Secure Access and Management of Smart Objects with SNMPv3

Sven Zehl, Thomas Scheffler
SvenZehl@web.de, scheffler@beuth-hochschule.de

BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN
University of Applied Sciences

ICCE-2013, Berlin September 11, 2013

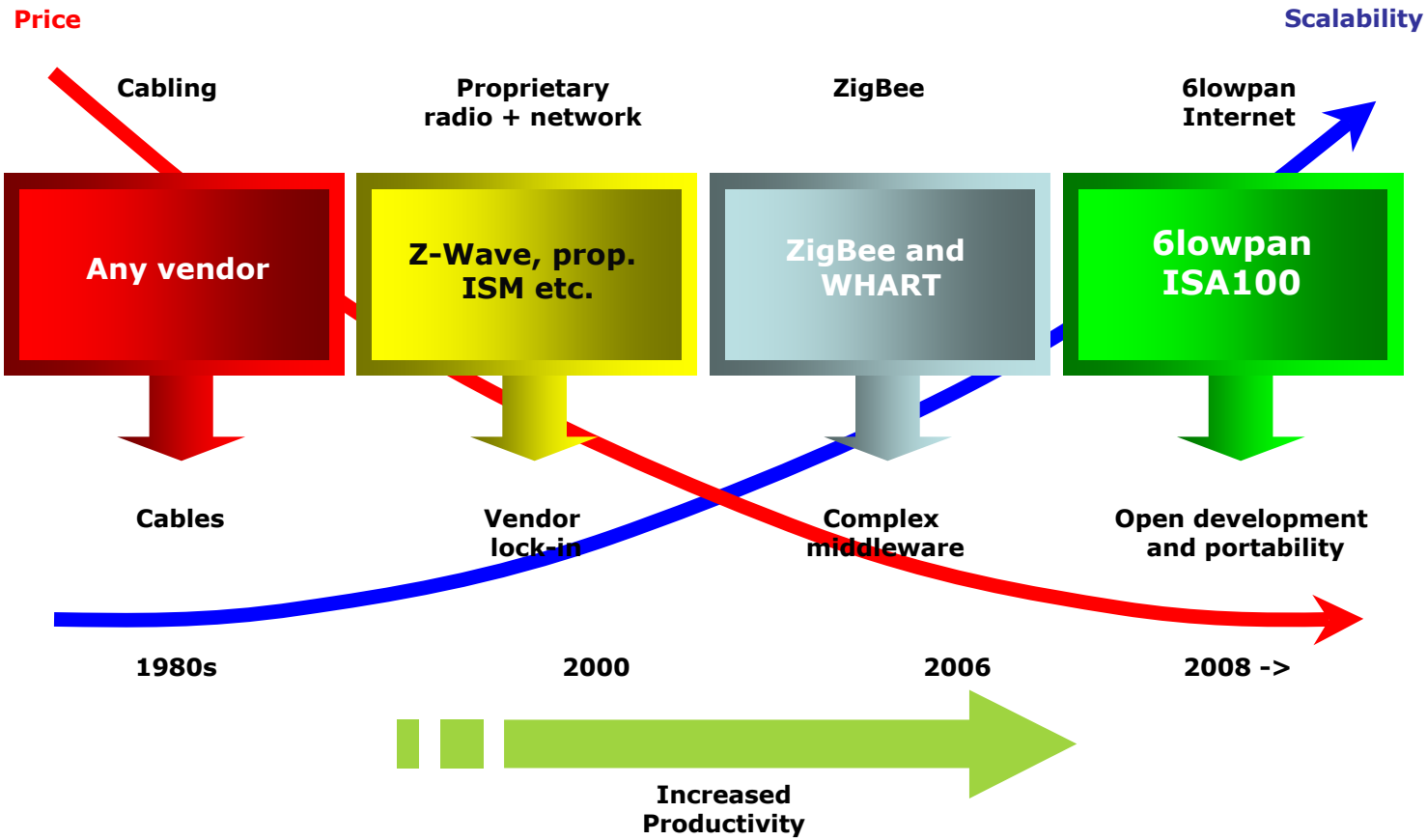
Outline

Smart Objects

*"... a **smart object** is an item equipped with a form of sensor or actuator, a tiny microprocessor, a communication device, and a power source."*

[Vasseur & Dunkels, 2010]

