

PASSIVE BLUETOOTH MONITORING IN SCAPY

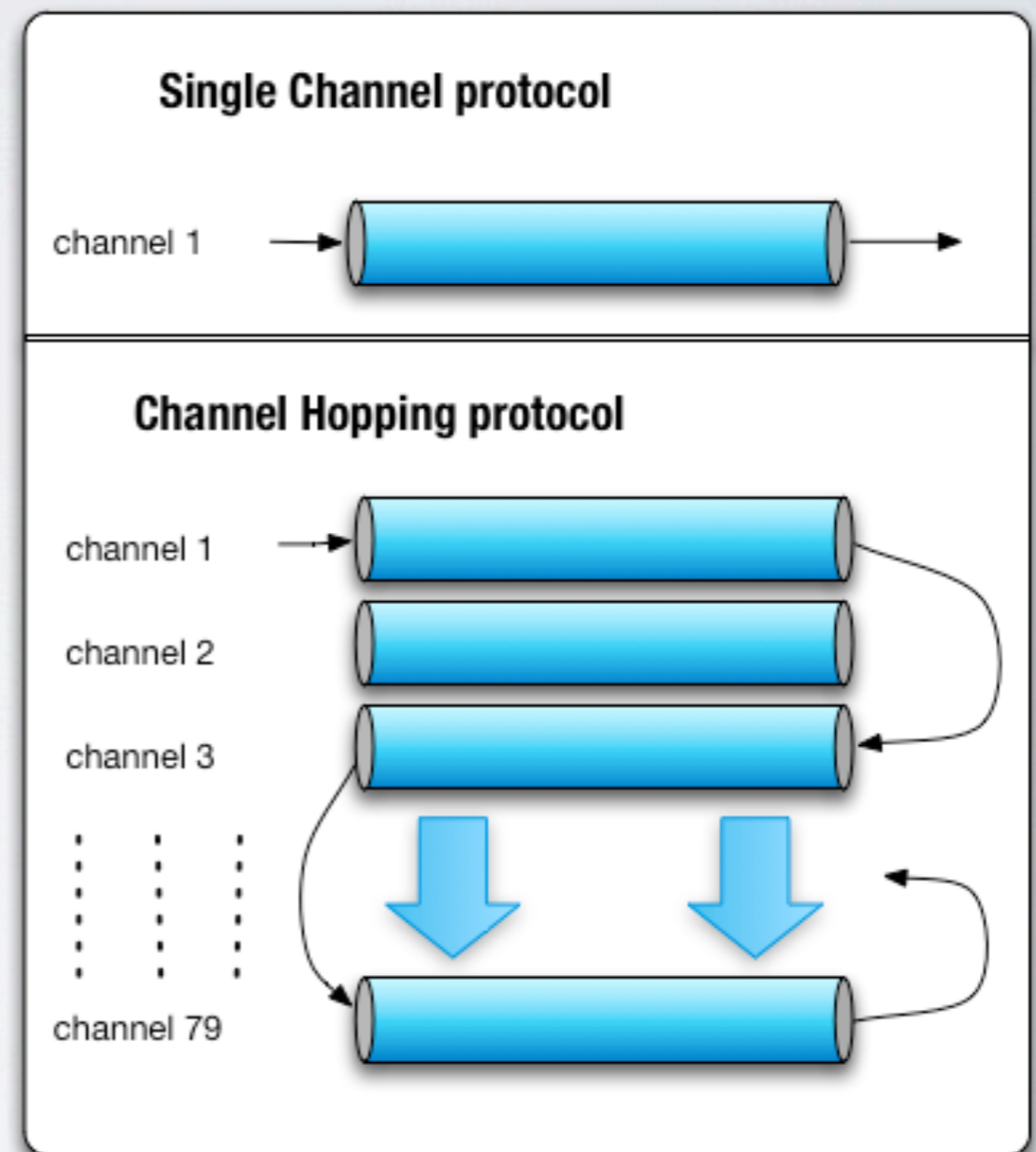
Ryan Holeman

AGENDA

- bluetooth essentials
- fundamental projects
- scapy-btbb project overview
- demo

