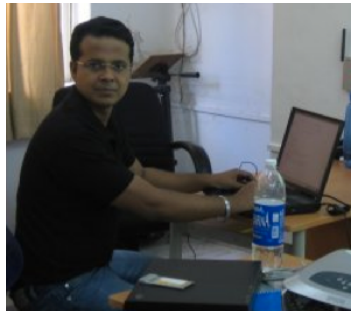
APAD: An EDR Grade Agent for Wi-Fi APs

Vivek Ramachandran

www.PentesterAcademy.com

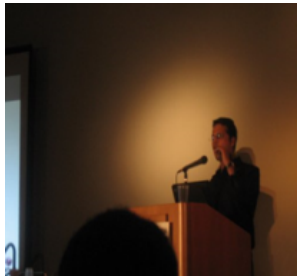
Vivek Ramachandran

B.Tech, ECE
IIT Guwahati



802.1x, Cat65k
Cisco Systems

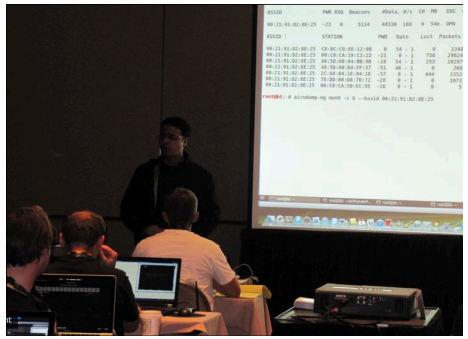
WEP Cloaking
Defcon 19



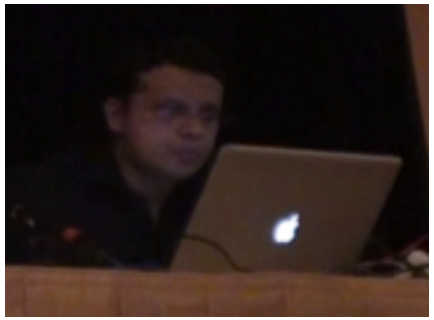
Caffe Latte Attack
Toorcon 9

Media Coverage
CBS5, BBC

Microsoft
Security Shootout



Trainer, 2011



Researcher

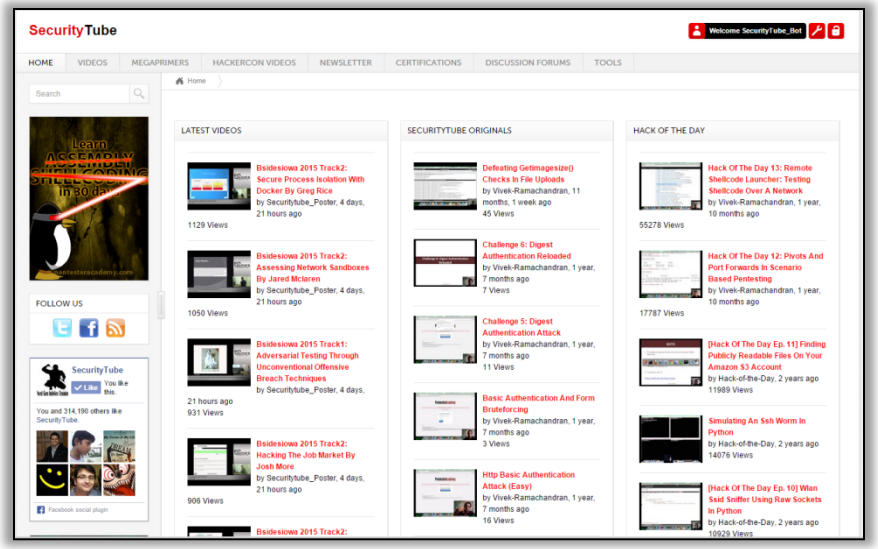
Security Research/ Trainer at Hacker Cons

