YGREKY

How and Why Do The Bad Guys Attack Embedded Products?

Marta Rybczynska - Founder, Ygreky

Who am I?

YGREKY

- PhD in Telecommunications
  - On anonymity systems
- 20+ years in open source
  - Contributions to the Linux kernel, Yocto Project, and more
  - Security team member of Eclipse Foundation and the Yocto Project
- Strong security focus
  - Security processes
  - Tooling (Yocto Project's cve-check)
  - Those days also: subject around the CRA implementation
- Founder of Ygreky, an open source security company

ALL OPINIONS HERE ARE MY OWN

YGREKY

Stories First

Spying vacuum cleaners

YGREKY

Images from https://www.abc.net.au/news/2024-10-04/robot-vacuum-hacked-photos-camera-audio/104414020 (2024)

We hacked a robot vacuum — and could watch live through its camera

The largest home robotics company in the world has failed to fix security issues with its robot vacuums despite being warned about them last year.

Without even entering the building, we were able to silently take photos of the (consenting) owner of a device made by Chinese giant Ecovacs.

And then things got even creepier.

By Julian Fell | Story Lab | Privacy

Thu 3 Oct

Attacks on firewalls and routers are common

YGREKY

Palo Alto Network Issues Hotfixes for Zero-Day Bug in Its Firewall OS

A sophisticated threat actor is leveraging the bug to deploy a Python backdoor for stealing data and executing other malicious actions.

One of the additional tools that the threat actor deployed on compromised systems was a novel Python backdoor that Volexity has named Upstyle. The security vendor said it found the threat actor using the Upstyle backdoor to execute a variety of additional commands including those for lateral movement within a target network and to steal credentials and other sensitive data from it.

Source: https://www.darkreading.com/cyberattacks-data-breaches/palo-alto-network-issues-hot-fixes-for-zero-day-bug-in-its-firewall-os (2024)

Specific device type - ATM (cash machines)

Various types of attacks over time

- Physical
  - Open the ATM, insert an installation CD (2010s)
  - Insert an (infected) USB key (2010s and 2020s)
- By the bank network
  - Malware instructing the ATM to give out money, eg by SSH tunnels (ATMitch, 2017)

YGREKY

Why?

Attacking embedded devices - untargeted attacks
Typical use cases

Attacking embedded devices - untargeted attacks
Typical use cases

- Just for fun/prestige

Attacking embedded devices - untargeted attacks
Typical use cases

- Just for fun/prestige
- Botnets
  - Denial of Service/Distributed Denial of Service - as a Service
  - Plans starting from 10 euros
  - Usages:
    - Shutting down competitors
    - More chaos/pression during a ransomware attack
    - Tunneling traffic
    - Gaming

Attacking embedded devices - untargeted attacks
Typical use cases

YGREKY

- Just for fun/prestige
- Botnets
  - Denial of Service/Distributed Denial of Service - as a Service
  - Plans starting from 10 euros
  - Usages:
    - Shutting down competitors
    - More chaos/pression during a ransomware attack
    - Tunneling traffic
    - Gaming
- Cryptocurrency mining
  - High-performance devices and servers

Attacking embedded devices - targeted attacks
Typical use cases

Attacking embedded devices - targeted attacks
Typical use cases

- Ransomware
  - Industrial infrastructure in addition to the general network

Attacking embedded devices - targeted attacks
Typical use cases

- Ransomware
  - Industrial infrastructure in addition to the general network
- Breaking infrastructure
  - Eg. wiping out flash content
  - Against competitors, for political reasons etc

Attacking embedded devices - targeted attacks
Typical use cases

- Ransomware
  - Industrial infrastructure in addition to the general network
- Breaking infrastructure
  - Eg. wiping out flash content
  - Against competitors, for political reasons etc
- Spying
  - Extracting data (customers, formulas...)
  - May be collecting data to attack someone else