Developments in sensor networks



source: http://6lowpan.net

Challenge: Management of Smart Objects

- Supporting a large number of objects and ad-hoc routing
- Small footprint (energy consumption, size, ...)
- Support for secure application layer
- Proprietary gateways
  Proprietary, untested protocols

Challenge: Management of Smart Objects

- Supporting a large number of objects and ad-hoc routing
- Small footprint (energy consumption, size, ...)
- Support for secure application layer
- Proprietary gateways
  Proprietary, untested protocols

$\Rightarrow$ Using established tools and free/open protocols
Home Automation Routing Requirements in Low-Power and Lossy Networks (RFC 5826)

Challenge: Management of Smart Objects

Development of a smart object to control a 230V consumer device:

- IPv6
  - global addressing and accessibility
  - auto configuration

Challenge: Management of Smart Objects

Development of a smart object to control a 230V consumer device:

- IPv6
  - global addressing and accessibility
  - auto configuration
- 8 bit microcontroller
  - small dimensions (installation in existing devices)
  - low energy consumption ($<$ 1W)
  - inexpensive (10-20 Euro)

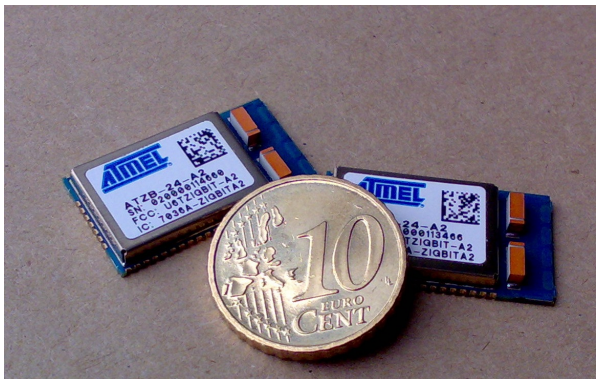
Challenge: Management of Smart Objects

Development of a smart object to control a 230V consumer device:

- IPv6
  - global addressing and accessibility
  - auto configuration
- 8 bit microcontroller
  - small dimensions (installation in existing devices)
  - low energy consumption ($<$ 1W)
  - inexpensive (10-20 Euro)
- Use of standardized tools for network management

