Implanting Security Features into Resource Constrained Embedded Systems

Matthias Wenzl

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
SBA Research

Background

IoT, IIoT, & Embedded Systems

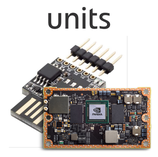
In the last decade, emerging use cases like "Ambient Assistive Technologies", "Car2X" communication, "Smart Homes", "Smart Cities" and Industry 4.0 transformed computer systems to ubiquitous companions in our daily lives. The majority of these use cases consists of embedded computing devices that are highly specialized for their particular purpose.

Requirements

- *Physical:* Operation in harsh conditions, size (e.g. intelligent drilling head).
- *Energy:* Long mission times (e.g. wild-life tracking).
- *Memory:* At least X% of volatile and non-volatile memory must be free during deployment.
- *Real-time requirements:* Adherence to computation time deadlines during operation (e.g., parking assistant).

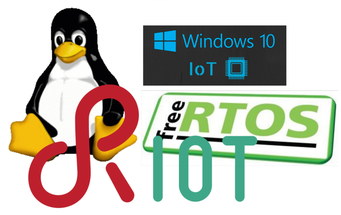
Hardware Heterogenity

- *ATTiny85:* 8-bit ISA, few kb RAM, few kb Flash, no MMU/MPU, low clock frequency, no pseudo random number generator in hardware
- *Jetson TX2:* 64-bit ISA, lots of GB RAM, few GB Flash, complete MMU, $>$ 1 GHz clock frequency, dedicated hardware acceleration units



Software Diversity

- *General purpose OS's:* Windows 10 IoT Core, Linux, *BSD
- *Embedded OS's:* RIOT, TI-RTOS, Free-RTOS, Contiki, QNX
- *Standalone applications:* no operating system at all



Problem & Motivation

IoT/IIoT Security Incidents

- S7 Simatic SPS (2019) Upload of an arbitrary program by utilizing protocol vulnerability
- BMW (2018) Remote exploitable vulnerabilities using the infotainment
- University IoT (2017) Take over of networked luminance sensors, lights and vending machines
- POS (2017) Take over of restaurant receipt printers using remote execution flaws
- Mirai (2016 and before) Botnet mostly exploiting weak default credentials of certain IoT devices
- Jeep (2015) Remote code execution in the Infotainment system

Why are Embedded System so vulnerable?

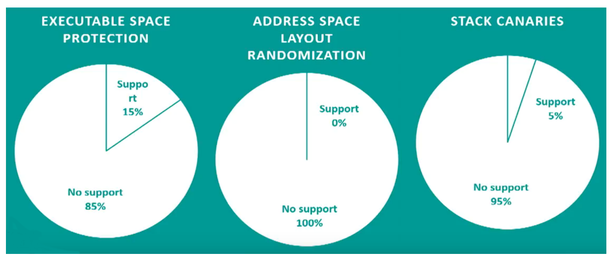


Figure 1: Availability of assorted security features in embedded systems without standard operating system. ("Ghost in the Machine: Challenges in Embedded Binary Security", Wetzels, Usenix Enigma, 2017)

An easy solution?

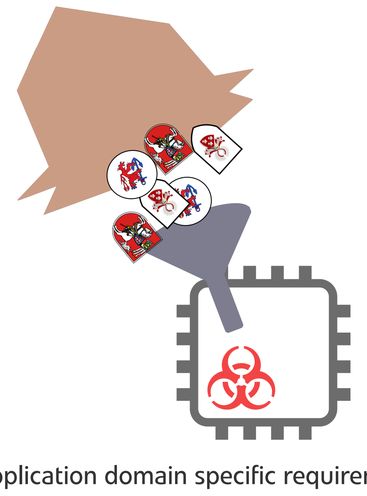


Figure 2: Application domain specific requirements as well as HW and SW diversity hinder the application of common security features in firmware.