Attacking embedded devices - targeted attacks
Typical use cases

YGREKY

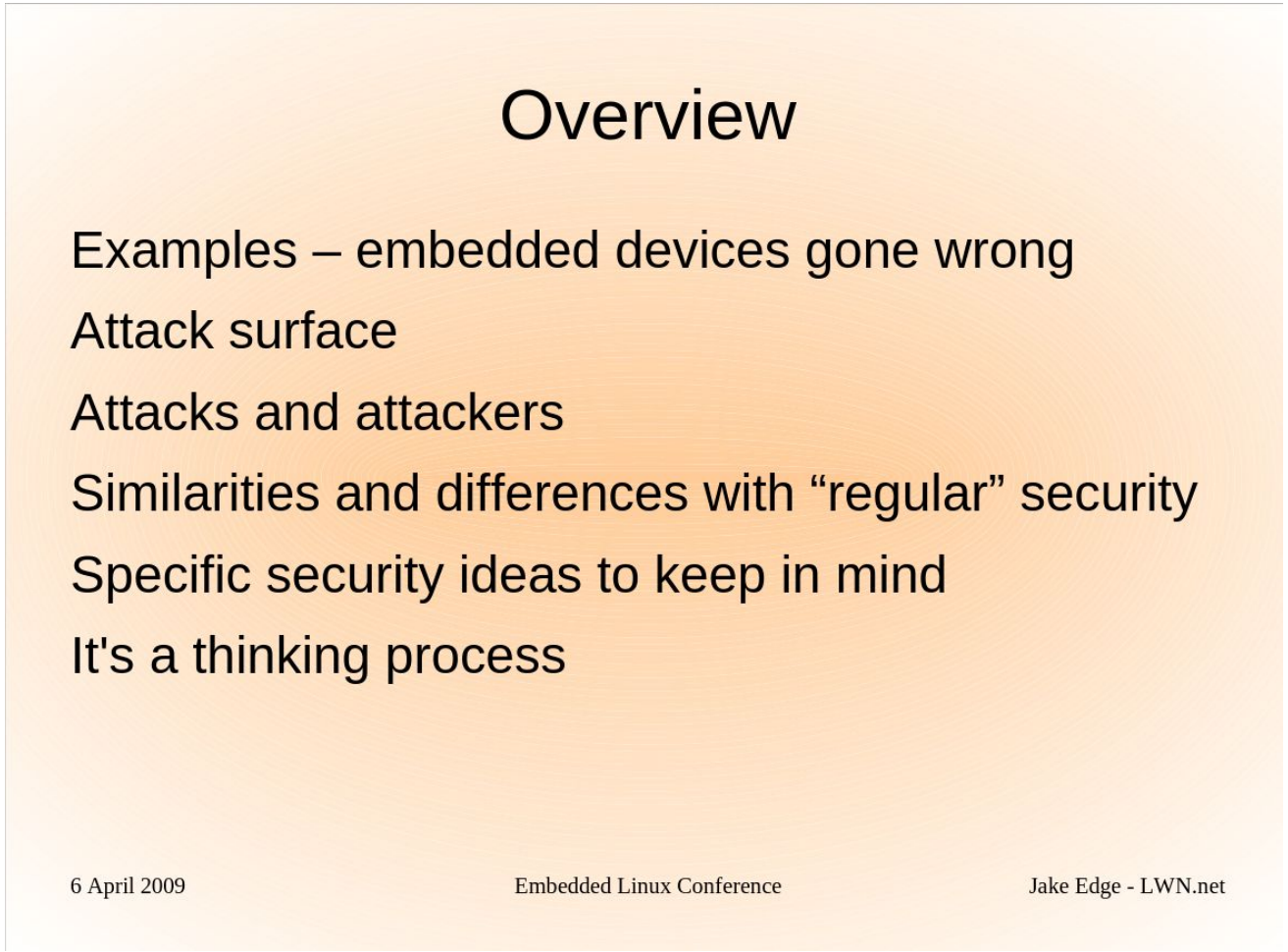
- Ransomware
  - Industrial infrastructure in addition to the general network
- Breaking infrastructure
  - Eg. wiping out flash content
  - Against competitors, for political reasons etc
- Spying
  - Extracting data (customers, formulas...)
  - May be collecting data to attack someone else
- Theft
  - Breaking physical protections to get the device (car...), make it perform an action (ATM...)
  - Extracting confidential code

YGREKY

How has it changed over time?

“Security Issues for Embedded Devices”
By Jake Edge, ELC 2009

YGREKY



The complete slide deck: https://elinux.org/images/6/6f/Security-issues.pdf

2009 and now: what is the same
Reviewing “Security Issues for Embedded Devices”

- Embedded is a target
  - No surprise
- All attack types exist still
  - New ones have appeared
- The procedure to identify risks is the same
  - The exact risks have changed

2009 and now: what has changed
Reviewing “Security Issues for Embedded Devices”

- Devices got more complex, components contain firmware
  - Network packet processing, multimedia handling - moved to component firmware
  - Developers rarely have the firmware’s source
- Apps control devices
  - Additional communication: device<->vendors’s server <->app
  - User data stored on the vendor’s server: risk of exposure

YGREKY

How attackers may target YOUR device?

YGREKY

YGREKY

“Under the CRA, secure boot is mandatory”

YGREKY

“Under the CRA, secure boot is mandatory”

COULD BE, IN YOUR CASE

YGREKY

“When can I get a CRA TODO list?”

Risk analysis: a structured approach

YGREKY

- Warning: many frameworks exist
- The CRA does not impose any specific one
  - But the risk analysis itself is mandatory

Risk analysis: step 1: needed data

- **Product scope:** what does your product do? What is OUT of scope?
- **Assets:** What do you protect?

Risk analysis: step 1: asset examples

YGREKY

- **Router:**
  - User data integrity (when in transit),
  - User network information confidentiality
  - User personal data (when stored)
- **Vacuum cleaner:**
  - Video stream
  - Audio stream
  - Location plans
  - User/family health
  - User property

Step 2: Analyze threats

- Simple option: brainstorm
  - Ask the project team to identify what could go wrong with the device

Step 1: Analyze threats

- Simple option: brainstorm
  - Ask the project team to identify what could go wrong with the device
- More complex: attack surface
  - Analyze actions by all external interfaces (USB, Ethernet, screen, keyboard)
  - Take into account the remote control
  - Review all data flows (internal/external)
  - And why not: which module developed by which team?