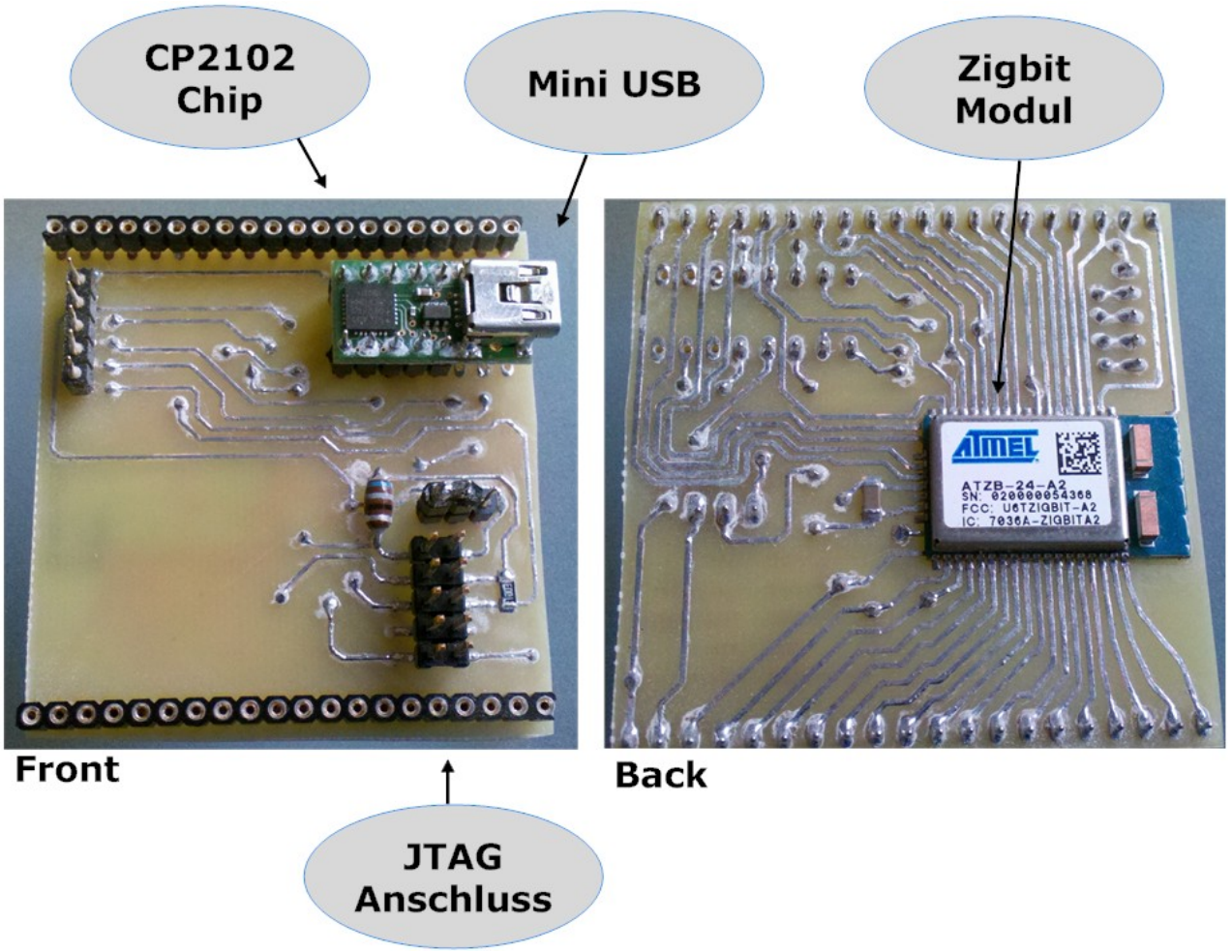
Hardware Description

- **Zigbit-Modul**
  - 8-Bit RISC (Atmega 1281)
  - 4 MHz
  - 128-KB Flash
  - 8-KB SRAM
  - AT86RF230 Radio Transceiver with Ceramic Chip-Antenna

