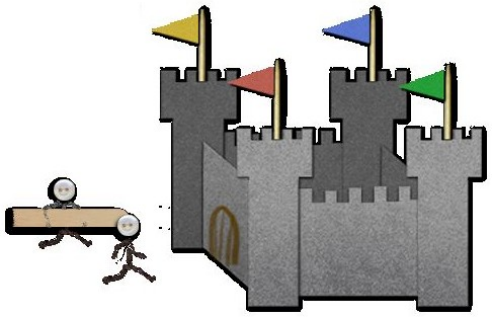


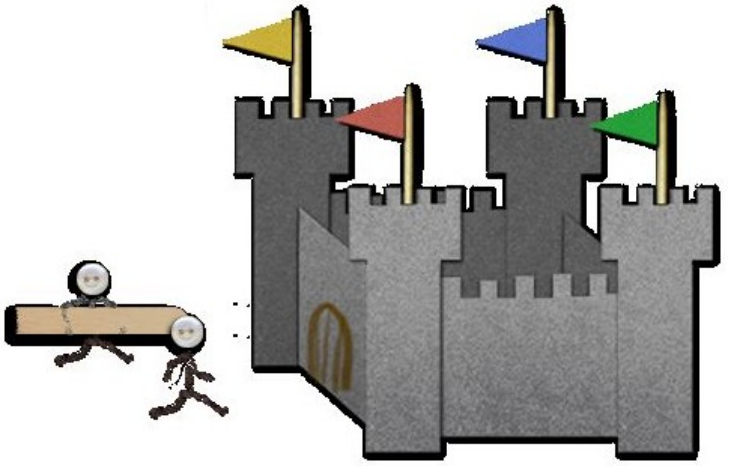
Defending Your Home Network

Alan Baker
San Jose IBM PC Club
March 11, 2019

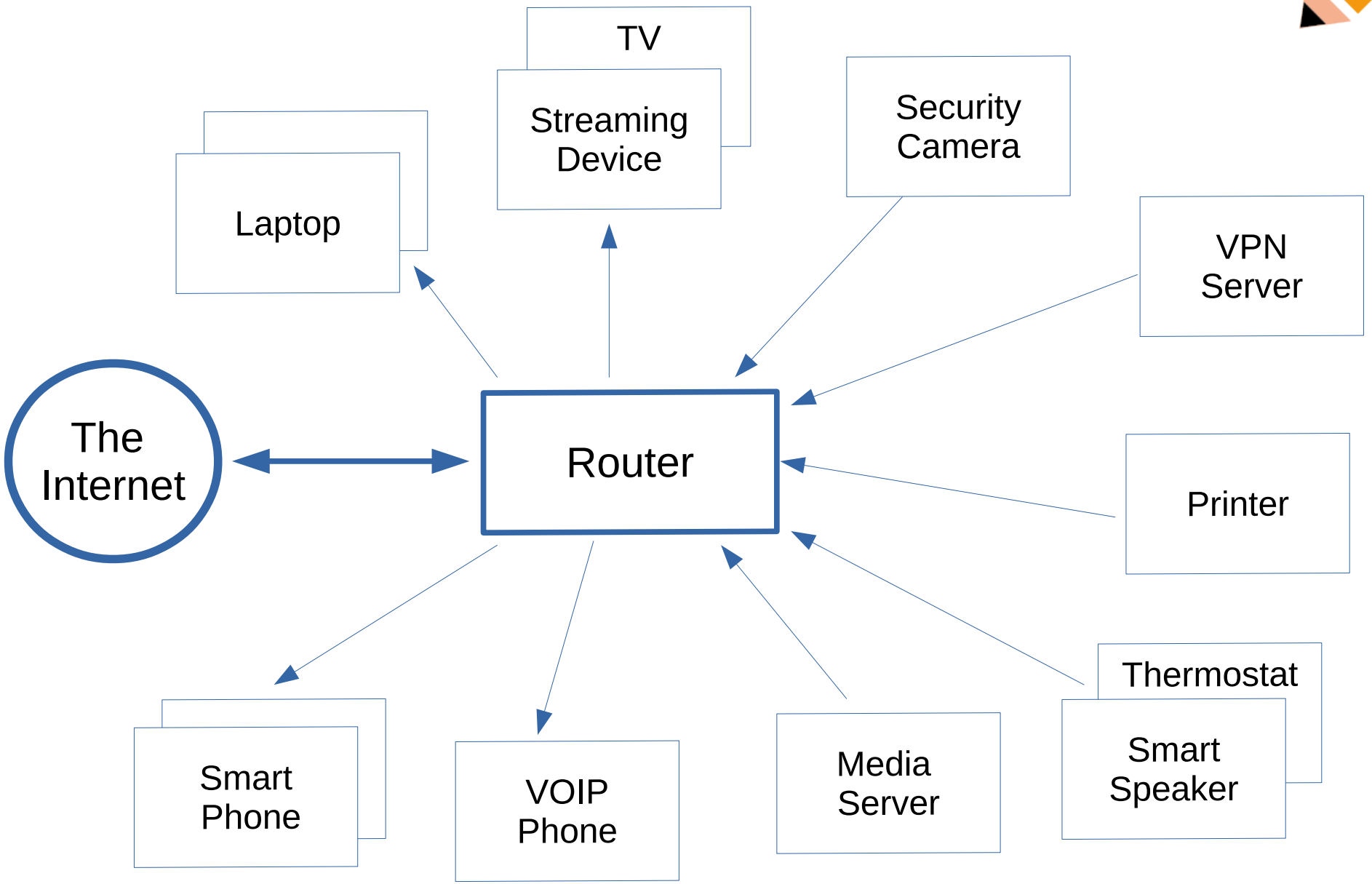
http://alanbaker.net/defending.pdf

Defending Your Home Network

- Your network’s devices and ports
- Device vulnerabilities and exploits
- What you can do



