Levels of Network Security for IoT Devices at Home

Security Level

Type 3: separate VLANS for personal, IoT & guest

- Separate networks for personal devices, IoT devices, and Guest - all internet connected
- Advantages:
  - Guest network does not contain IoT devices & IoT are less at risk from bad guests
- Disadvantages:
  - These systems are prosumer type devices currently requiring complicated VLAN configurations
- Risks:
  - IoT Devices can still be attacked externally through immature device upgrade methodology and insecure web services
- Investment: $$$ WiFi router with VLAN network capability (these are more complex devices needing some technical expertise)

Features for future versions of consumer WiFi routers

https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot

https://www.lifewire.com/guest-network-for-home-tutorial-818204

https://www.pcmag.com/how-to/10-ways-to-set-up-your-wi-fi-for-guests

Type 2: guest network for IoT devices

- Private network for personal computing & entertainment devices and Guest network for IoT devices
- Advantages:
  - IoT devices are on a separate VLAN, have their own internet access but cannot communicate with the personal devices on the private network, reducing the risk of attacks from “owned” IoT devices
  - Easy to setup on “guest capable” WiFi routers
- Disadvantages
  - Communication from personal devices to IoT devices is through the internet and cloud services
  - Some of your guests have the guest network password where the IoT devices live (can you trust them?)
- Risks:
  - IoT Devices can still be attacked externally through their potentially hacked cloud services
  - Bad guests can attempt to connect and hack into IoT devices (caveat: a bad guest needs alone time on the Guest network)
- Investments: $ WiFi router with integrated guest network capability (ex: D-link, Google, Linksys, eero)

Minimal security level for households we care for

Type 1: wild, wild west with caged IoT devices

- Single network with personal computers, entertainment and IoT devices (but all IoT devices are configured to not have any internet connections and must be controlled via personal devices on the local private network)
- Advantages:
  - IoT devices cannot be ”owned” or hacked using rouge cloud services or compromised updates
- Disadvantages
  - Some devices may not be able to operate without internet access
  - IoT devices have to be updated manually (if at all)
  - IoT devices cannot be controlled remotely through cloud services (needs a VPN into a local server)
- Risks:
  - IoT devices are not updated and can lose value
- Investment: nil $ but takes regular attention to check and keep devices updated

”Consumers typically do not have the technical ability, or in many cases even the user interfaces, to effectively and safely implement patches.” Internet Society : IoT Security for Policymakers

Type 0: wild, wild west with free ranging IoT devices

- Single network with personal computers, entertainment and IoT devices all internet connected
- Advantages:
  - No management needed but like unmanaged systems, they get messy
  - All IoT devices can communicate on the internet for controls and data & system software updates
- Risks:
  - all IoT devices can communicate with personal devices providing a potential vector for hackers
  - IoT Devices can be attacked externally through their potentially own hacked cloud services
- Investment: nil $ (using simple router or simply configured router)

Most hacked devices: security cameras, smart hubs, NAS, printers, TVs, IP phones

Network Configuration Complexity

Copyright StoneTurner LLC 2020