PASSIVE BLUETOOTH MONITORING AND ANALYSIS WITH SCAPY AND PANDAS

Ryan Holeman
Twitter: @hackgnar

AGENDA

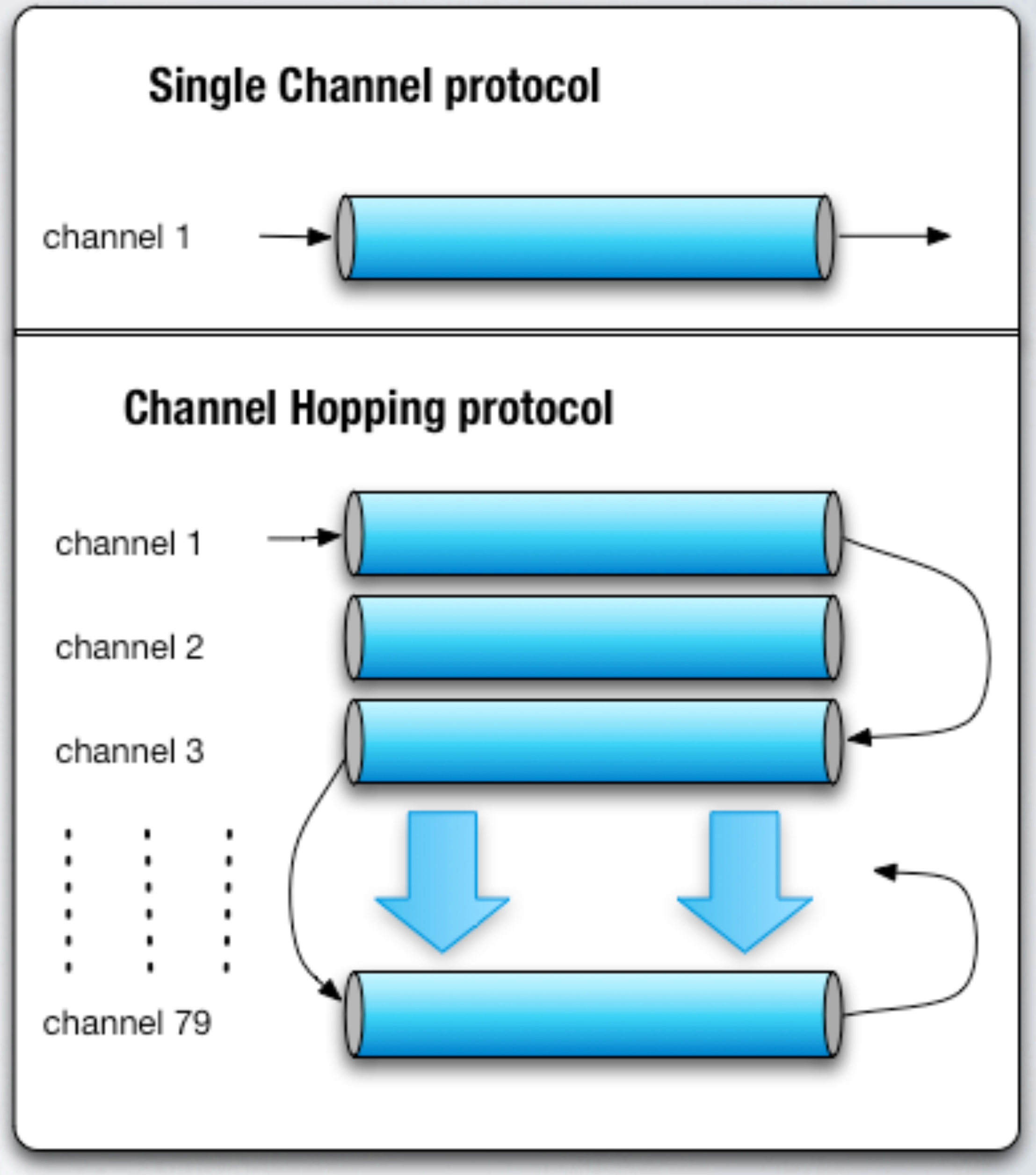
- bluetooth essentials
- fundamental projects
- scapy-btbb layer
- python & ubertooth
- demos