A Home Network



Blinking Lights

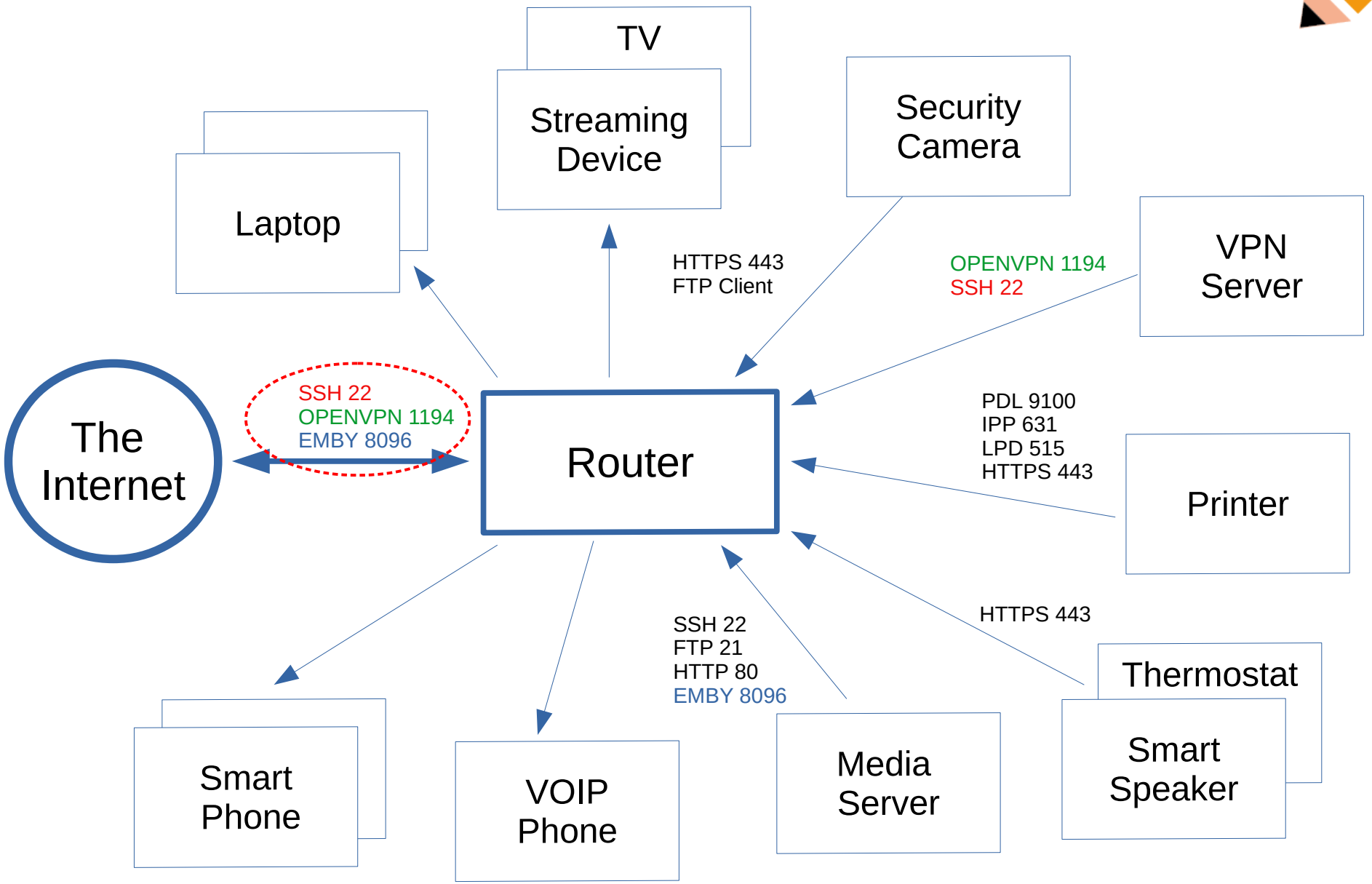
- Why does your router's activity light blink even when there's no traffic going in our out?
- Handshaking
- Reconnaissance by bad guys
- Looking for vulnerabilities

Casing the Joint

Bad guys' scripts are constantly assessing your:

- Hardware
  - For vulnerable default settings