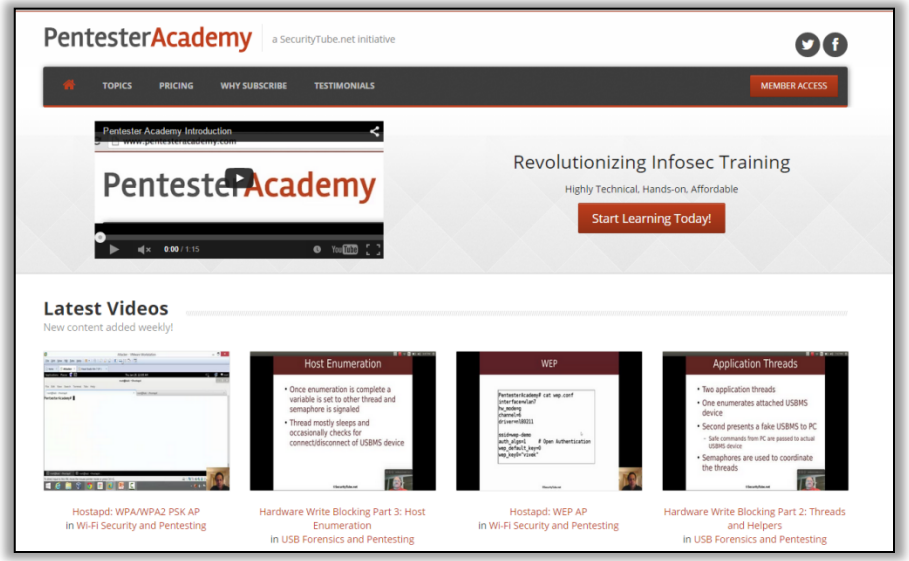
HACKTIVITY

Kelet-Közép-Európa legnagyobb hackerkonferenciája

2011. szeptember 17-18.

SecurityTube and Pentester Academy





AttackDefense Labs

https://attackdefense.com/challengedetails?cid=1243

ATTACK DEFENSE

- Dashboard
- Ongoing Labs 1
- Latest Additions
- Community Labs

EARN CREDENTIALS

- Verifiable Badges

THE BASICS

- Network Recon
- Real World Webapps
- Traffic Analysis
- Webapp CVEs
- Metasploit
- Offensive Python
- Network Pivoting
- Cracking
- Infrastructure Attacks
- Privilege Escalation
- Deliberately Vulnerable
- Forensics
- Firmware Analysis
- Reverse Engineering
- Secure Coding
- IoT

All Section Labs

EDR Demo: MIPS OpenWRT

pa-embedded-iot | Level: Easy | Total Lab Runs: 2 | Running

Lab Link | Stop

Lab Scoreboard

5	1	Mark Complete
# Played on AD	# Played by you	

Mission | Prohibited Activities | Technical Support

In this companion lab, we will be showing a live demo of how low-level kernel based EDR system can be used to detect and deter attacks.

To understand and use this demo, please follow the course.

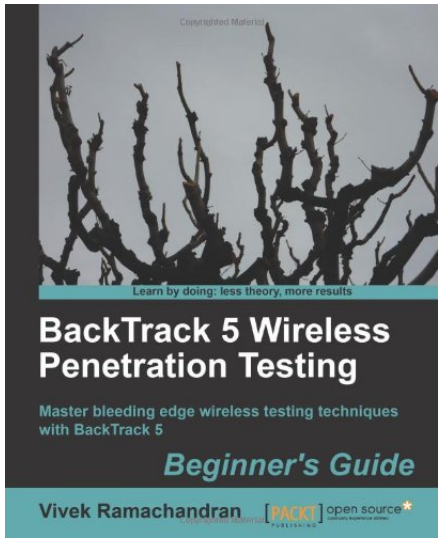
This lab contains build-system for OpenWRT MIPS Malta and Qemu emulator for MIPSEL. The home directory of user john contains the following directories:

- openwrt-buildsystem: OpenWRT build system configured for MIPS Malta
- ready-to-run: Ready to run kernel and filesystem images for MIPS Malta
- rootkit-code: Source code for rootkits

Objective: Compile kernel modules and test those on Qemu emulated MIPS malta machine.

