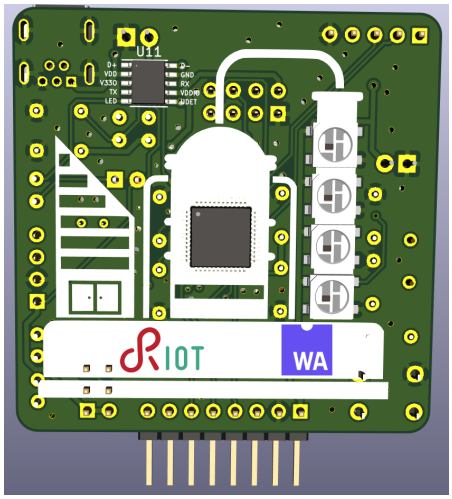
Communication and Networked Systems

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

INF

Master Thesis
Secure Computing Environment for IoT Nodes Using RIOT

RIOT [1] is an operating system for constrained devices (class 0 and upwards using RFC 7228 terminology) which typically power the Internet of Things (IoT). These devices traditionally lack a Memory Management Unit (MMU), rendering traditional concept of user space processes as foundation of memory protection, privilege separation, and access control infeasible. However, the availability of Memory Protection Units (MPUs) and the use of Virtual Machines (VMs) allow for alternative approaches for memory protection and, hence, privilege separation and access control. This topic focuses on how Capability Based Access Control (CBAC) can be used to enable software running in a VM to securely access functionality of the host operating system, RIOT.



Symbolic image of an embedded system running a WASM VM on RIOT

Goals of the Thesis

The goal of this thesis is to design and prototypically implement an interface that enables software running in the WebAssembly (WASM) VM to access functionality of RIOT through system calls, which are secured by CBAC. To achieve this, a serialization format needs to be specified that includes both the byte code of the program to run and its capabilities. At least the integrity and authenticity of the serialized program (byte code and capabilities) needs to be protected using widely accepted cryptographic methods. The verification of capabilities needs to be implemented efficiently. This is especially important since the overhead of cryptographic verification of the integrity and authenticity of the capabilities could easily dominate the costs of some system calls, if that verification is performed for every repetition of the same system call and capability during the same run of the program.

Task

- extend the RIOT common system call code so that an optional permission verification hook can be added

Project type	Master Thesis
Duration	1 Term
Language(s)	English, German
Field	Computer Science

Contact	Marian Buschsieweke
E-Mail	buschsie@ovgu.de
Room	G29-314
Tel.	+49 391 67-52673

- use this hook to perform the verification of capabilities
- prototypically implement the capability check for at least three system calls of your choice
- design and prototypically implement an interface and library for WASM programs that perform system calls protected with CBAC
- evaluate the suitability of CBOR Web Tokens for the serialization of authenticated WASM programs
- design and implement a serialization format for WASM programs, so that both their byte code and capabilities can be transferred via network while cryptographically ensuring integrity and authenticity of the program. (CBOR Web Tokens may be used for this, depending on the result of the previous step.)
- evaluate the security of the system by providing an attack tree and discussing the probability of a successful attack and potential defence measures
- evaluate the overhead of the use of CBAC for system calls in terms of runtime overhead, additional memory (RAM and ROM) consumption for both the OS and the WASM programs, and the additional lines of code required in the source of the WASM program

References

[1] Emmanuel Baccelli and Oliver Hahm and Mesut Güneş and Matthias Wählisch and Thomas Schmidt. RIOT OS: Towards an OS for the Internet of Things. 32nd IEEE International Conference on Computer Communications (INFOCOM). 2013.

Project type	Master Thesis		Contact	Marian Buschsieweke
Duration	1 Term		E-Mail	buschsie@ovgu.de
Language(s)	English, German		Room	G29-314
Field	Computer Science		Tel.	+49 391 67-52673