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

Motivation

- Motivation
 - Network Interface Controllers
 - How to model a NIC
 - Using software verification tools for hardware devices?
- 2 Non proof-producing verification
 - Subsection 1
 - How trustful is it?
- Proof-producing verification
 - Subsection 1
- 4 Conclusion

Privacy

Motivation

000000000

- Smartphones
- Smart TVs

Security

Proof-producing verification

- Hospital equipment
- Traffic control systems
- Power plants

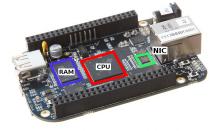
https://www.wired.com/2014/04/hospital-equipment-vulnerable/ It's Insanely Easy to Hack Hospital Equipment https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ Hackers Remotely Kill a Jeep on the Highway—With Me in It

Proof-producing verification

Vulnerabilities come because of:

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

0000000000



Proof-producing verification

Figure: BeagleBone Black.

0000000000

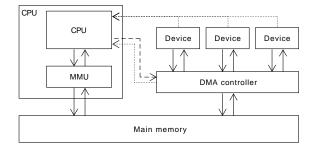


Figure: Communication between CPU and devices.

Table of Contents

- Motivation
 - Network Interface Controllers
 - How to model a NIC
 - Using software verification tools for hardware devices?
- 2 Non proof-producing verification
 - Subsection 1
 - How trustful is it?
- Proof-producing verification
 - Subsection 1
- 4 Conclusion

Proof-producing verification

Motivation

0000000000

Conclusion

- Motivation
 - Network Interface Controllers
 - How to model a NIC
 - Using software verification tools for hardware devices?
- 2 Non proof-producing verification
 - Subsection 1
 - How trustful is it?
- Proof-producing verification
 - Subsection 1
- 4 Conclusion

Simple frame

Section 2

Proof-producing verification

Non proof-producing verification

Table of Contents

- Motivation
 - Network Interface Controllers
 - How to model a NIC
 - Using software verification tools for hardware devices?
- 2 Non proof-producing verification
 - Subsection 1
 - How trustful is it?
- Proof-producing verification
 - Subsection 1
- 4 Conclusion

Title

- Motivation
 - Network Interface Controllers
 - How to model a NIC
 - Using software verification tools for hardware devices?
- 2 Non proof-producing verification
 - Subsection 1
 - How trustful is it?
- Proof-producing verification
 - Subsection 1
- 4 Conclusion

Title

Section 3

Proof-producing verification

Table of Contents

- Motivation
 - Network Interface Controllers
 - How to model a NIC
 - Using software verification tools for hardware devices?
- 2 Non proof-producing verification
 - Subsection 1
 - How trustful is it?
- Proof-producing verification
 - Subsection 1
- 4 Conclusion

Title

Motivation 000000000

Section 4

Conclusion

References I