Note: Use of "make clean" in the openwrt-buildsystem will lead to more time consumption during compilation. Similarly, selecting new packages might not work as the lab is not connected to the internet.

Books

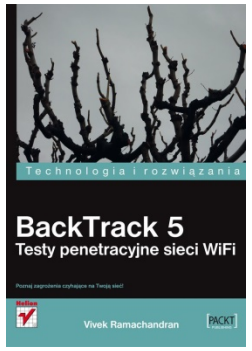


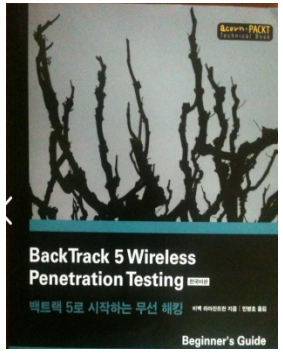
BackTrack 5 Wireless Penetration Testing Beginner's Guide

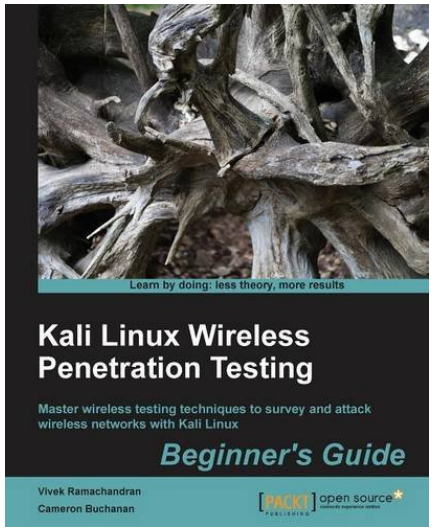
by Vivek Ramachandran (Author)

