SEWiFi

Building a Security Enhanced USB WiFi Dongle

Ryan Holeman

Who am I?

- Security Researcher at Ziften Technologies
- Frequent conference speaker
- Father, skater, hacker

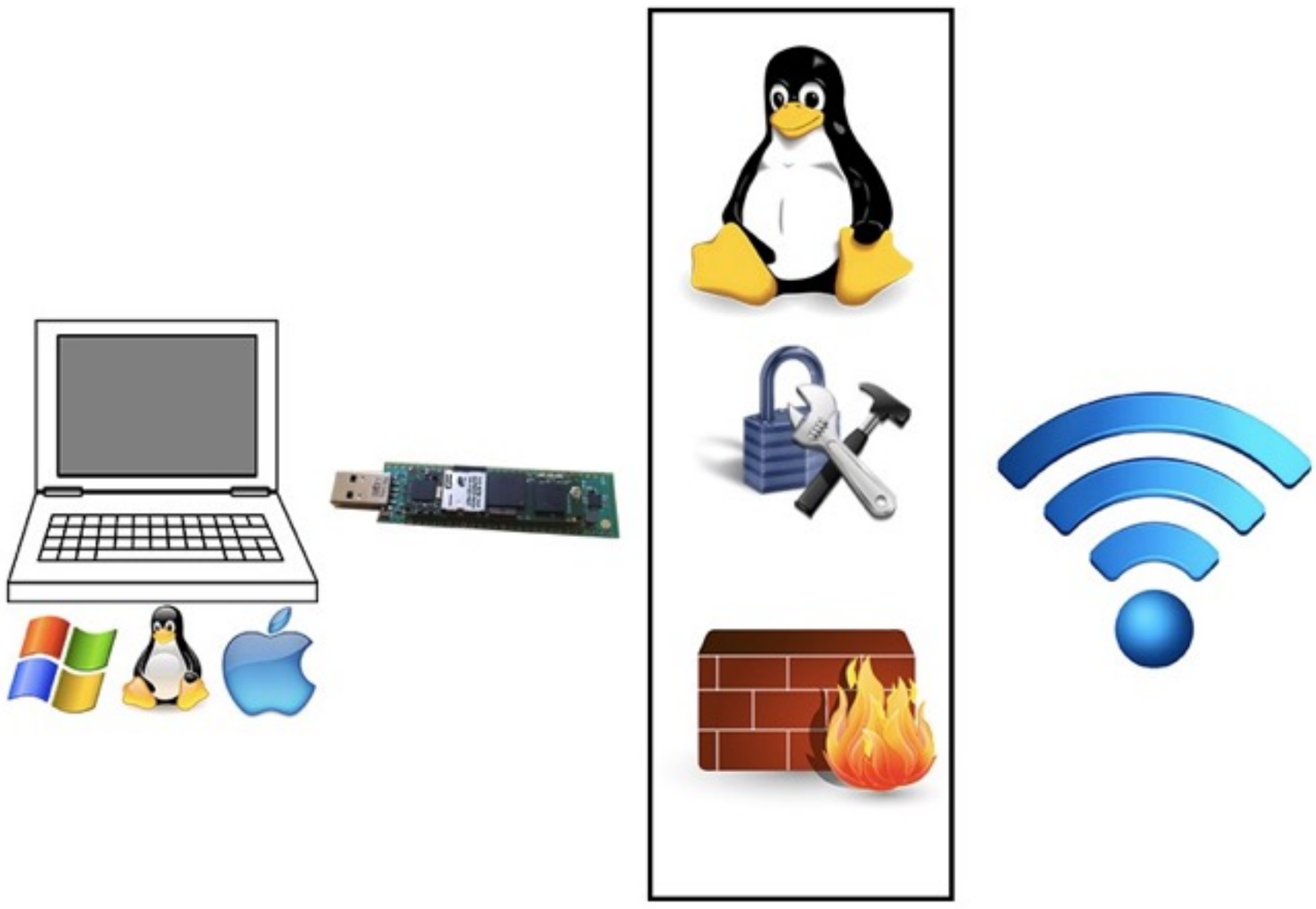
Problem

- Most networks are typically insecure.
- Everyday users are unaware of:
  - Common security practices
  - Setup & use of security tools
- Proper security procedures take time to setup and differ across operating systems