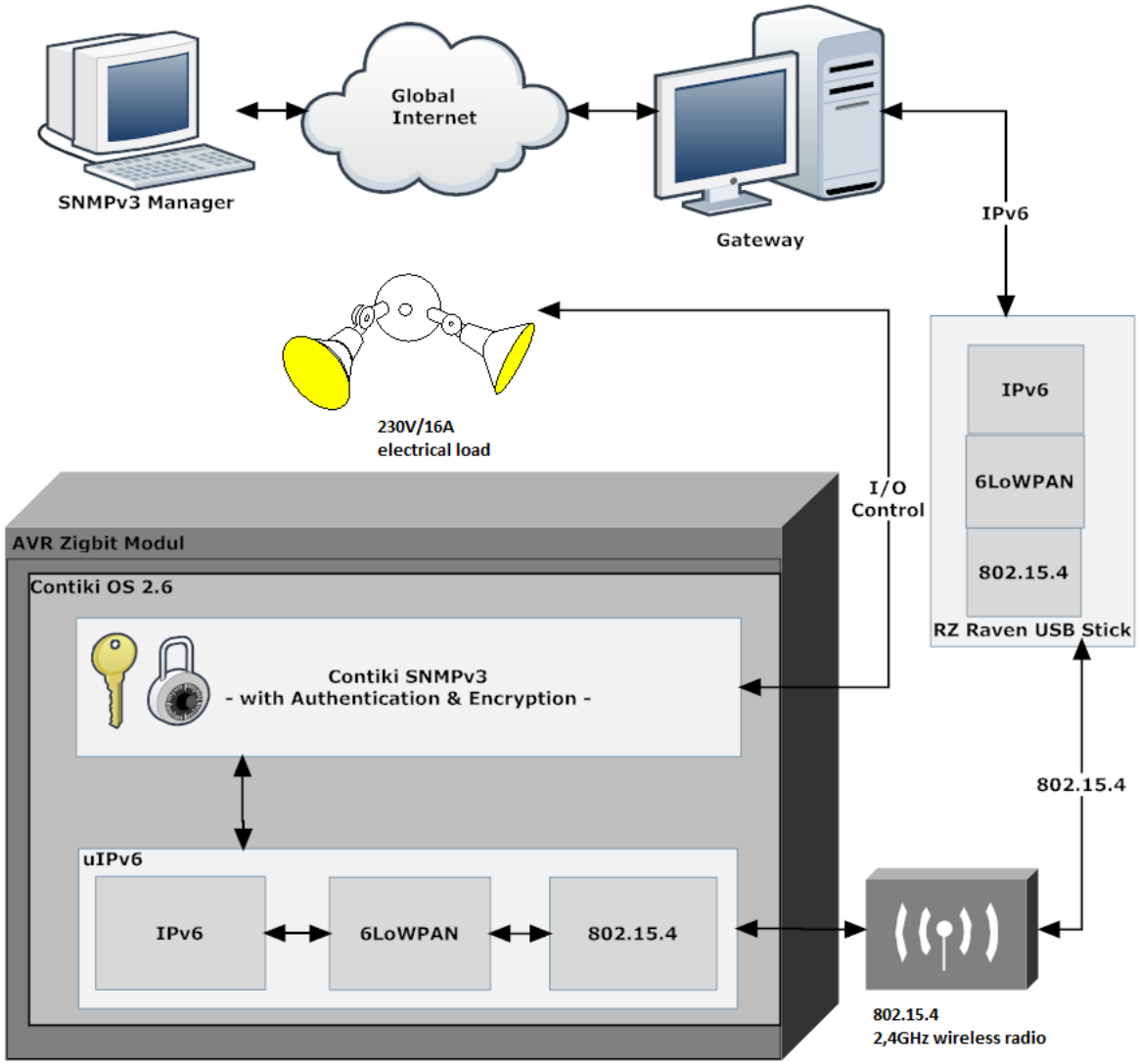


- **Atmel Raven USB-Stick**
  - 8-Bit RISC (Atmega AT90USB1287)
  - 8 MHz
  - 128-KB Flash
  - 8-KB SRAM
  - AT86RF230 Radio Transceiver with PCB Antenna

Breakout Board



Overview of the Implementation



Outline

Contiki OS

- Open operating system for embedded devices
- Originally developed by *Swedish Institute of Computer Science* - active international developer community

Contiki OS

- Open operating system for embedded devices
- Originally developed by *Swedish Institute of Computer Science* - active international developer community
- Ports available for different hardware platforms (AVR, ARM, MSP430,...)
- Support for multithreading and protosockets

Contiki OS

- Open operating system for embedded devices
- Originally developed by *Swedish Institute of Computer Science* - active international developer community
- Ports available for different hardware platforms (AVR, ARM, MSP430,...)
- Support for multithreading and protosockets
- Deployed IPv6 network stack
  - $\sim$ 40 kByte Flash/ROM
  - $\sim$ 2 kByte RAM
  - Development environment available as a VM: **Instant Contiki**
  - http://www.contiki-os.org/

Outline

Management of Smart Objects

Idea:

Use of standardized tools for network management.

Management of Smart Objects

Idea:

Use of standardized tools for network management.

Simple Network Management Protocol (SNMP):

- established protocol in the network management domain
- standardized in RFC 3411 (and other RFCs)
- security features include confidentiality, authenticity and user management (SNMPv3)
- many tools and software libraries available (Net-SNMP, etc.)

Contiki SNMP

- Implementation by Jacobs-Universität Bremen
  - adaptation of NetSNMP Code for Contiki OS (8-bit microcontroller)
  - support for SNMPv1 and SNMPv3
  - http://cnds.eecs.jacobs-university.de/software/contiki-snmp/

Contiki SNMP

- Implementation by Jacobs-Universität Bremen
  - adaptation of NetSNMP Code for Contiki OS (8-bit microcontroller)
  - support for SNMPv1 and SNMPv3
  - http://cnds.eecs.jacobs-university.de/software/contiki-snmp/
- Supports the GET, GETNEXT and SET operations

Contiki SNMP

- Implementation by Jacobs-Universität Bremen
  - adaptation of NetSNMP Code for Contiki OS (8-bit microcontroller)
  - support for SNMPv1 and SNMPv3
  - http://cnds.eecs.jacobs-university.de/software/contiki-snmp/
- Supports the GET, GETNEXT and SET operations
- **User-based Security Model** with the **HMAC-MD5-96 authentication** and **AES-128-CFB symmetric encryption**

SNMP Implementation

SNMPv3 Managed Objects

- Controlling the state of the output-pins of the microcontroller
- Questioning the wireless signal strength (RSSI) and the inbuilt temperature sensor