51 customer reviews

- Sept. 9th 2011
- 13,000+ copies sold
- Polish and Korean translation







Kali Linux: Wireless Penetration Testing Beginner's Guide

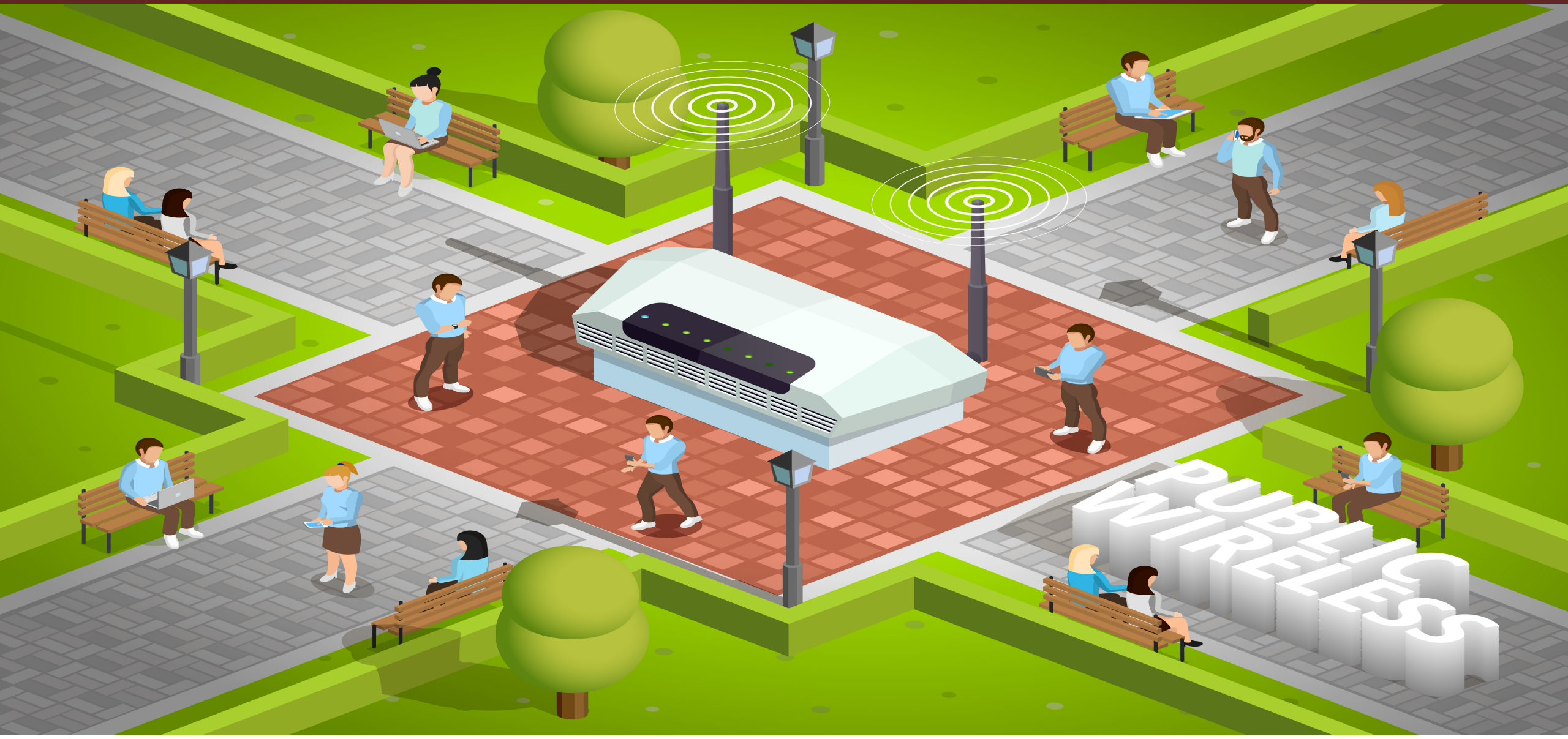
2015

by Vivek Ramachandran (Author), Cameron Buchanan (Author)

35 customer reviews

- March 30th 2015
- Minor Edits for Kali Linux
- New chapter added by co-author

Wi-Fi APs: They are everywhere ☺



Wi-Fi AP: Hackers Live Here!

- Stone age security
- Older kernels, outdated software
- No AV, IDS or any modern security
- No proper logging or alerting

How can good security be built on insecure infrastructure?

What could go wrong?

- DNS Hijacking
- Traffic redirection, monitoring and mangling
- Stealing credentials, accounts, money
- Pivot point to attack other networks
- Propagate spam
- You get arrested … ☹

I have a dream … of secure access points

Can something be done?

Enterprise Grade EDR? Server side DR?

What runs your Wi-Fi AP?

OpenWRT: Popular Distribution

openwrt.org

Register | Log In

OpenWrt
Wireless Freedom

Search | Search

Recent Changes | Media Manager | Sitemap

Welcome to the OpenWrt Project

English (en)

- Welcome to OpenWrt
- Supported Devices
- Packages
- Downloads
- Documentation
- Submitting patches
- Reporting bugs
- Wiki contribution guide
- OpenWrt Forum
- FAQ
- About OpenWrt/LEDE
  - Rules
  - Infrastructure
  - Trademark Policy
- About this site
- Contact Us

start

Welcome to the OpenWrt Project

The OpenWrt Project is a Linux operating system targeting embedded devices. Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management. This frees you from the application selection and configuration provided by the vendor and allows you to customize the device through the use of packages to suit any application. For developers, OpenWrt is the framework to build an application without having to build a complete firmware around it; for users this means the ability for full customization, to use the device in ways never envisioned.

See the Table of Hardware for supported devices. For more information about OpenWrt project organization, see the About OpenWrt pages.

OpenWrt endorses Battlemesh v12

The OpenWrt project supports this year's "Wireless Battle of the Mesh - Building Community Networks for Fun and Non-Profit".