Step 1: Analyze threats
With the attack surface

- Example risks
  - An attacker uses the vacuum cleaner to attack other devices in the home network
  - The attacker streams audio/video from the cleaner without authorisation
  - The attacker moves the cleaner around the house (possible damage to property, privacy…)
  - The attacker grabs user data from the vendor's server
  - The attacker changes firmware on the cleaner

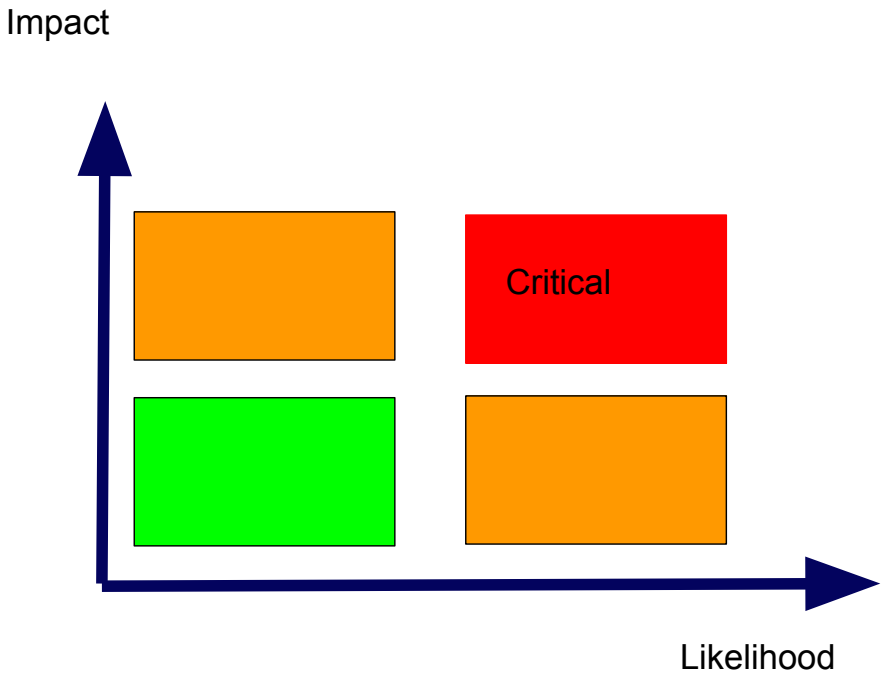
YGREKY

How to deal with attack scenarios?

Step 3: Evaluate

- Probability
  - What is the likelihood the scenario happens?
- Impact
  - If it happens, what the impact will be?
- Typically numeric scale 1-3 or 1-5

Step 3: Evaluate



- For each item from the previous step:
  - Evaluate the likelihood
  - Evaluate the impact
- Sort your list by likelihood X impact

Step 3: Evaluate

- Vacuum cleaner example
  - Brainstorming: the attacker can stream video without authorisation (**impact: 4, likelihood 2**)

Step 3: Evaluate

YGREKY

- Vacuum cleaner example
  - Brainstorming: the attacker can stream video without authorisation (impact: 4, likelihood 2)
  - After code analysis (done by external contractor, no maintenance, no tests, in a language nobody in the team knows) (**impact: 4, likelihood: 4**)

YGREKY

What to do with the sorted list?

Step 4: Handle/treat

YGREKY

- Find actions to:
  - Eliminate
    - Example: Remove a risky interface
    - Example: Add encryption
  - Minimize
    - Example: Perform detailed code review of a module with many security issues
    - Example: Change the library used
- Typically there's a value of **"accepted risk"**

YGREKY

Let’s bring everything together

Summary

YGREKY

- Circular process
  - Can (and) will come back to each stage
- Document each step
- Review regularly
  - When adding important new features
  - Periodically
  - When you learn about new attacks/threats

Resources

- ENISA “Interoperable EU Risk Management Toolbox”
  - https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox
- NIST “Guide for Conducting Risk Assessments” NIST Special Publication 800-30
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- ISO 27001 and 27005 (if you have access)

YGREKY

Can you *try* to do the exercise it for your product now?

Summary (1/2)

- Attackers target embedded devices for multiple reasons:
  - Directly (your device is a target)
  - Indirectly (someone else is a target)
- Millions of devices out there
  - Similar issues, similar unfixed vulnerabilities
  - Internet-connected devices considered easy targets

Summary (2/2)

- When implementing protections
  - 100% secure does not exist
  - Different protections work for different use cases
- Risk analysis advantages
  - Structured reflexion of attackers, their scenarios, resources you want to protect
  - Allow to prioritize response, and save time

Questions?

Contact: Marta Rybczynska
marta.rybczynska@ygreky.com
LinkedIn:
https://www.linkedin.com/in/mrybczynska/