Proposed Solution

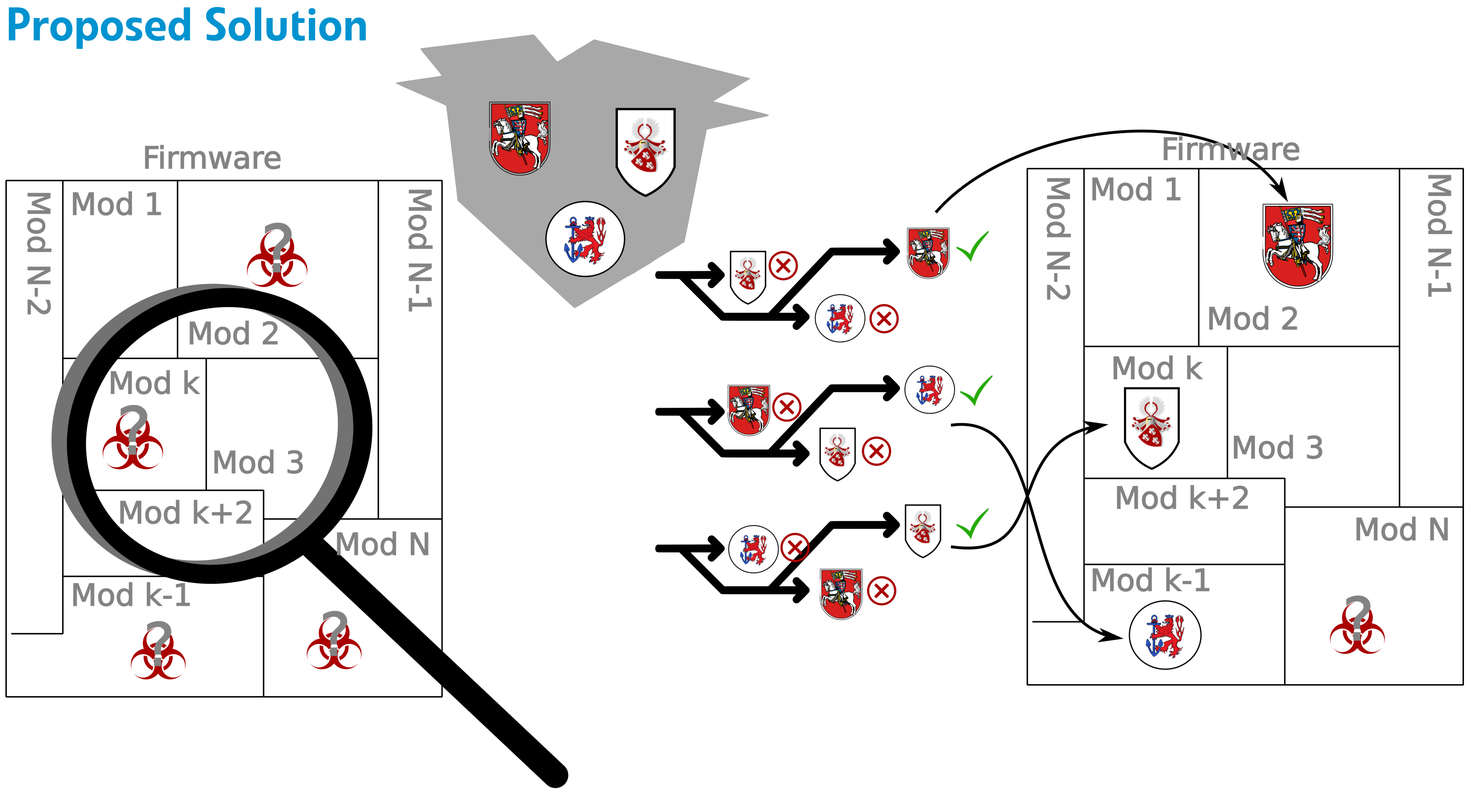


Figure 3: Detection of vulnerable points $\rightarrow$ Select security feature $\rightarrow$ Implant security feature $\rightarrow$ Perform global optimization in order to maximize the number of protected vulnerable points with respect to the system's constraints.

- Detection of potential vulnerable spots $\rightarrow$ taint tracing
- Select appropriate security feature with respect to: run-time, memory complexity, effectiveness.
- Implant security feature using binary rewriting.
- Perform global optimization in order to maximize the number of protected vulnerable points with respect to the system's constraints.
  - **Strategy 1:** Maximize the number of protected vulnerable spots, but allow some to be protected by less effective mitigation techniques
  - **Strategy 2:** Protect the vulnerable spots with high ratings with the most efficient exploit mitigation techniques available, but have less protected in total.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.
This work is partly supported by the Austrian Forschungsförderungsgesellschaft (FFG) in the context of project ISaFe (871230).