The event aims to bring together people from across the globe who are interested in community networks, including wireless mesh network technologies, fiber infrastructure, Do-It-Yourself Internet Access Providers, and more generally how to create and maintain a thriving community of people involved in building their own networks.

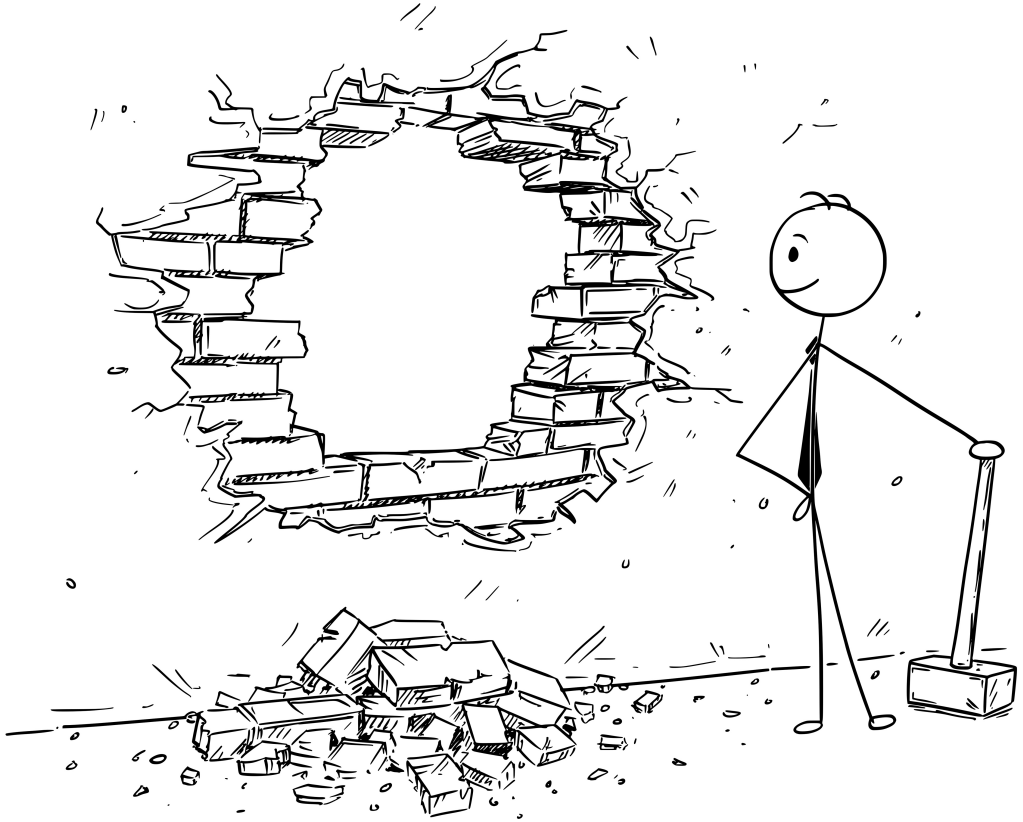
We envision 7 days full of expert presentations, practical workshops, late-night hacking sessions, and fruitful discussions: whether you are a mesh networking enthusiast, community networking activist, protocol developer, or have an interest in networking in general, come and join the event!

Thanks to generous sponsors, the battlemesh is free of charge and open for all, and every year the local organization team strives to keep participation costs low by negotiating deals for accommodation and food.

This year, the event will take place from Monday 8th to Sunday 14th of July, 2019 in Saint-Denis (Paris), France. The event is locally organized. Check out continuously updated information about the event at

https://www.battlemesh.org/BattleMeshV12

Principle of Least Privilege?



[SOLVED] Security Question (all processes runs as root user)

Installing and Using OpenWrt

D [redacted] [redacted]

This would be very hard to change.

LEDE is a full Linux system, so you can set it up as normal with different users (and some daemons, not just dnsmasq do this by default).

