Towards Low-Power and Low Data-Rate Software-Defined Radio Baseband with RISC-V Processor for Flexibility and Security

Mohamed EL-BOUAZZATI, Philippe TANGUY, Guy GOGNIAT
Lab-STICC, team ARCAD, Université Bretagne Sud
firstname.lastname@univ-ubs.fr

Abstract

This work discusses opportunities and challenges of using Software Defined Radio (SDR) in baseband processor architectures dedicated to IoT end-devices. In that context, it demonstrates a novel architecture for flexible, secure and low-power network-based RISC-V processor. It is based on a multi-layer data tracing approach (network, execution and hardware) to detect ongoing logical attacks using the network as an entry point.

SDR architectures related work

This table presents a comparison of IoT SDR baseband processor architectures and their features:

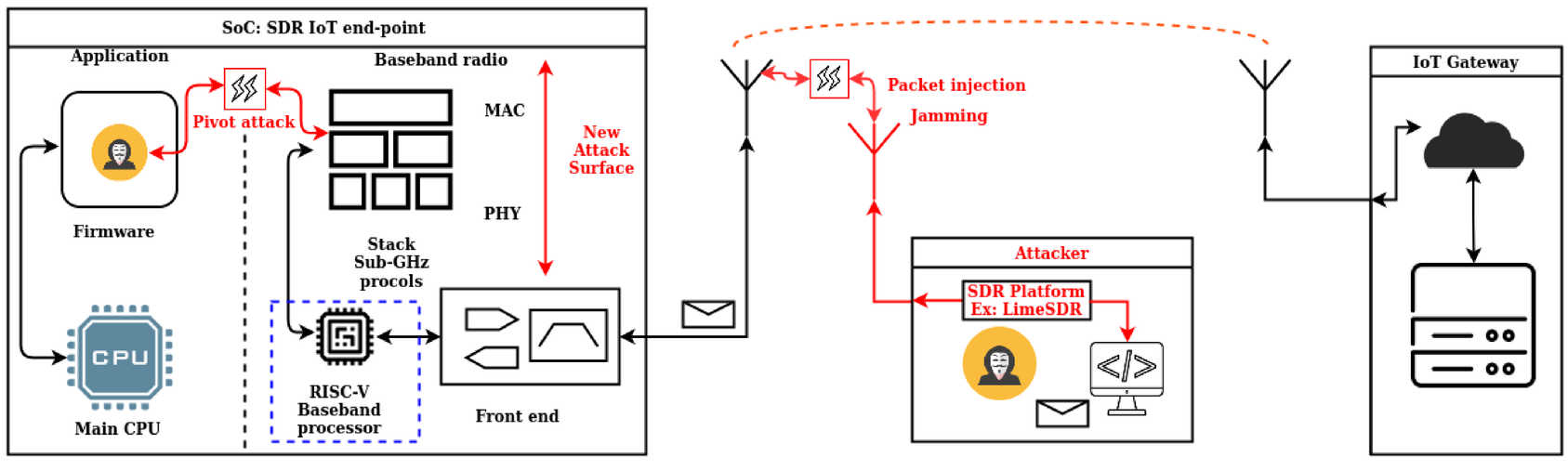
Architecture	FPGA [1]	CPU (dedicated) [2]	CPU (Generic) [3]	Cortex M0+
Multi-Protocol	✗	✗	✗	✗
Programmability	+	+	+++	+++
Security	✗	✗	✗	✓
Flexibility	+++	+	++	++
Dynamic power	$\sim 100mW$	$\sim 10mW$	$\sim 10\mu W$	$\sim 10\mu W$

State of the art regarding security

- The emergence of low-cost high-performance platforms and associated software allows attackers to access lower layers of networks [4]
- 33 vulnerabilities in TCP/IP stacks allow to perform code execution, DoS, and data ex-filtration [5]
- Exploitation of buffer overflow vulnerabilities to perform DoS attacks and remote execution of malware on the target [6]

