UNIVERSITY OF TRENTO

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

PISTIS: Trusted Computing Architecture for Low-end Embedded Systems

Michele Grisafi
University of Trento, Italy
michele.grisafi@unitn.it

Mahmoud Ammar
Huawei Research, Germany
mahmoud.ammar@huawei.com

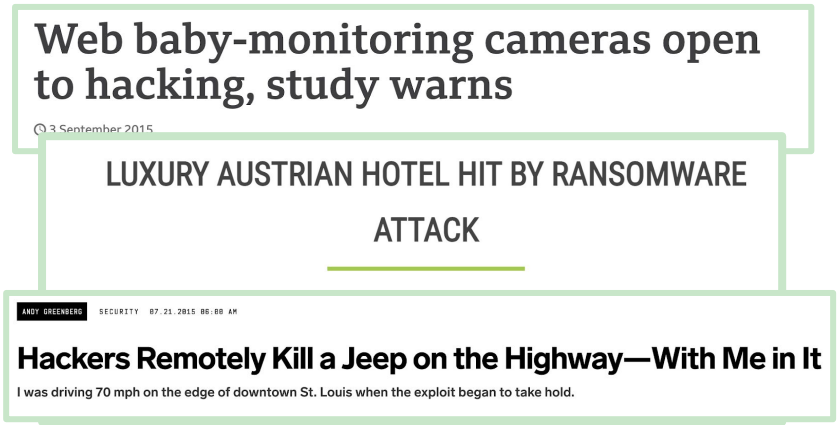
Marco Roveri
University of Trento, Italy
marco.roveri@unitn.it

Bruno Crispo
University of Trento, Italy
bruno.crispo@unitn.it

The issue at hand - embedded systems

The issue:

Embedded systems are at **risk**



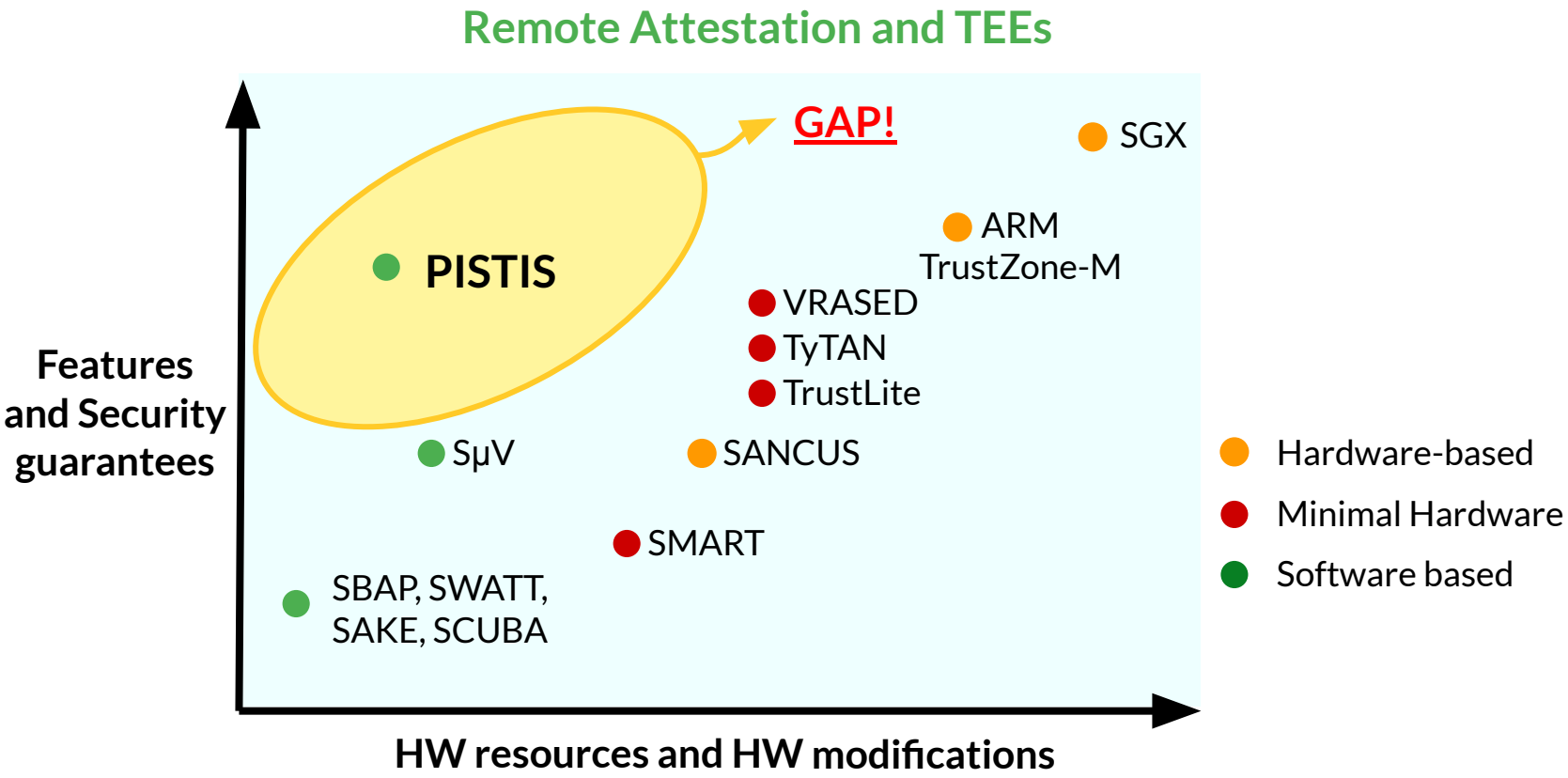
The solution:

