Why Does my Toolbox Need Its Own Forklift?

“Why isn't one packet sniffer good enough?”

Presented by

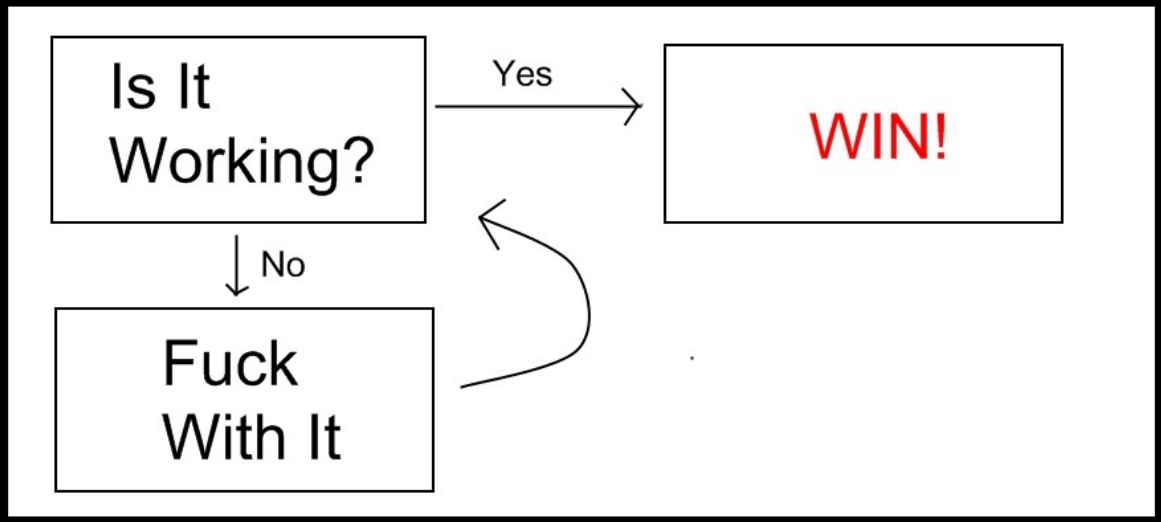
Vyrus of DC949

What is Packet Sniffing Really?

- Almost EVERY tcp/ip sniffer (or at least the ones you and I have used)
  - Uses some form of the PCAP library to sniff data
  - Is not application protocol specific
  - Provides some form of user interface to control what network data is being captured or displayed

- Most network sniffers created to be application specific suffer from
    - False positives or errors in the network traffic detection process
    - Developmental stagnation
    - Security! (yes, even your packet sniffer can be a security risk <_<)

So NOW what!?



TROUBLESHOOTING

This is all I do, and people think I'm an expert.