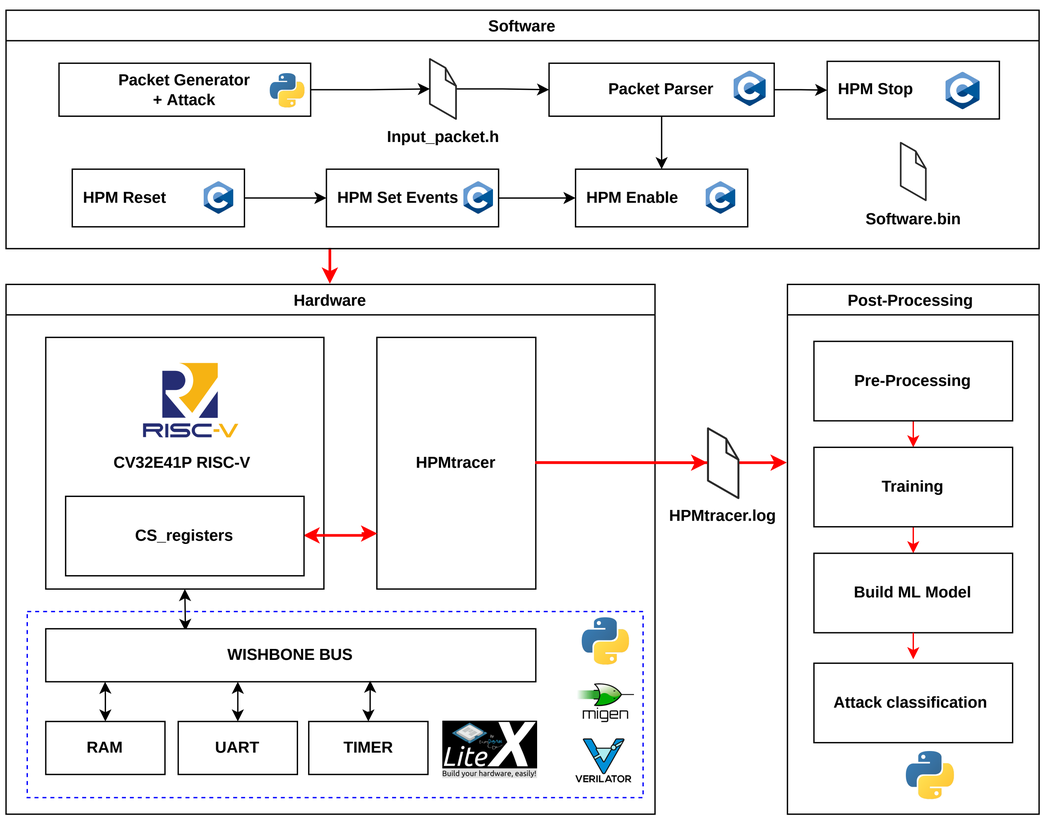
Potential threat models

- Jamming Attack ✓
- Logical Attacks: Packet Injection, . . . ✓
- Physical Attacks ✗



