source
  - Contributions to the Linux kernel, various RTOSes
  - Co-maintainer of meta-security YP layer
  - Yocto Project security team and Open Embedded Technical Steering Committee member
- Founder/CEO of Ygreky
  - Consulting (processes, architecture, audits)
  - Teaching (“Embedded Security”, webinars)
  - Current contribution to CRA-related standardisation
  - Conference keynotes



Where do we start?

The Year in Embedded Security

YGREKY

- Regulation
  - CRA & friends -> 1,5 years from now
- Cryptography
  - Post-quantum getting real
- Tools
  - AI and AI-assisted development, hardening improvements
- Dependencies and SBOMs
  - Bootloader security
- Vulnerabilities

Regulations

Regulations (1)
CRA (Cyber Resilience Act) and friends

YGREKY

- Next dates
  - Exploited vulnerability and security incident reporting: September 2026
  - Full CRA applies: December 2027
- What happened in 2025 - regulations
  - Work on standards - many went to the first review round
    - Reminder: standards are not mandatory
    - Persisting problems: availability for a fee, small number of people writing them
  - European Vulnerability Database (EUVD) early preview online
    - https://euvd.enisa.europa.eu/
    - But no reporting feature yet
  - Commission FAQ on manufacturers
    - Support period counts from sales (of the manufacturer)
    - Confirmed that risk assessment is the base
    - Read it at: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions

Regulations (2)
CRA (Cyber Resilience Act) and friends

YGREKY

- What happened in 2025 - the embedded market
  - Increased awareness
    - Check your vendor, if no trace of a CRA plan - warning!
    - Some vendors start providing SBOMs
  - Misinformation
    - Presenting features as mandatory (even if they are not)
    - Claiming CRA compliance (verify three times!)

Regulations (2)
CRA (Cyber Resilience Act) and friends

YGREKY

- What happened in 2025 - the embedded market
  - Increased awareness
    - Check your vendor, if no trace of a CRA plan - warning!
    - Some vendors start providing SBOMs
  - Misinformation
    - Presenting features as mandatory (even if they are not)
    - Claiming CRA compliance (verify three times!)
  - Are you ready?
    - Do you already have your update plan in place?
    - Do you have your vulnerability management in place?
    - Do you know what risk assessment is?
      - This is the **critical** part
      - “How and why do the bad guys attack embedded products” from ELCE2025 https://osseu2025.sched.com/event/25Vx4/how-and-why-do-the-bad-guys-attack-embedded-products-marta-rybczynska-ygreky

Cryptography

Cryptography
Post-quantum getting real

YGREKY

- Quantum computing may break current public key algorithms
  - Impact: signatures, public key (including your SSH access)
  - Not impacted: encryption like AES
- Timeframe: from a few years to decades
  - Why important for embedded?
    - Devices in the field!
    - Space/memory needed for extra code
    - No HW acceleration in older processors
- Notable software support for post-quantum
  - OpenSSL 3.5 (LTS) April 2025 https://openssl-library.org/post/2025-02-12-openssl-3.5-go-nogo/ and https://openssl.foundation/news/the-features-of-3-5-post-quantum-cryptography
    - Then LMS signature verification in 3.6

Cryptography
Post-quantum getting real

- Have you looked into post-quantum already?

Tools

Tools
Tools impacting embedded security

YGREKY

- Compilers
  - -fhardened in GCC 14.1 and 15.1
  - Execute-only improvements on AArch64 in LLVM 21.1.0
- Move to memory-safe languages
  - “The end of the Rust experiment” in Linux (December) -> as a success
    - See https://www.phoronix.com/news/Rust-To-Stay-Linux-Kernel
- AI and AI-based tooling
  - AI-Accelerated Development: Practical Applications for Embedded Systems Engineers by Christophe Conil https://www.youtube.com/watch?v=86UczUYjVQ0
  - Security vulnerabilities both good and bad found with IA (talks this year at FOSDEM)

Dependencies and SBOMs

SBOMs
Software Bill of Materials

- Generation becoming more common
  - Working in the Yocto Project, Zephyr…
  - Even some SDK vendors provide SBOMs now
- Unsolved problems in embedded
  - Patched source trees
    - And naming of forks
  - Copied code
  - SBOMs of firmware (WiFI, Bluetooth…)

Bootloaders
Looking into dark places

YGREKY

- Bootloaders
  - Close to hardware, high permissions
  - “The Bootloader: An Underestimated Risk To Embedded Linux Security” by Richard Weinberger https://www.youtube.com/watch?v=HbALPAiBxa0
  - “Hardening the Barebox Bootloader” by Ahmad Fatoum https://www.youtube.com/watch?v=tav_ct4emX8&list=PLbzoR-pLrL6rSxIlgQx8OYw74Az63TpaB&index=15

Vulnerabilities

Some vulnerabilities from 2025
Where can it hit embedded?

YGREKY

- BusyBox wget CVE-2025-60876
  - Attacker could inject headers from a crafted request
- Sudo CVE-2025-32463
  - Allows local user obtaining root even if not listed in sudoers https://www.sudo.ws/security/advisories/
- Git unsafe checkout of submodules CVE-2025-48384
  - Unsafe checkout might cause execution of code from attacker-controlled repository

Wrapping-up

Wrapping-up
We’re moving fast

- Regulations, changes in cryptography…
- More interest in security subjects
  - Multiple talks at Embedded Linux Conference Europe in August
  - “Yocto Project Virtual Summit” (December) had one day of security subjects!
- If you have information to add in the next version of this talk…
  - Contact me!

Questions?