But you have to ask yourself exactly what threat you are defending yourself against.

The theory is that if someone breaks one daemon, they have a harder time affecting others if they are run as different users, but the things that run on a LEDE device tend to be fairly locked down (minimizing their vunlerabilities) and rather central to the operation of the system.

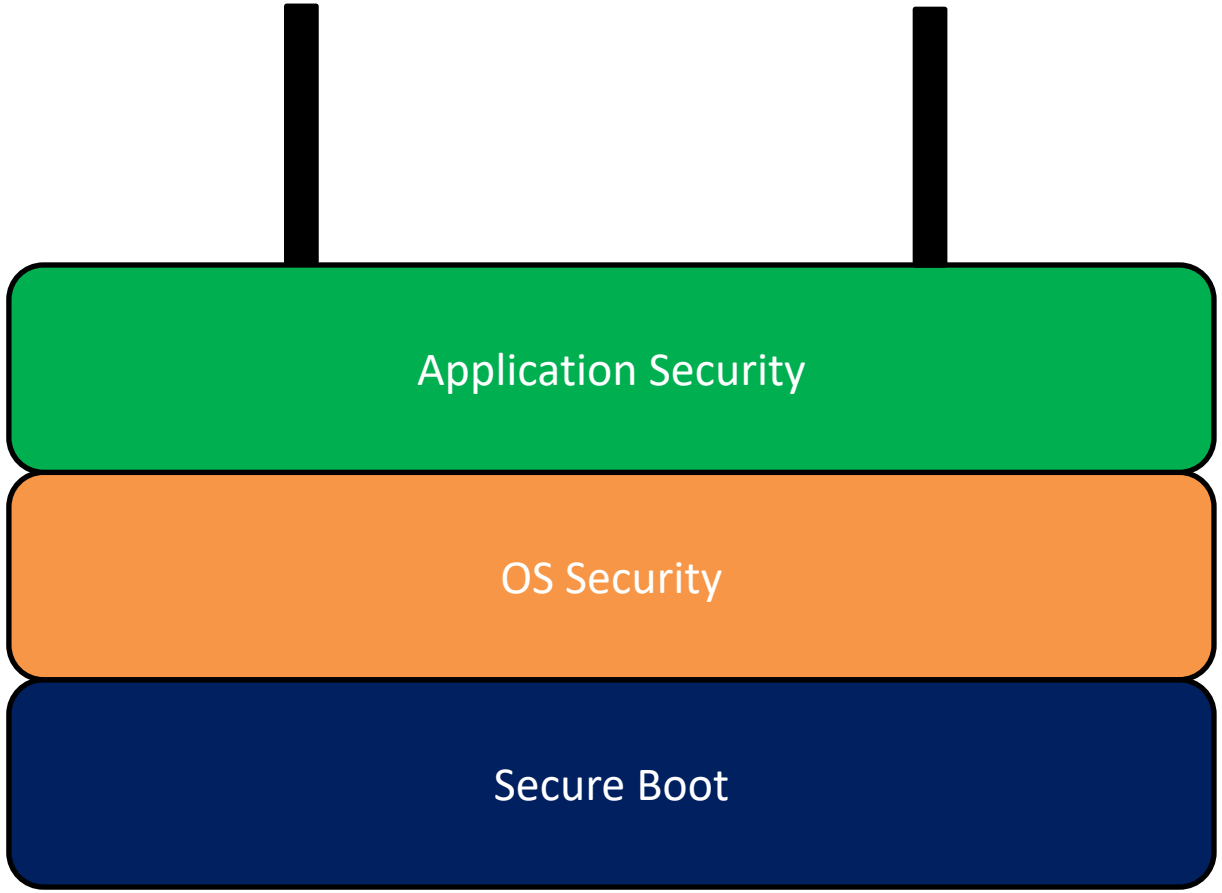
If someone takes over DNS/DHCP (i.e. dnsmask), they can do a lot of nasty things to you, does it really matter that they can't affect the routing tables?