SNMP Implementation

SNMPv3 Managed Objects

- Controlling the state of the output-pins of the microcontroller
- Questioning the wireless signal strength (RSSI) and the inbuilt temperature sensor

Application example

Controlling the state of the electrical socket:

```
snmpset -v3 -c public -u sk -l authPriv -a md5 -A password1 \
    -x aes -X password2 udp6:[fd00:142::11:22ff:fe33:4455]  \
    iso.3.6.1.4.1.22109.100.600.1.0 i 1

SNMPv2-SMI::enterprises.22109.100.600.1.0 = INTEGER: 1
```

Making the implementation RFC compliant

1. Random generation of 64-bit integer values for IV generation
2. Capturing the number of SNMP engine boots
3. Evaluation of the securityLevel of the user
4. Revised calculations within the Timeliness Module
5. Generation of authenticated reports

Making the implementation RFC compliant

1. Random generation of 64-bit integer values for IV generation
2. Capturing the number of SNMP engine boots
3. Evaluation of the securityLevel of the user
4. Revised calculations within the Timeliness Module
5. Generation of authenticated reports

Random generation of 64-bit integer values for the Initialization Vector

RFC 3826:

The 128-bit IV is obtained as the concatenation of the authoritative SNMP engine's 32-bit *snmpEngineBoots*, the SNMP engine's 32-bit *snmpEngineTime*, and a local 64-bit integer. The 64-bit integer is initialized to a pseudo-random value at boot time.

Random generation of 64-bit integer values for the Initialization Vector

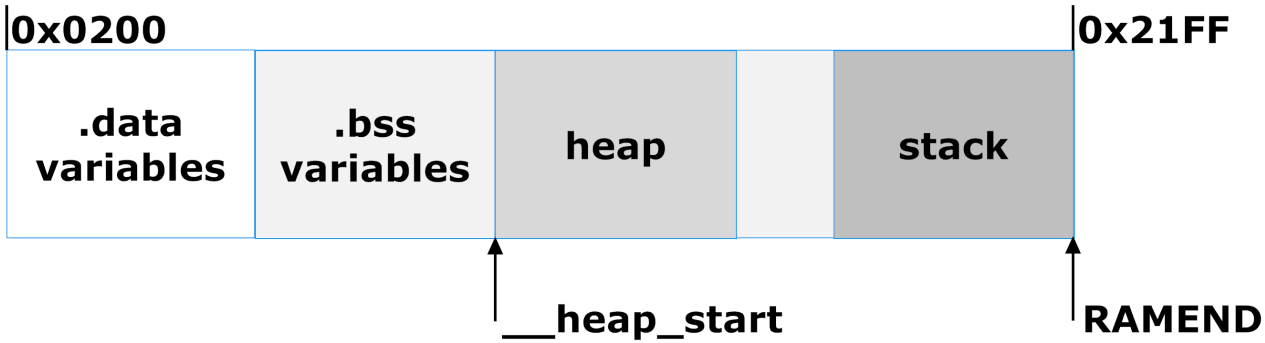
RFC 3826:

The 128-bit IV is obtained as the concatenation of the authoritative SNMP engine's 32-bit *snmpEngineBoots*, the SNMP engine's 32-bit *snmpEngineTime*, and a local 64-bit integer. The 64-bit integer is initialized to a pseudo-random value at boot time.

Idea:

Use the inherently random content of the SRAM to derive a *random seed value* for the random number generator after the device has been powered up.

Generation of Random Seed Value




```
1  u32t get_seed(){
2     u32t seed = 0;
3     u32t *p = (u32t*) (RAMEND + 1);
4     extern u32t __heap_start;
5     while (p >= &__heap_start + 1)
6        seed ^= * (--p);
7     return seed;
8  }
```

Capturing the number of SNMP engine boots

Challenge:

Ordinary SNMP implementations use the file system to store this parameter persistently.