ESSENTIAL

BLUETOOTH

Text

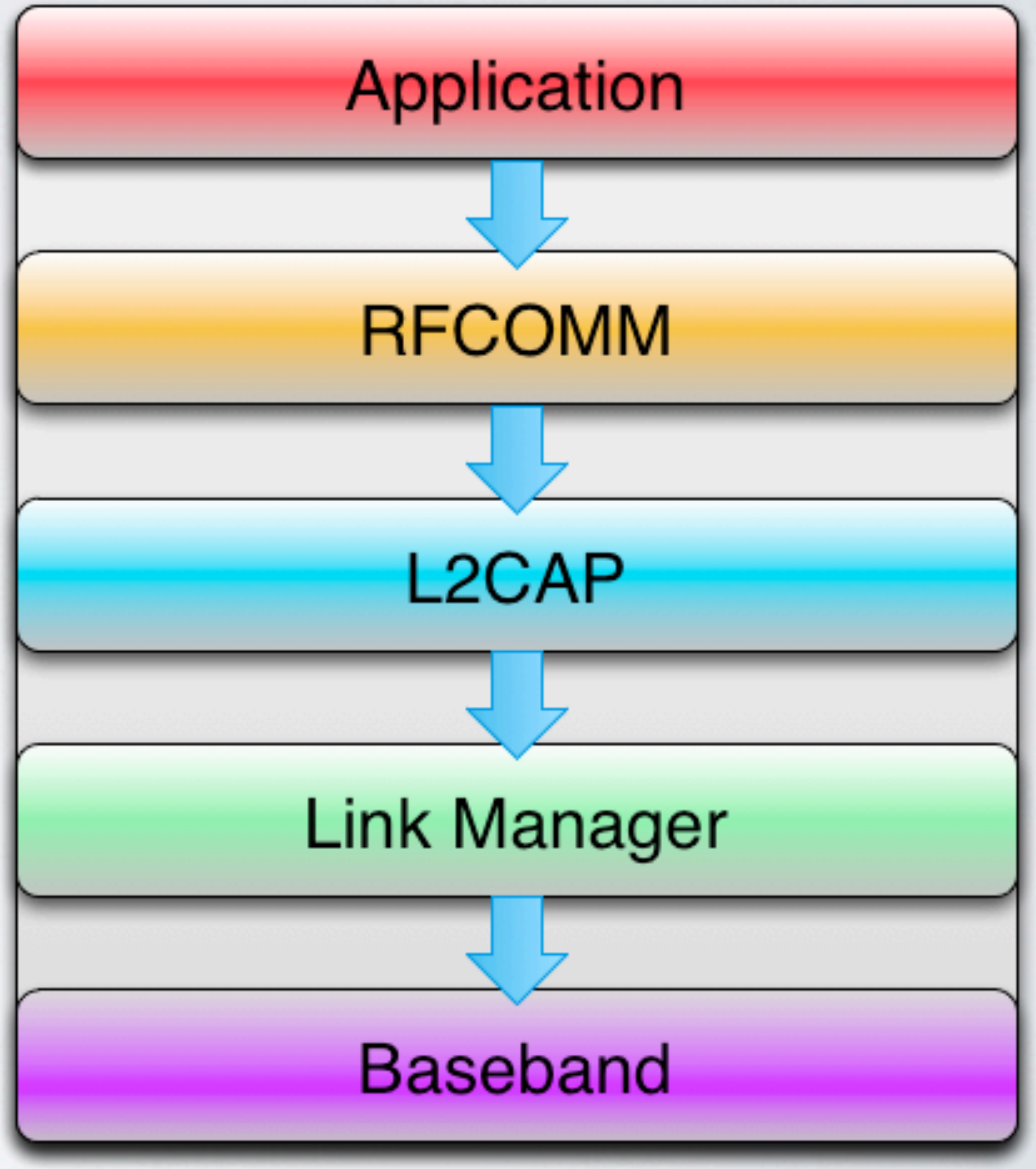
- bluetooth is a frequency hopping protocol