It all depends on what you are running on the router, sometimes it's worth running some things as a different user so that if they get hacked it's harder to affect other things, sometimes it's not worth the effort.

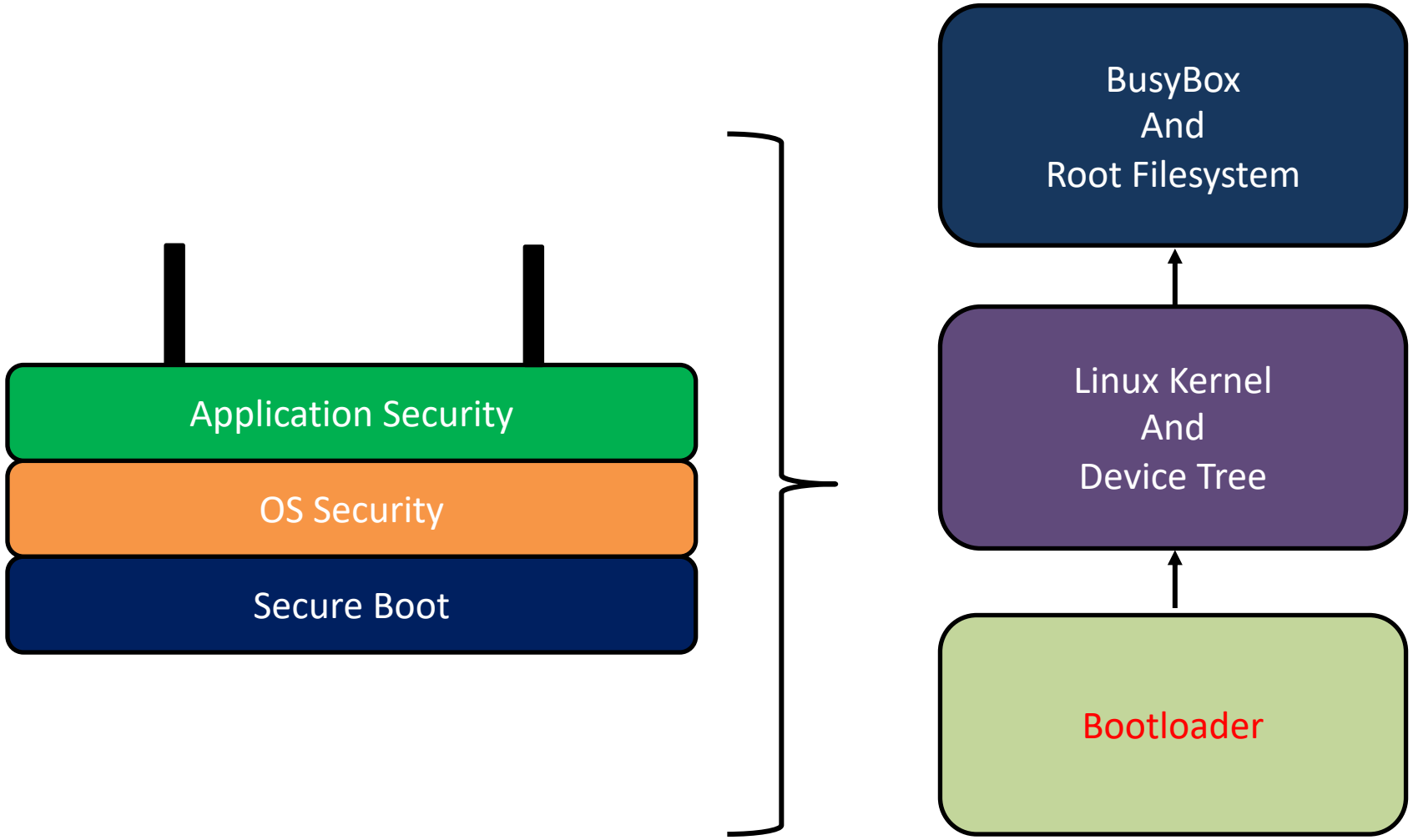
For the LEDE project, the user support complexities of explaining all the possible permission issues to people tip the balance to making the default system not use a lot of userids.