Security Services
(e.g., Remote Attestation)

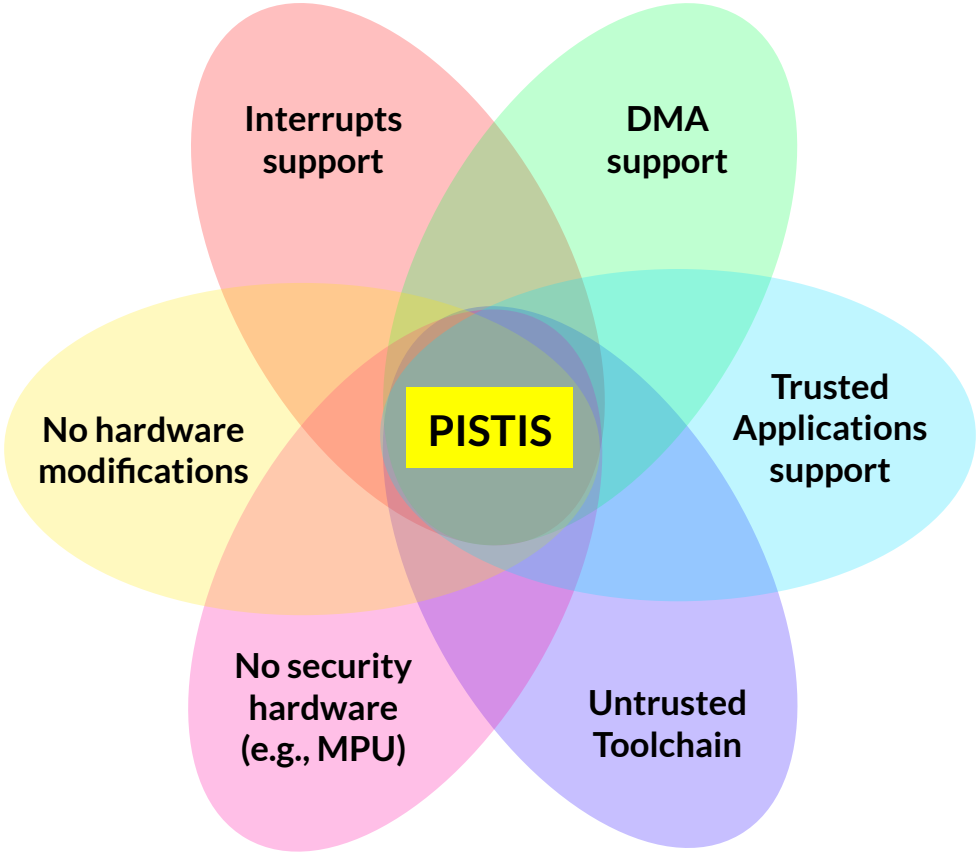
enabled by…

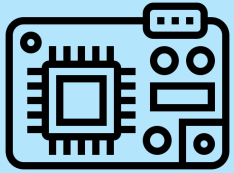
Trusted Execution Environments (TEEs)