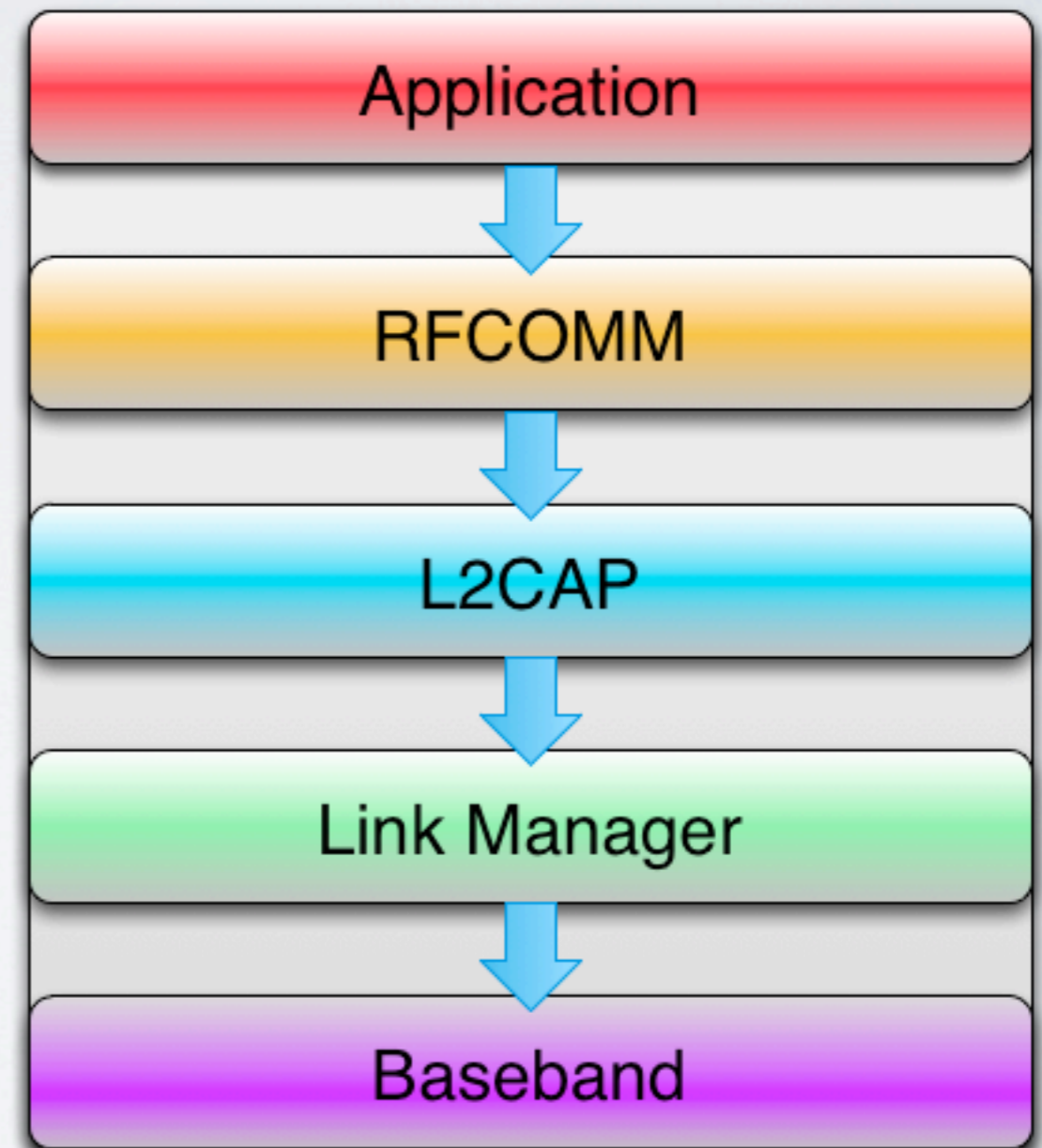
ESSENTIAL BLUETOOTH

- bluetooth is a frequency hopping protocol



ESSENTIAL BLUETOOTH

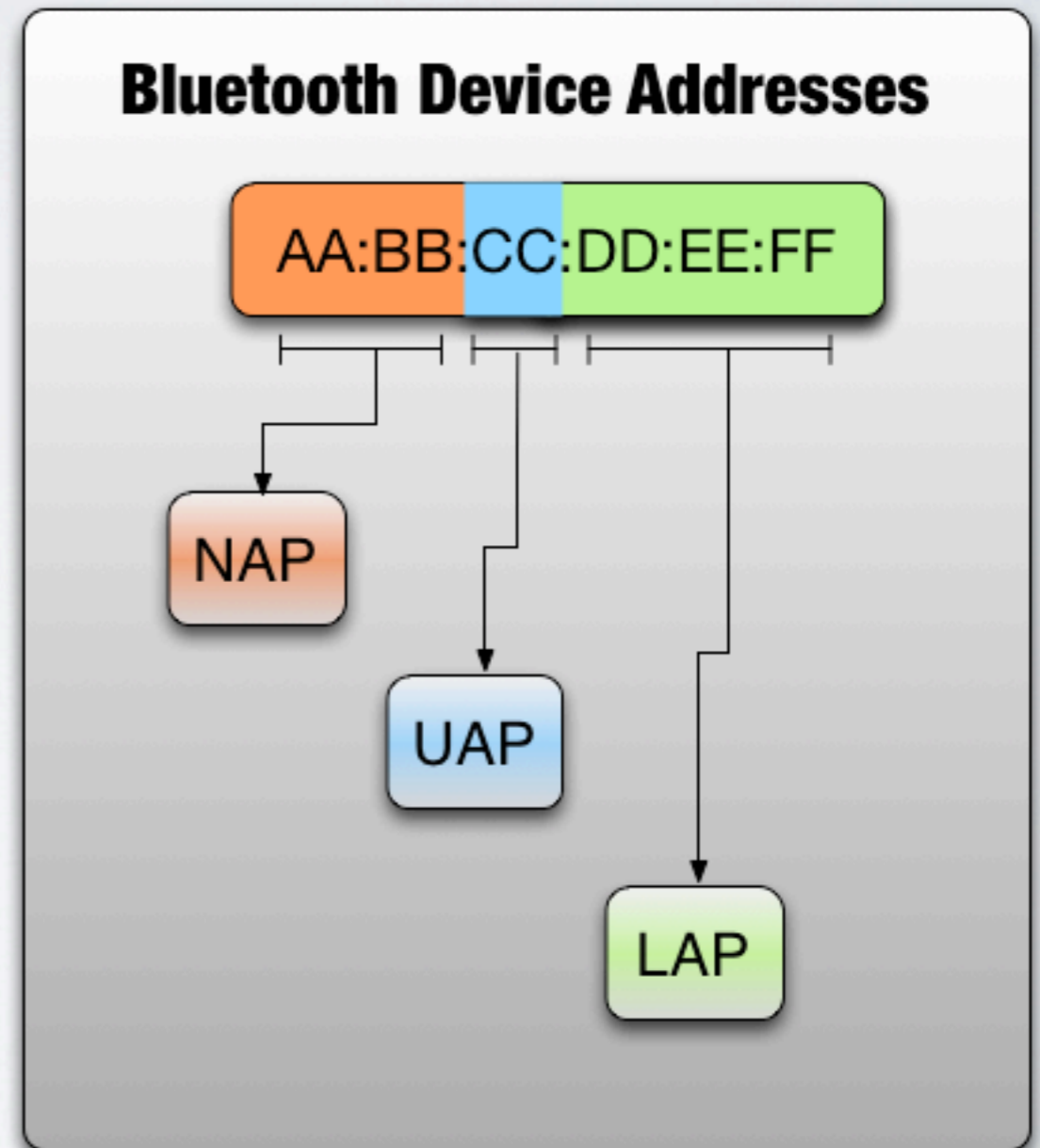
- BTBB - bluetooth baseband
- air traffic between master and slave bluetooth devices



ESSENTIAL

BLUETOOTH

- nap
 - non-significant for communication
 - vendor association
- uap
 - upper address part
 - vendor association
 - calculated from btbb packets
- lap
 - lower address part
 - easily obtained in btbb packet



FUNDAMENTAL PROJECTS

SCAPY

- Philippe Biondi
- python network analysis and manipulation tool
- supports many protocols and layers
 - Ethernet, Tcp/Ip, 802.11, 802.15.5, etc

FUNDAMENTAL PROJECTS

LIBBTBB

- Dominic Spill and Mike Ossmann
- provides methods for:
 - uap discovery, clock discovery, etc
- wireshark plugin
 - wireshark btbb support

FUNDAMENTAL PROJECTS

UBERTOOTH

- bluetooth baseband sniffer
- Mike Ossmann
- kismet plugin



SCAPY-BTBB

GOALS

- bluetooth baseband traffic in python

SCAPY-BTBB

CONTRIBUTIONS

- btbb layer in scapy
- a stream utility for pcap files in scapy
- btbb helper methods
 - vendor from nap/uap
 - distinct address lists from btbb traffic
- extensive documentation of related projects

SCAPY-BTBB

RELEVANCE

- real time and postmortem data analysis for btbb traffic
- compatibility across hardware
 - though pcap files
- easily incorporated into:
 - developer debugging tools
 - auditing tools
 - exploitation tools

DEMO

REFERENCES

- scapy
 - Phillippe Biondi
 - secdev.org/projects/scapy
- libbtbb
 - Dominic Spill & Mike Ossmann
 - sourceforge.net/projects/libbtbb
- ubertooth
 - Mike Ossmann
 - ubertooth.sourceforge.net
- kismet
 - Mike Kershaw
 - kismetwireless.net
- bluez
 - bluez.org
- pybluez
 - pybluez.googlecode.com
- wireshark
 - wireshark.org
- ipython
 - ipython.org
- pandas
 - pandas.pydata.org

PROJECT HOME AND CONTACT INFO

- project home
 - hackgnar.com/projects/btbb
- contact
 - email: ripper@hackgnar.com
 - twitter: [@hackgnar](https://twitter.com/hackgnar)