Goals

- Provide a **seamless** security stack in a device which is familiar to all users
    - plug in a USB device and it works
- Must be cross platform
- Small & affordable

Architecture

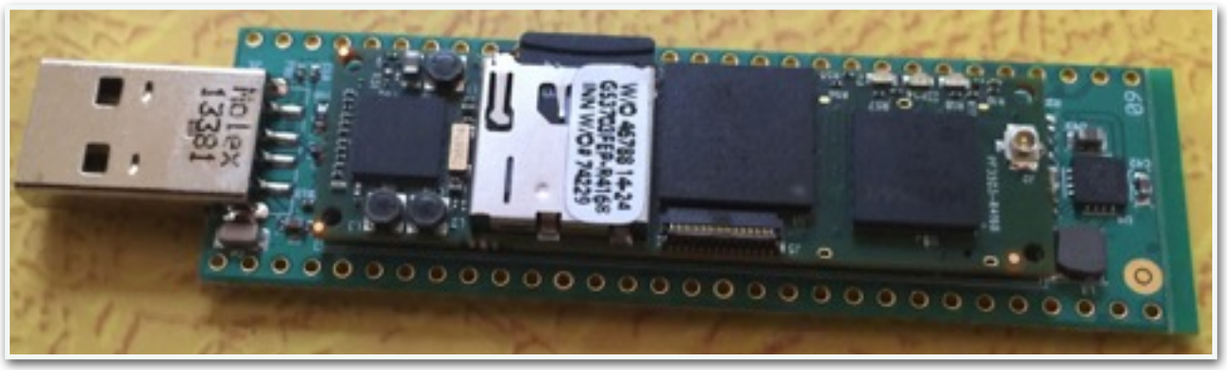


Hardware

- Requirements:
  - WiFi, CPU, USB, size
- Possible alternatives were:
  - Beagle Bone Black
  - Raspberry pi
  - Rooted phone
  - Other low resource SoHo routers

Rev One Hardware

- Gumstix Overo IronSTORM-P COM
  - ARM Cortex A8 1GHz 512 RAM & NAND
  - Thumbo USB daughter board
  - Not fully open source



Rev One Software

- OS
  - Debian Wheezy w/ sewifi bundle deb package.
- IDS/IPS
  - BRO-IDS - Stock configuration rev 1.
- Firewall
  - IPTABLES - NAT and block rules.
- Others
  - Openvpn & various network and recon tools

Build Your Own Rev One

- Gumstix
  - Iron/Fire/Air Overo Storm-P board
  - Thumbo or other USB daughter board
- Docs
  - Build or download a precompiled SEWiFi image
    - github.com/hackgnar/gumstix-overo-images
  - Alternative install on base Armel Debian Image
    - github.com/hackgnar/sewifi

Rev One Current State

- Is it rev #1 usable?
    - Yes, if you are a Linux savvy individual.
- Is rev #1 easy to use for everyday users?
    - Probably not
- Rev #1 security Stack?
    - First iteration. Bro, IPTables, OpenVPN, random tools
- Rev #1 hardware?
    - Gumstix/Thumbo.
- Rev #1 affordability?
    - ~$200.

Rev Two Milestones

- Seamless
    - usb gadget wifi driver
    - web config & captive portal
- Hardware
    - Rev #2 is an Intel Edison \w custom daughter board
    - Drops price point to sub $100 range.
- Security stack changes:
    - Add: alt IDSs, DNSSec, Tor, https proxy, alt VPNs, etc
    - IDS config changes, IDS actions, dynamic firewall.
- Tidy up the base configuration
- Possible cross hardware support

The End

- Questions?
- Contact
  - @hackgnar or ryan@hackgnar.com
- More info:
  - github.com/hackgnar or hackgnar.com