The state of the art



A TEE to fill the gap





Low-end MCU
in an embedded system,
CPS, OT or IoT environment

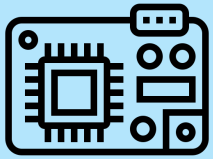
Software-based remote
adversary.
DoS out of scope

When to use Pistis

Trusted Execution Environment (TEE)
with a set of
Trusted Applications (TAs)

PISTIS

Untrusted programmer with the
source code of an application



MCU

Malware

Untrusted Application

Memory Isolation

Remote Attestation

...

Secure Code Update

RoT

Runtime Library

Run-time attack

MitM

3

Corrupt toolchain

Inject malware

1

Trusted Application

Runtime Library

Untrusted Application

2

PISTIS toolchain

Untrusted source files

PISTIS

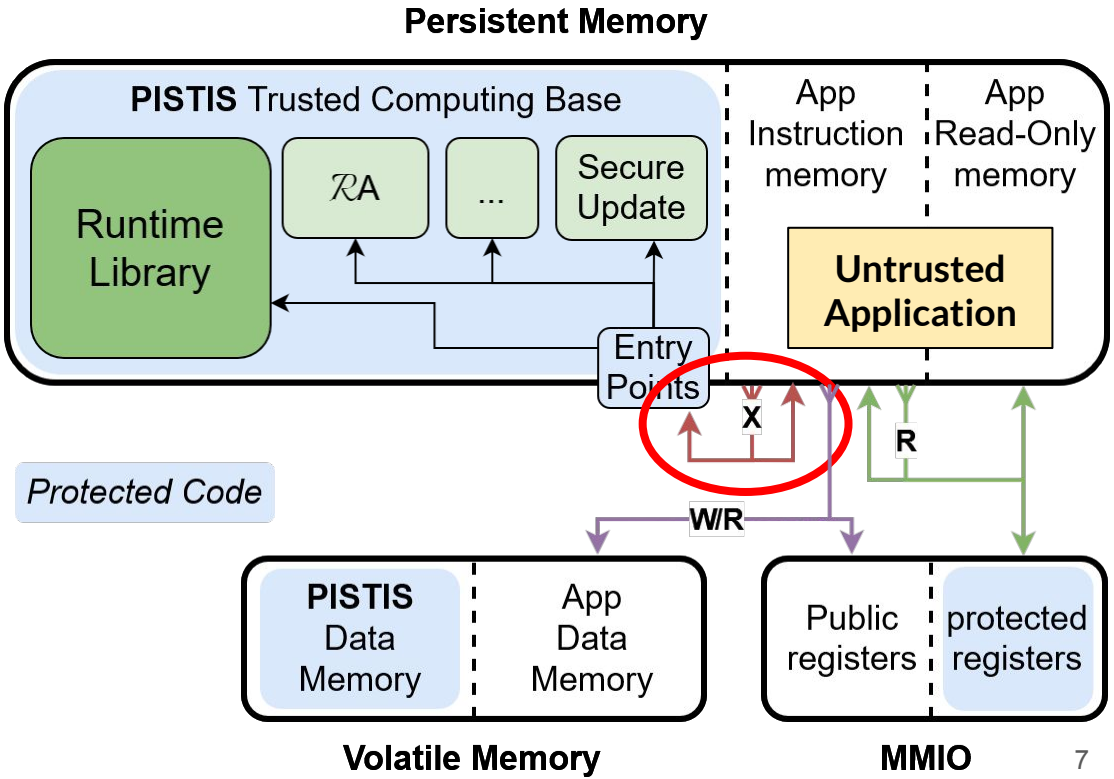
Memory isolation - our policy

How?