- Software
  - For exploitable bugs
- Open ports
  - For ports that shouldn't be exposed to the internet

A Home Network's Ports



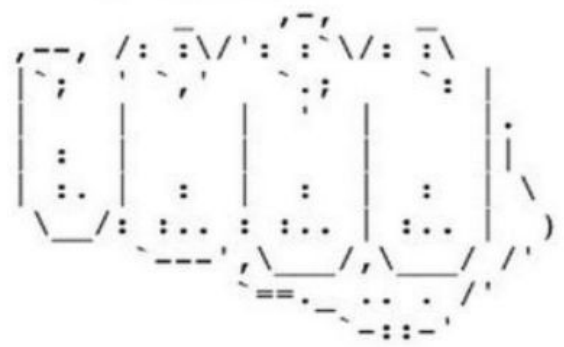
Finding Exploitable Devices is Easy

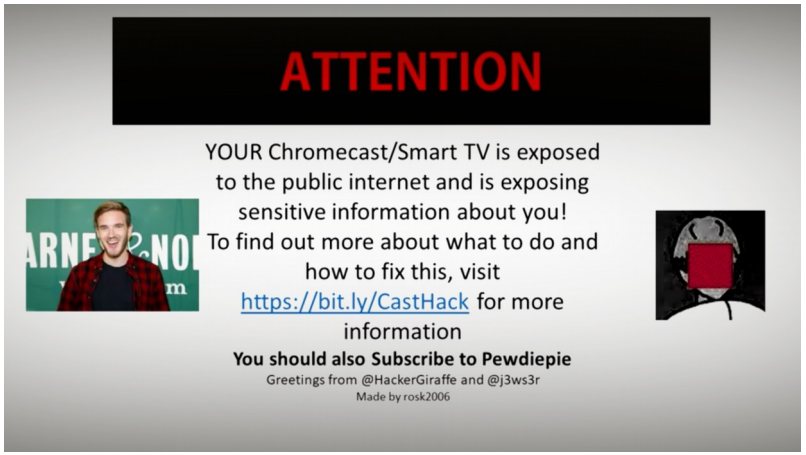
- Shodan’s bots find and index vulnerable internet-connected devices. Just like Google.

