Experiments on automation of formal verification of devices at the binary level

Thomas Lacroix

INSA Lyon
Soutenance de PFE (Option R&D)

19/06/2019

Section 1

Motivation

Table of Contents

Security critical systems

Privacy

- Smartphones
- Smart TVs

Security

- Hospital equipment
- Traffic control systems
- Power plants

Security critical systems - vulnerable

https://www.wired.com/2014/04/hospital-equipment-vulnerable/
It's Insanely Easy to Hack Hospital Equipment

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
Hackers Remotely Kill a Jeep on the Highway—With Me in It

Vulnerabilities come because of:

- Increased surface of attack (more and more features, codebases explode in size)
- Connected to networks $\rightarrow$ remote attacks

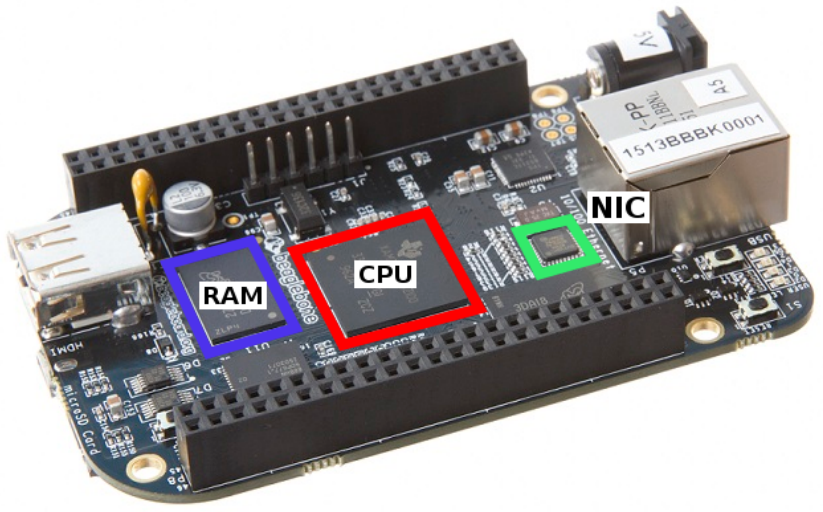

Figure: BeagleBone Black.

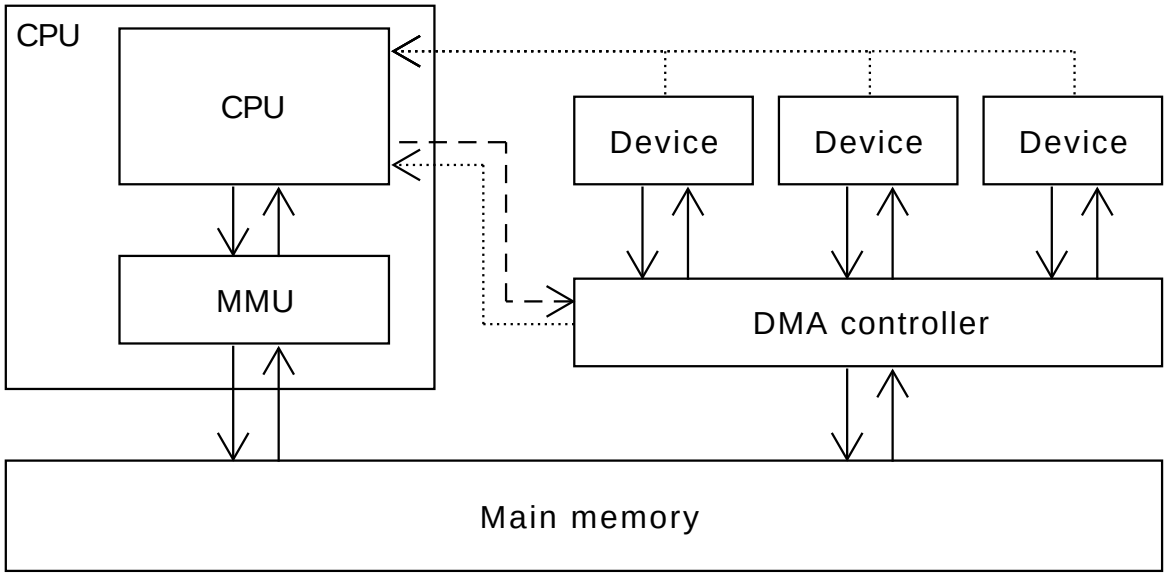

Figure: Communication between CPU and devices.

Table of Contents

Simple frame

Table of Contents

Simple frame

Section 2

Non proof-producing verification

Table of Contents

Title

Table of Contents

Title

Section 3

Proof-producing verification

Table of Contents

Title

Section 4

Conclusion

Questions

References I