1. Divide memory in regions
2. Deploy PISTIS and the application in different regions
3. **Enforce Access Control Policy at runtime**

Software instrumentation and virtualization

Make sure all of the instructions of the application are compliant with our Access Control Policy



A software-based approach

Sample code

.S
```
CALL appFun
CALL R10
```

Custom untrusted toolchain

Replaces **unsafe instructions** with virtual calls to the TCB

.S
```
CALL appFun
MOV R10, R4
CALL vrtCall
```

Deploy

.o
```
CALL appFun ✓
MOV R10, R4
CALL vrtCall ✓
```

Run

```
CALL appFun
MOV R10, R4
CALL vrtCall
```

Compile bypassing instrumentation

.o
```
CALL appFun ✓
CALL R10 ✗
```

✗ REJECT

Binary verification

Rejects applications with **unsafe instructions**

Run-time checks

Check safety of **virtual calls**

```
vrtCall:
is *(R4) safe?
```

CALL

STOP

Performance evaluation

Evaluated on a TI MSP430F5529 MCU with a set of **13 embedded applications**, including CPU, I/O and memory intensive operations, and an official **TI benchmark**.

App	Memory Footprint		Runtime Overhead		Deployment	
	Orig.	Mod.	Orig.	Mod	Orig.	Mod.
SerialMSP	302 B	356 B (**+17.88%**)	334.1976 ms	335.325 ms (**+0.34%**)	3293 ms	409 ms **-87.58 %**
CopyDMA	444 B	628 B (**+41.44%**)	118.4960 ms	238.656 ms (**+101.40%**)	4901 ms	696 ms **-85.80 %**
XorCypher	247 B	475 B (**+92.31%**)	245.6500 ms	446.104 ms (**+81.60%**)	4999 ms	517 ms **-89.66 %**
Bitcount	3684 B	5462 B (**+48.26%**)	5.7520 ms	5.786 ms (**+0.59%**)	5373 ms	2253 ms **-58.07 %**
SHA-256	1376 B	1546 B (**+12.35%**)	49.1888 ms	89.046 ms (**+81.03%**)	8091 ms	4866 ms **-39.86 %**
ML-acc	6174 B	9452 B (**+53.09%**)	1456.9092 ms	3311.829 ms (**+127.32%**)	15383 ms	10039 ms **-34.74 %**
PrimeFactor	2192 B	3286 B (**+49.91%**)	4.0810 ms	5.938 ms (**+45.50%**)	28267 ms	3765 ms **-86.68 %**
32bitMath	522 B	766 B (**+46.74%**)	0.9310 ms	1.294 ms (**+38.99%**)	5148 ms	824 ms **-83.99 %**
16bitSwitch	102 B	126 B (**+23.53%**)	0.0050 ms	0.006 ms (**+20.00%**)	3318 ms	191 ms **-94.24 %**
8bitMatrix	844 B	860 B (**+1.90%**)	0.5760 ms	0.577 ms (**+0.17%**)	4043 ms	960 ms **-76.26 %**
MatrixMul	500 B	516 B (**+3.20%**)	0.3430 ms	0.344 ms (**+0.29%**)	3706 ms	678 ms **-81.71 %**
firFilter	3312 B	5430 B (**+63.95%**)	1093.5059 ms	2359.619 ms (**+115.78%**)	21400 ms	5487 ms **-74.36 %**
dhrystone	1335 B	2411 B (**+80.60%**)	102.9200 ms	177.336 ms (**+72.30%**)	6747 ms	2415 ms **-64.21 %**
Average		**+41.17%**		**+52.72%**		**-73.63%**

UNIVERSITY OF TRENTO

To recap PISTIS

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Why do we need it?

- To bridge the security gap for low-end embedded systems
- Need for feature-rich and strong security solutions
- PISTIS might be the cheapest available option

What is it?

- Trusted Execution Environment (TEE)
- Support for TAs (e.g., Remote Attestation)
- Support for secure DMA and Interrupts operations

How does it work?

- Policy-based Memory Isolation
- Software-based Trusted Computing Base
- Software instrumentation and virtualisation

Q&A → *michele.grisafi@unitn.it*

`github.com/CybersecurityUnitn/PISTIS` ← Check it out!