Test-bed

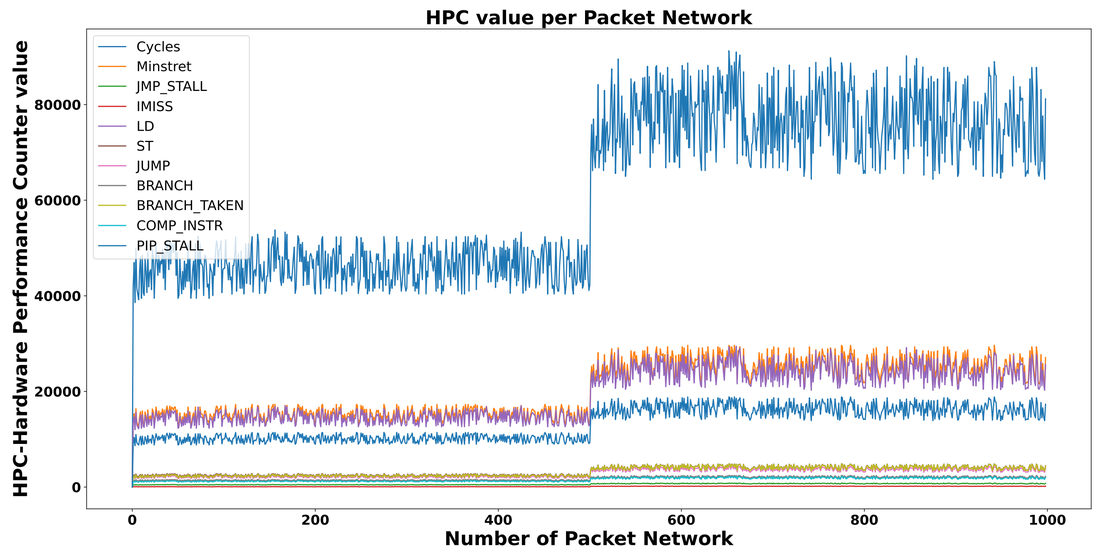
This block diagram demonstrates our test bed for evaluating the multi-layer data tracer:



The attack is exploiting CVE-2020-11068 with simple buffer overflow in parser firmware.

Dataset

This graph shows 11 events of hardware performance counter (HPC) values based on 1000 packets (Last 500 of them are subject to a buffer overflow vulnerability).



Classification Comparison

This table shows the evaluation results of the comparison of several classification algorithms.

Method	Accuracy	Precision	Recall	F1 score
Nearest Neighbors	0.998	0.995	1.00	0.998
Linear SVM	0.998	0.995	1.00	0.998
RBF SVM	0.765	1.000	0.550	0.710
Gaussian Process	0.887	1.000	0.785	0.879
Decision Tree	0.998	0.995	1.000	0.998
Random Forest	0.998	0.995	1.000	0.998
Neural Net	0.583	0.977	0.206	0.340
AdaBoost	0.998	0.995	1.000	0.998
Naive Bayes	0.995	0.995	0.995	0.995
QDA	0.995	0.995	0.995	0.995

Conclusion and perspective work

- Inclusion of other metrics for tracing (network, software)
- Implementation of a hardware tracer and co-processor for detection
- Integration to an existing IDS framework

Bibliography

[1] M. Hessar, A. Najafi, V. Iyer u. a., “TinySDR : Low-Power SDR Platform for Over-the-Air Programmable IoT Testbeds,” *Proc. of NSDI*, 2020.
[2] Y. Chen, S. Lu, H. S. Kim u. a., “A low power software-defined-radio baseband processor for the Internet of Things,” *Proceedings - International Symposium on High-Performance Computer Architecture*, Jg. 2016-April, S. 40–51, 2016, ISSN: 15300897. DOI: 10.1109/HPCA.2016.7446052.
[3] H. Belhadj Amor, C. Bernier und Z. Prikryl, “A RISC-V ISA Extension for Ultra-Low Power IoT Wireless Signal Processing,” *IEEE Transactions on Computers*, 2021, ISSN: 15579956. DOI: 10.1109/TC.2021.3063027.
[4] L. Microsystems, *LimeSDR mini*, https://limemicro.com/, [Online; accessed 06-June-2021], 2017.
[5] F. R. Labs, *AMNESIA:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices*, https://www.forescout.com/research-labs/amnesia33/, [Online; accessed 06-June-2021], 2020.
[6] S. D. Hitefield, M. Fowler und T. C. Clancy, “Exploiting Buffer Overflow Vulnerabilities in Software Defined Radios,” *IEEE 2018*, S. 1921–1927, 2018. DOI: 10.1109/Cybermatics_2018.2018.00318.