ESSENTIAL

BLUETOOTH

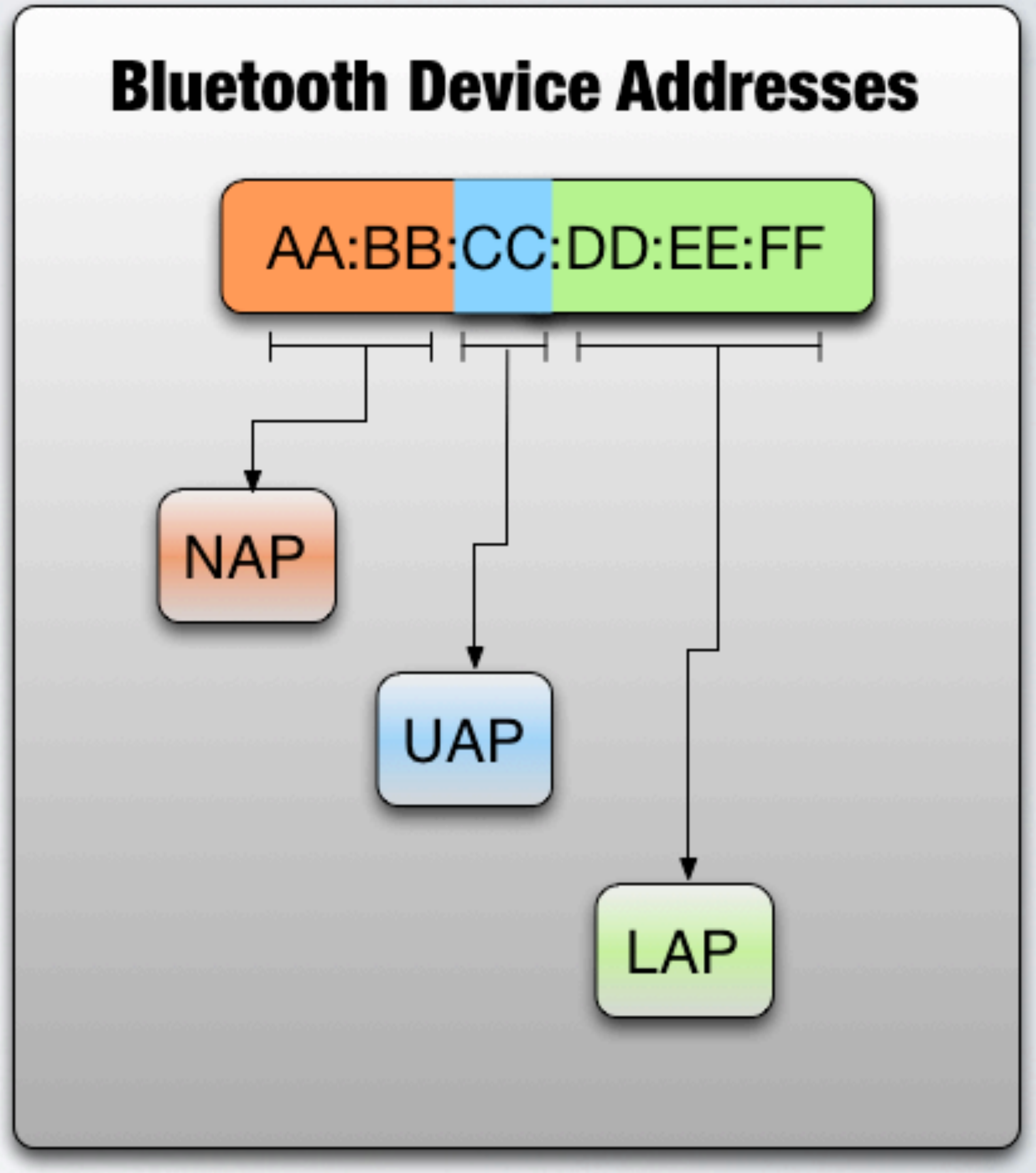
- BTBB - bluetooth baseband
- air traffic between master and slave bluetooth devices
- passive monitoring typically happens at this layer