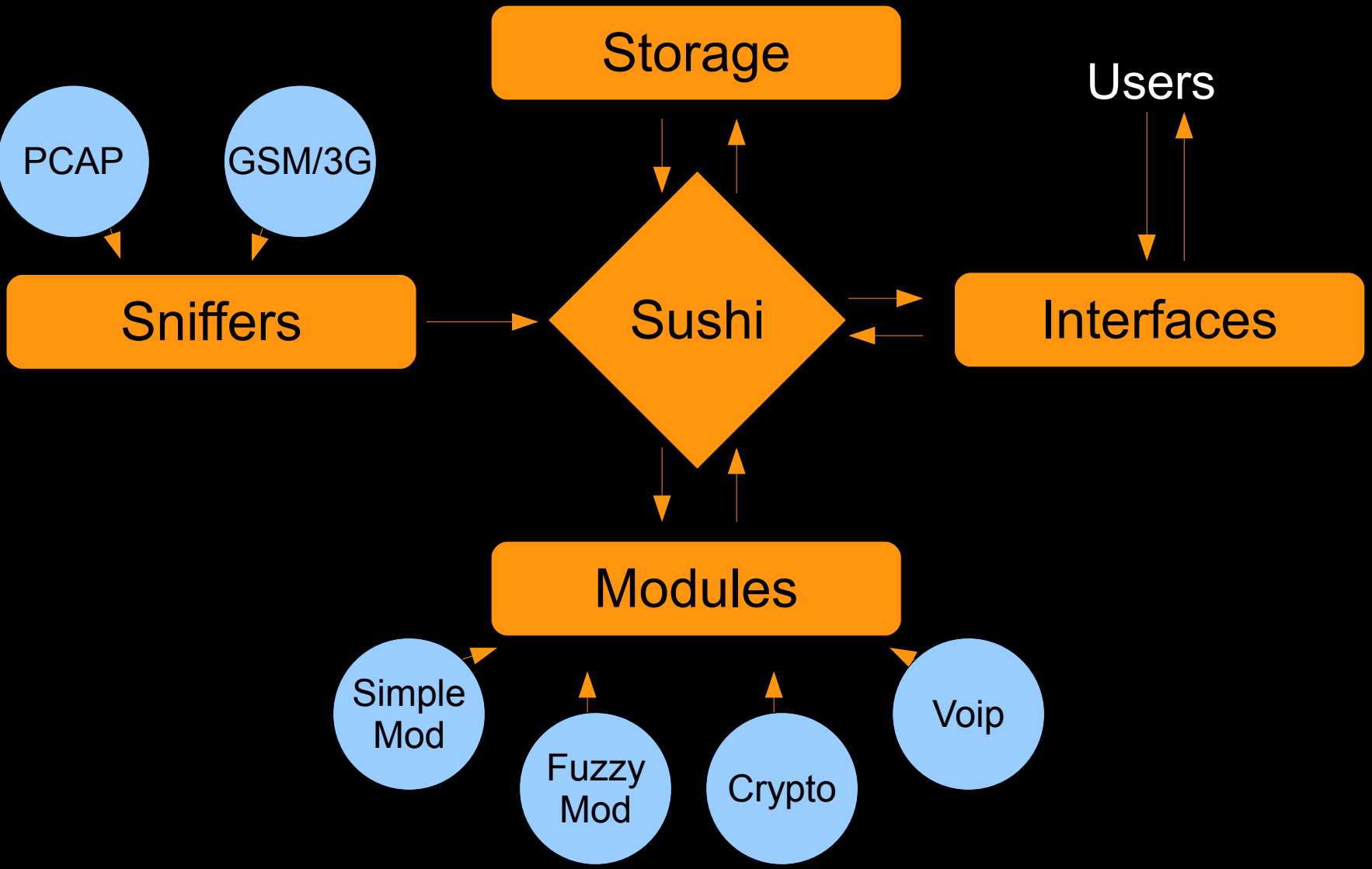
Sushi

Yea... its THAT cool ;)

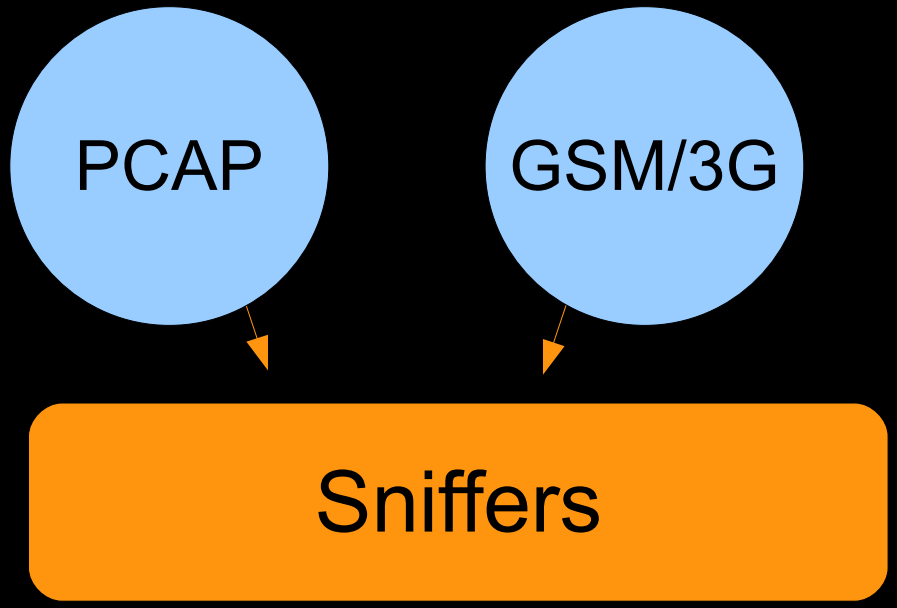
Sushi, the Modular Sniffing Framework

Sushi is my attempt to solve the problem!