[redacted]

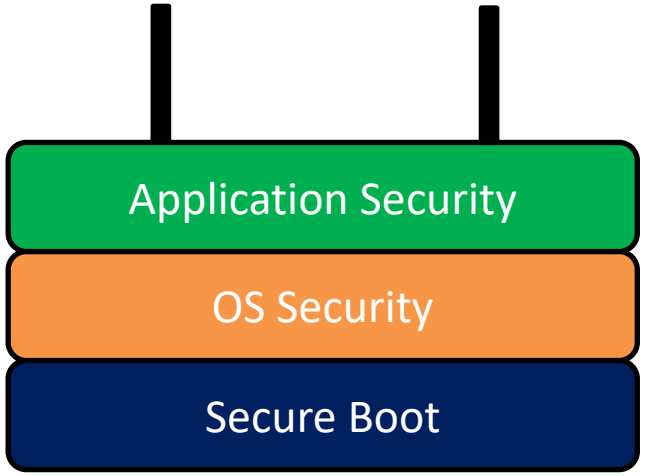
Securing Wi-Fi Routers



Embedded Device Booting

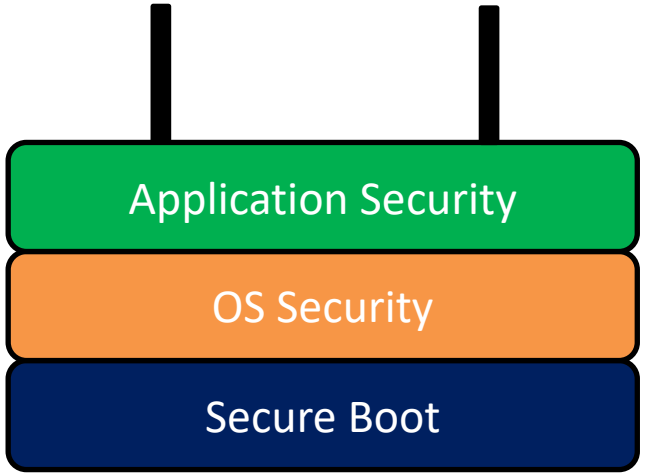


Secure Boot



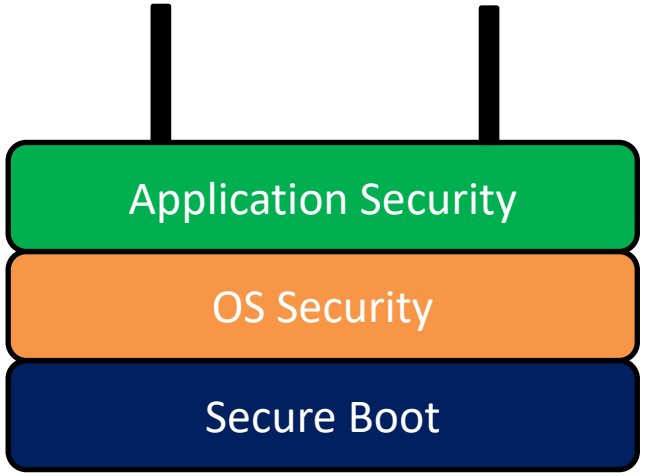
- Chain of Trust
- Trusted Bootloader
- Trusted Kernel
- Trusted FS and Apps

OS Security



- Latest, patched kernel
- Signed modules only
- Kernel mode Attack Detection
- Kernel mode Attack Defense

Application Security



- Multi-user system
- Principle of least privilege
- Use of namespaces, cgroups
- Application isolation

APAD: A Beginning

- Kernel mode component
- Detects attacks and defends when needed
- Writes to system logs
- Logs shipped for remote analysis
- Network wide detection: spatial and time

Demo