Hacker Giraffe

- Used Shodan to find 50,000 vulnerable printers and 70,000 vulnerable smart TV's
- Sent them the following:

```
--- WHAT TO DO ---
1. Unsubscribe from T-Series
2. Subscribe to PewDiePie
3. Share awarness to this issue
#SavePewDiePie #PrinterHack2
4. Tell everyone you know. Seriously.
5. Fix your printer. It can be abused!
6. BROFIST!
```





Things You Can Do

- Find your devices' vulnerabilities and update the software.
- Find ports exposed to the internet and close unneeded ports.
- Disable remote access and UpnP in your router
- Backup

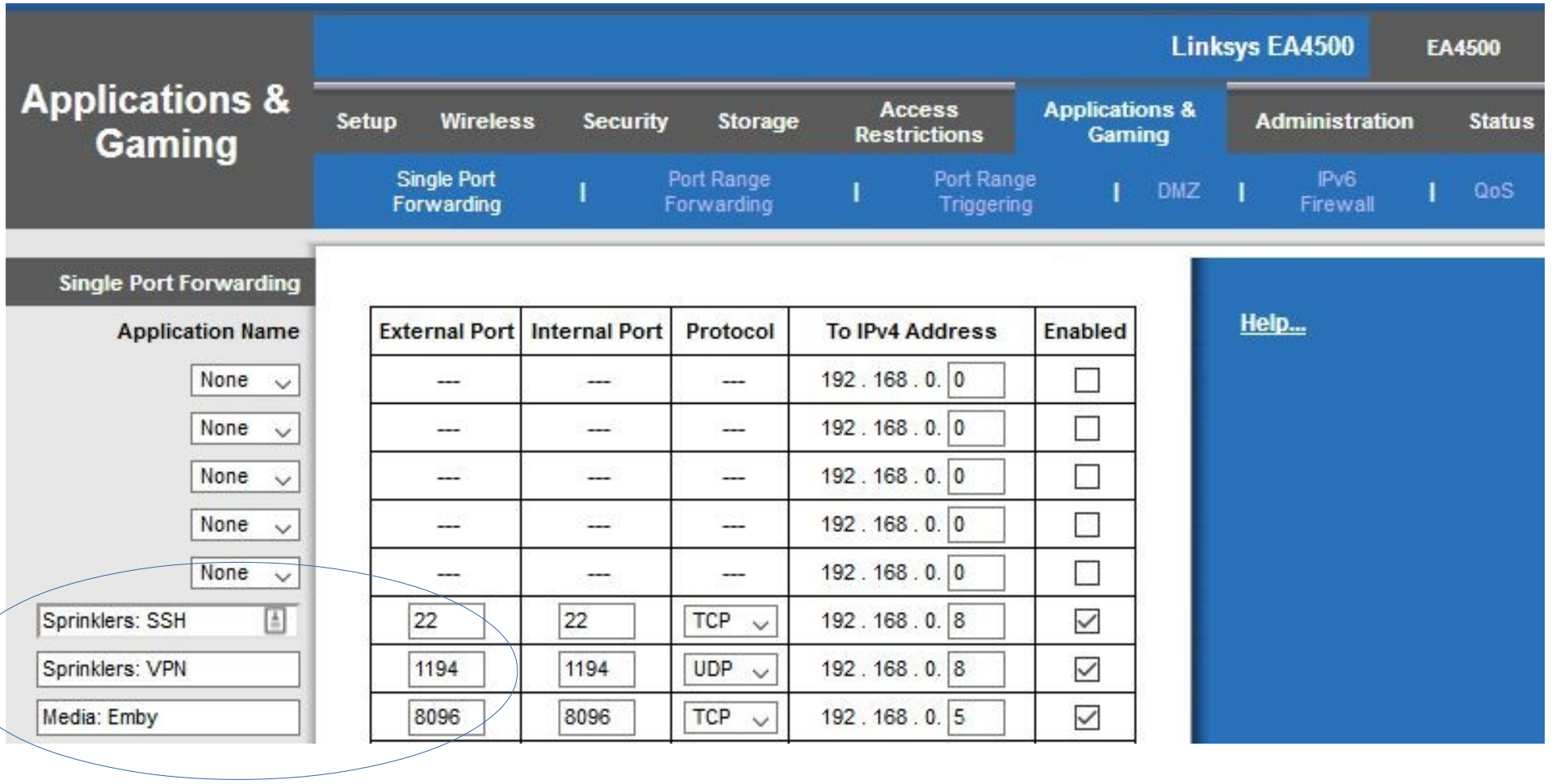
Vulnerabilities

- Which of your devices are vulnerable?
- Google will tell you.
- Each vulnerability is worth $$$ to someone.
- Apply vendor’s updates to each device.

