Snout, an IoT Pentesting-Tool

John Mikulskis, Johannes K Becker,
Stefan Gvozdenovic, and David Starobinski

Boston University

BOSTON UNIVERSITY

Objectives

- Create a SDR Pentesting tool that focuses on IoT devices
- Create an extensible and open-source tool that benefits the security community

Functionality

Device Enumeration: Snout can passively monitor wireless communication and enumerate devices, or actively query devices for information.

Vulnerability Assessment: Different vulnerabilities can be detected by listening to ongoing communication (passively) or by triggering vulnerable processes (actively). Snout can also find specific vendor, OS, and protocol versions.

Advanced Packet Replay: Snout can replay received packets as-is or with specific modifications, such as dynamic sequence number increments or other packet modifications, making it a useful tool for replay vulnerability detection.

Packet Fuzzing: Snout allows the user to configure smart fuzzing on *both* the preamble and the body of packets, enabling a large range of use cases around physical layer fuzzing.

Contributions

- An open-source IoT pen-testing tool (Snout) capable of communicating with a variety of non-IP based wireless devices.
- A collection of open-source software architecture that enables Snout.
- Device enumeration capabilities of Snout for two major wireless IoT protocols (Bluetooth LE and Zigbee) that can be used both interactively and through automated tasks.
- Passive and active detection of a recent Zigbee vulnerability.

Snout Setup

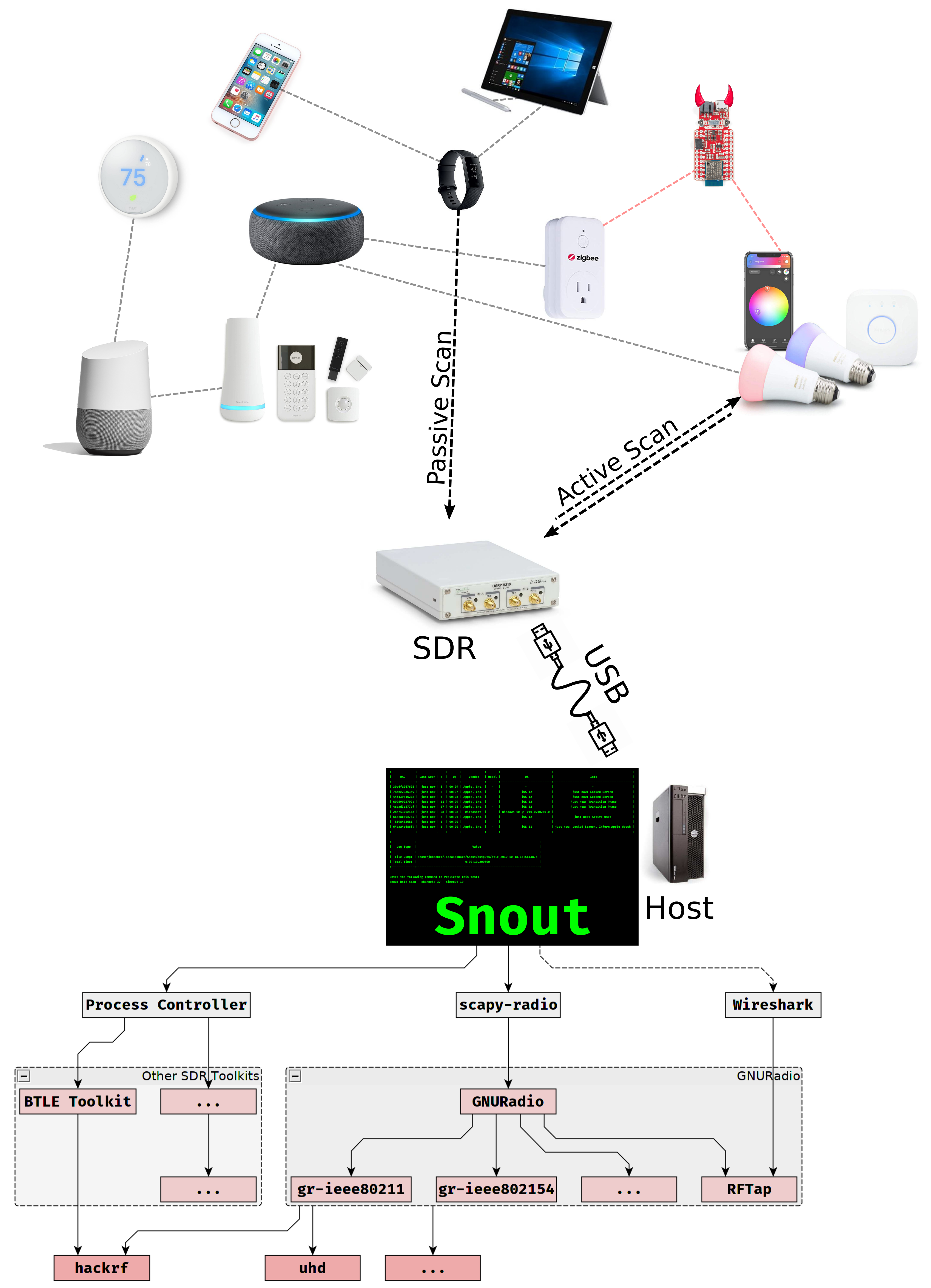

Figure 1:Snout makes use of SDR hardware to passively or actively interact with IoT devices.

Usage

```
Usage: snout [OPTIONS] [[zwave|zigbee|wifi|btle]] COMMAND [ARGS]...

  Welcome to Snout!

  This application is designed to provide a powerful and accessible scanning tool for IoT devices with the
  use of Software Defined Radios.

Options:
  -auto, --automatic TEXT  List of commands to automatically enter. The program generates this
  -c, --channels TEXT      Specify the channels. Int (11), inclusive range (11:26), list ([11,12,13]), or
                           all (all)
  -d, --display            Display the results interactively in the terminal after the scan
  -h, --hardware TEXT      Choose a specific hardware to use. This is useful if several SDRs are plugged in
  -f, --filename TEXT      Filename to dump the ouptut to. If not given, a timestamped file in
                           /home/jkbecker/.local/share/Snout/outputs is created
  -w, --wireshark          Open up the test in wireshark
  --help                   Show this message and exit.

Commands:
  scan      Perform a scan operation
  transmit  Perform a transmission operation
```

Components

GNU Radio flowgraphs, such as IEEE 802.11 and 802.15.4 transceivers and RF metadata parsers like RFTap, which can be controlled directly from within Snout.

scapy-radio, which adds GNU Radio compatibility to the packet manipulation library scapy and can be used as an abstraction layer for packet transcoding.

Special-purpose SDR software, such as Xianjun Jiao's BTLE toolkit, which can provide general-purpose controllers and input/output interfaces to low-level processes.

Results

- Zigbee Touchlink vulnerability detection
- BTLE enumeration and passive device property extraction.
- Dockerized variant for ease of use and adaptability.

Additional Information

- Snout is soon to be released on GitHub as open-source
- Snout is still in active development
- More protocals are planned to be added to the tool
- The design is extensible and not limited to only gnuradio applications

Acknowledgements

The authors thank Jonathan Pinchera for designing the Snout logo ((•••)). The authors further thank Byoungsul Lee, Christina Chimienti, Mohammed Uddin, Seung Hee Lee, and Spencer Liu for their 2018-2019 Senior Design Team project "IoT Nmap" at Boston University, which served as an early prototype of Snout.
This research was supported in part by NSF grant CNS-1409053.

Contact Information

- Web: https://snout.tools/
- Email: {jkulskis,jkbecker}@bu.edu

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 | Alexandria, Virginia