ESSENTIAL

BLUETOOTH

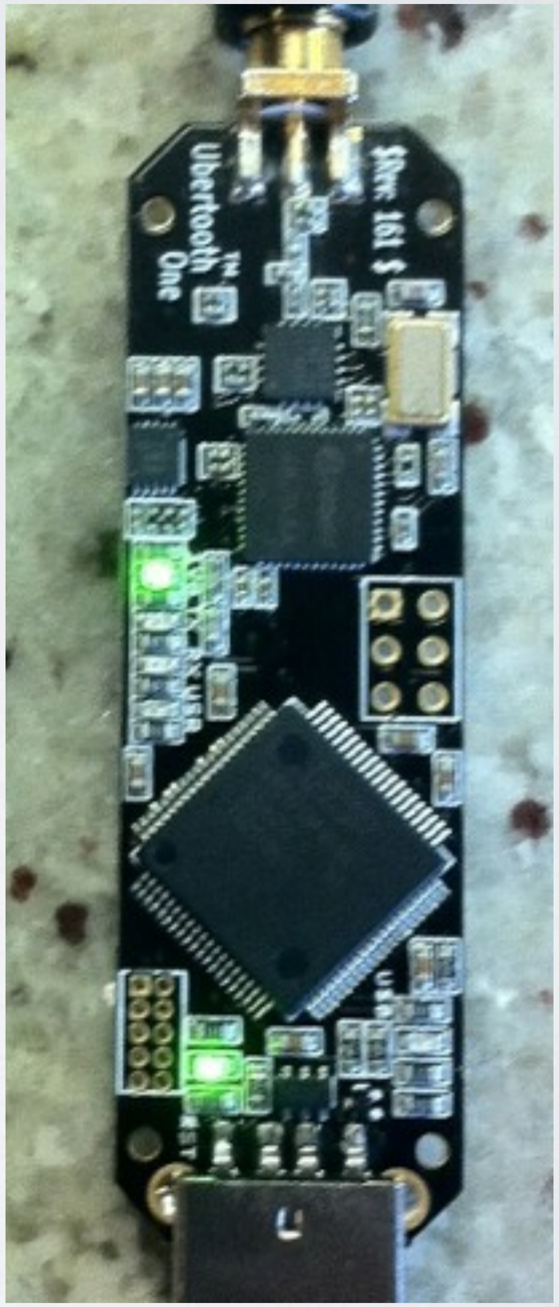
- nap
  - non-significant for communication
  - vendor association
- uap
  - upper address part
  - vendor association
  - calculated from btbb packets
- lap
  - lower address part
  - easily obtained in btbb packet



FUNDAMENTAL PROJECTS

UBERTOOTH

- bluetooth baseband hardware
- created by Mike Ossmann
- new lead dev Dominic Spill
- kismet plugin



FUNDAMENTAL PROJECTS

LIBBTBB

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

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

PROJECT

GOALS

- bluetooth baseband traffic in python
- direct python interface for ubertooth

SCAPY-BTBB

CONTRIBUTIONS

- btbb layer in scapy
  - btbb data is loaded via scapy PcapReader
- a scapy pcap stream data structure
  - allows for real time scapy packets via pcap files

SCAPY-BTBB

CONTRIBUTIONS

- btbb helper methods
  - vendor from nap/uap
  - nap reduction from uap
  - distinct address lists from btbb traffic
  - packet meta data lookup
  - packet type summary

- documentation of related projects

PYTHON & UBERTOOTH

CONTRIBUTIONS

- direct ubertooth interface
  - ability to control ubertooth via pure python

- libubertooth compatible data dumps
  - helpful for pure python ubertooth data

PYTHON & UBERTOOTH

CONTRIBUTIONS

- lap parsing
- simple packet identification
- simple uap identification
- scapy integration

DEMO

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

SCAPY-BTBB

CURRENT & FUTURE WORK

- python ubertooth libs
  - full libbtbb functionality in python
  - full ubertooth functionality in python
- scapy
  - bluetooth low energy layer
  - sane defaults for scapy btbb packet building
- bluetooth database project

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

- updated slides and content:
  - github.com/hackgnar/lockdown_2013
- project home
  - hackgnar.com
- contact
  - email: ryan@hackgnar.com
  - twitter: @hackgnar