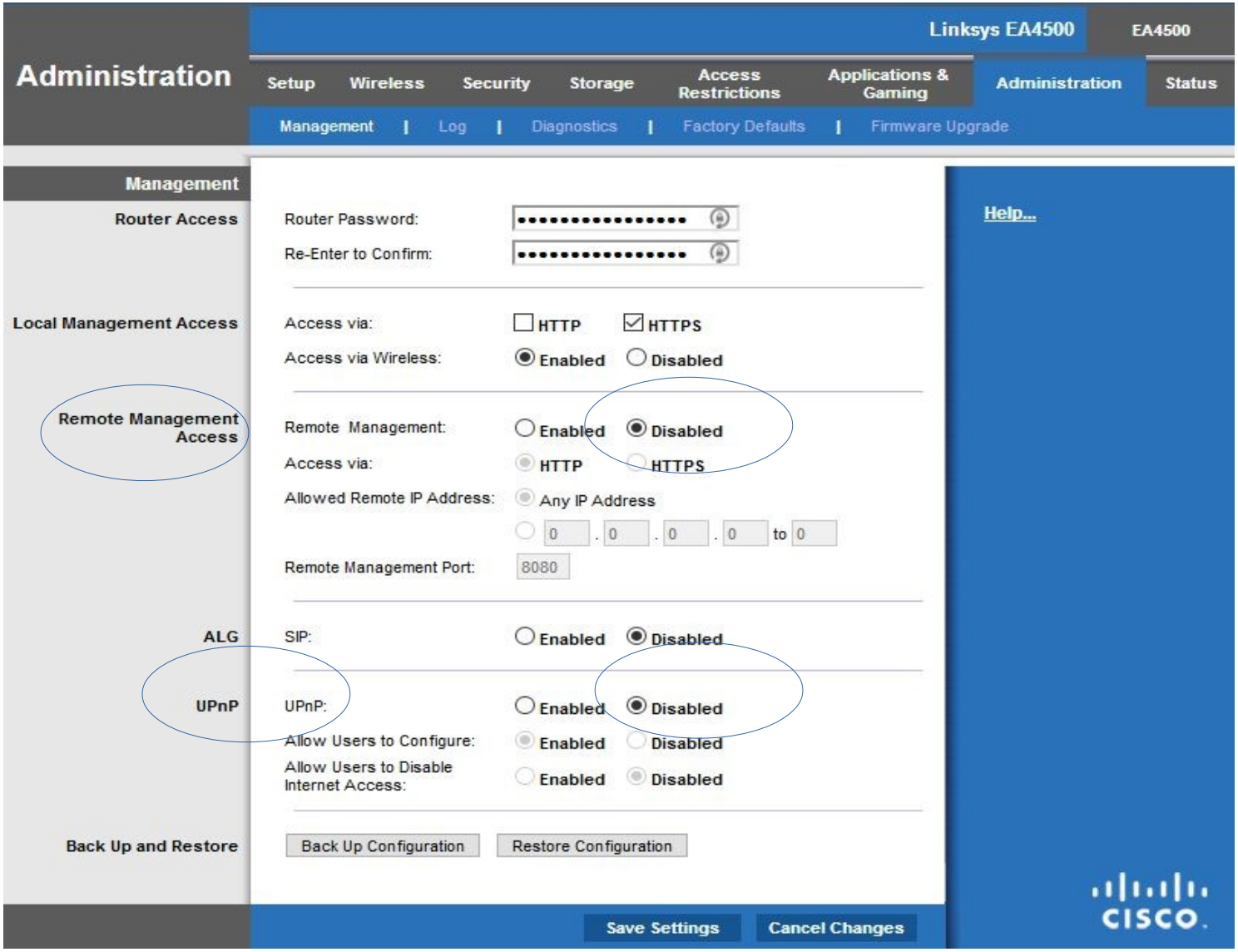
Scan your own network

- Fing: Easy to use Android scanner app
- Nmap/Zenmap: In-depth Linux/Windows scanner
- GRC Shields Up: Scans for open ports on your network from the internet side

Expose Only Specific Ports



Disable Remote Access, UpnP



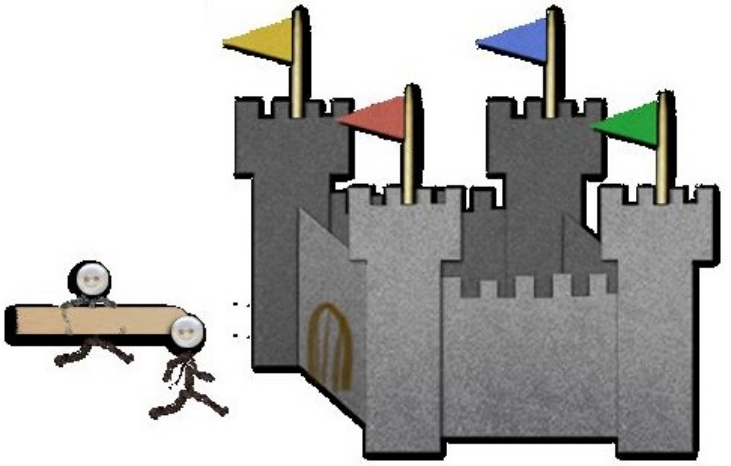
Is Online Backup a Good Idea?

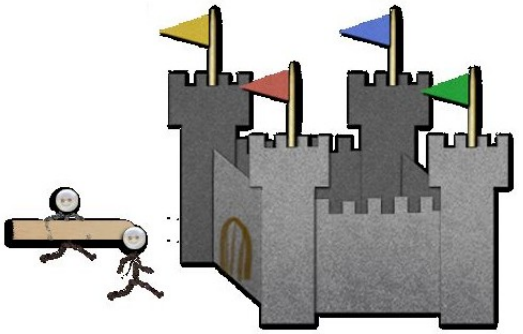
- In February 2019, unknown intruders wiped out VFEmail's secondary backup system, then their primary backup system, then their servers.
- Each system had different passwords.
- VFEmail restored an old offline backup from 2016, but everything since 2016 was lost.

- Recommendation: a) Back up everything b) to an external drive then c) unplug it.

Defending Your Home Network

- Your network’s devices and ports
- Device vulnerabilities and exploits
- What you can do





Defending Your Home Network

Alan Baker
San Jose IBM PC Club
March 11, 2019

http://alanbaker.net/defending.pdf