Sushi: A Closer Look



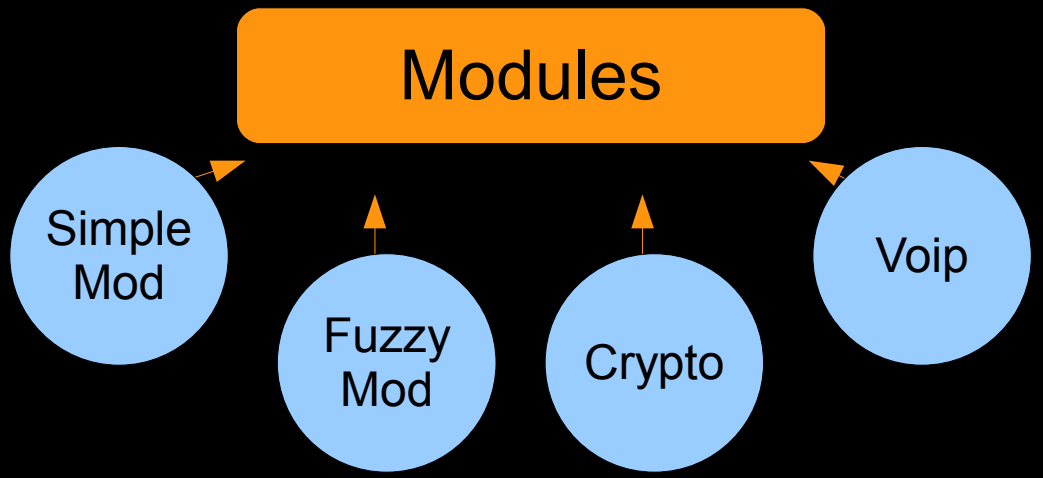
Sushi::Sniffers



- Sniffer Queue
  - PCAP
  - Memory: RAM,hard drive,test clip
  - Bluetooth
  - Signal: oscilliscope/anolog on unit data, geiger counter, audio device (dsp, mic)
  - Robots: servos, sensors, etc
  - Video: camera, monitor
  - Radio:CDMA/3G,FRS,TV,HD, AM,FM
  - Satelites

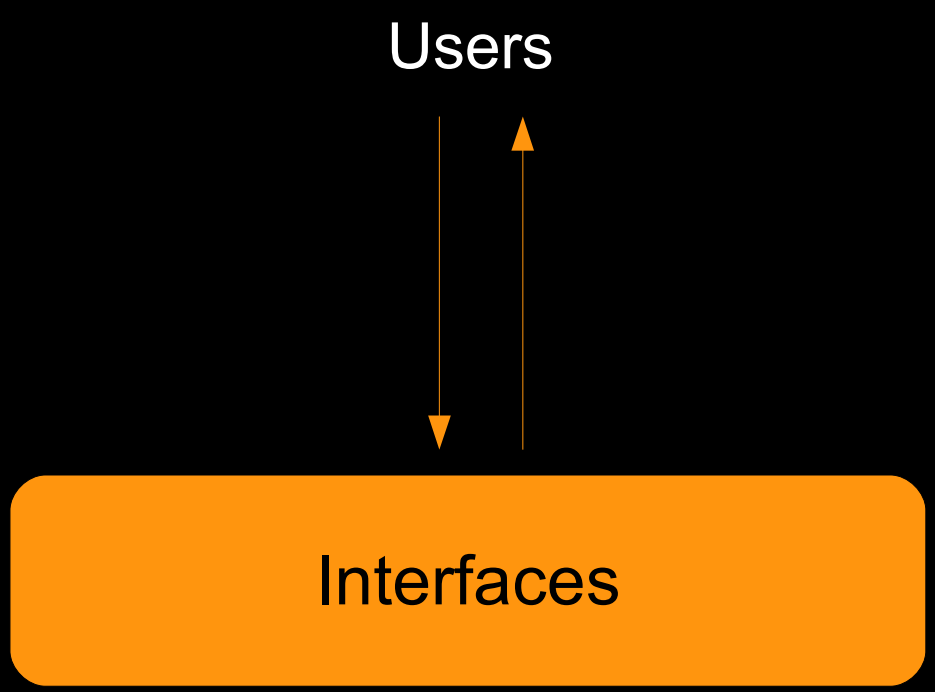
Sushi::Modules

- Module Queue
  - SimpleMod - The inspirational dream module
  - FuzzyMod - The original "AI" characterization/decode/simplemod rule writer
  - Cryptonomicron - Encryption/Encoding SECRET DECODER RING
  - etc...



Sushi::Modules

- Interface Queue
  - Local or Remote
  - raw output (for simple use or shell scripting)
  - Ncurses
  - X-gui
  - etc...



Sushi::Storage

- Storage Specification Initial
  - Mapping of "sniffer sources" (like 'pcap', 'pcap-eth1', 'pcap-eth1-vyrusbox', etc)
  - Mapping of "interface buffers" (like 'ncurses', 'mysql', 'mysql-localhost', '*sql*', etc)
  - Mapping for modules

Questions?

Contact

- CP@dc949.org
- merlin@dc949.org
- vyrus@dc949.org
- http://dc949.org/
- irc://irc.efnet.net/dc-949