Capturing the number of SNMP engine boots

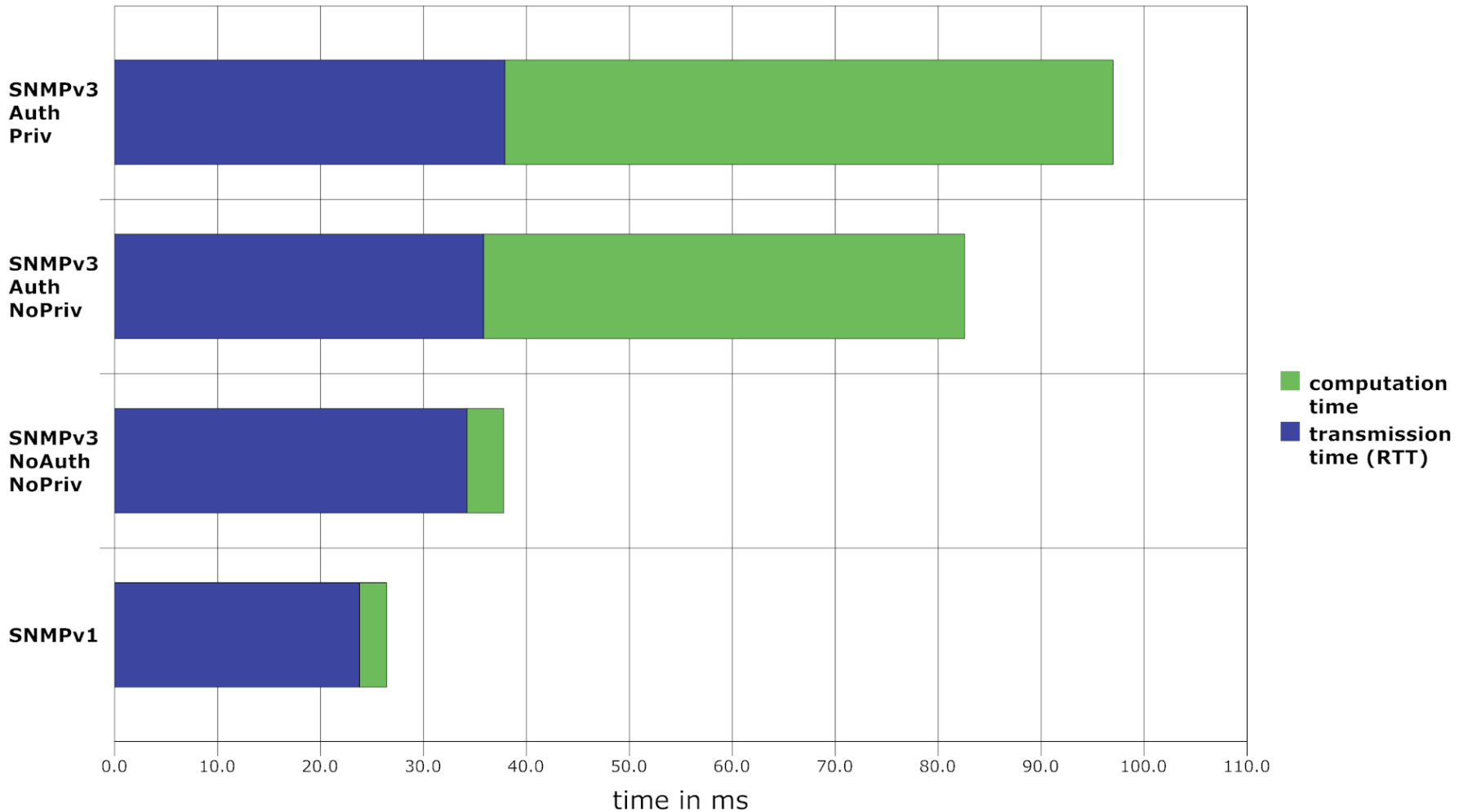
Challenge:

Ordinary SNMP implementations use the file system to store this parameter persistently.

```
1  u8t incMsgAuthoritativeEngineBoots(){
2     if((eeprom_read_dword(&MsgAuthoritativeEngineBoots))
          <2147483647){
3        eeprom_update_dword(&MsgAuthoritativeEngineBoots, (
            eeprom_read_dword(&MsgAuthoritativeEngineBoots)
            +1));
4     }
5     else{
6        printf("Maximum Number of
            MsgAuthoritativeEngineBoots reached\n");
7     }
8     return 0;
9  }
```

Outline

Computation and transmission time



Outlook

- Support for *SNMP Traps*
- Suitable Hardware Platform (SNMP + RPL) $>$ 8 KByte SRAM

Contact

Email: scheffler@beuth-hochschule.de

WWW: http://prof.beuth-hochschule.de/scheffler/

Projekt: https://wiki.ipv6lab.beuth-hochschule.de/contiki/

BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN
University of Applied Sciences