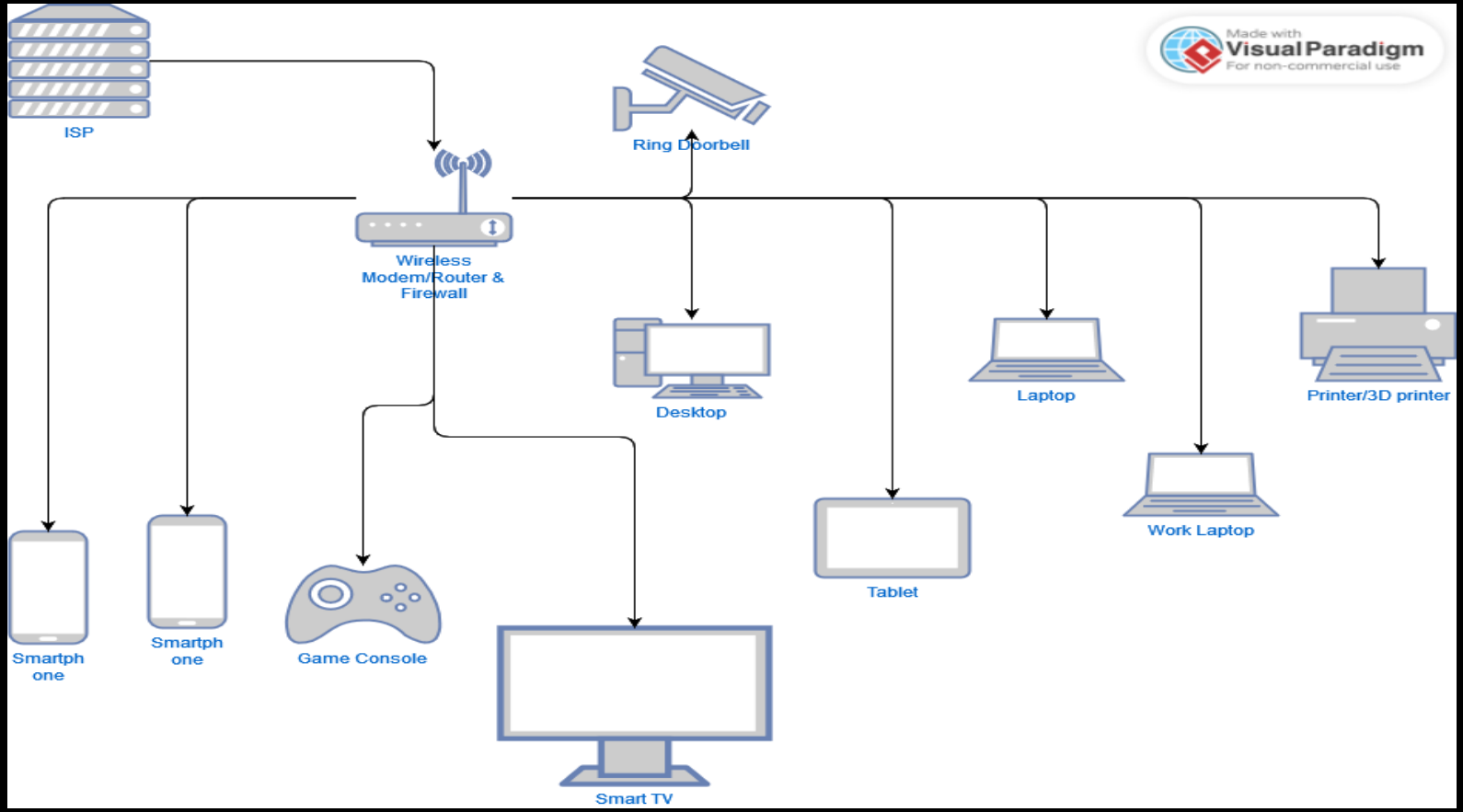
Home Security Series

Part 1: Home Networking

Traditional Home Network



Problems?

- No security
- No privacy
- At risk for being hacked*
- Difficult to manage

- Anyone can just “join”
- Single failure point
- *Lateral movement* is easy
- Potential for slower speeds

Mitigation

- Segmentation – create VLANs
- Isolation – cut off access
- Default Deny and No Default LAN
- Firewall rules

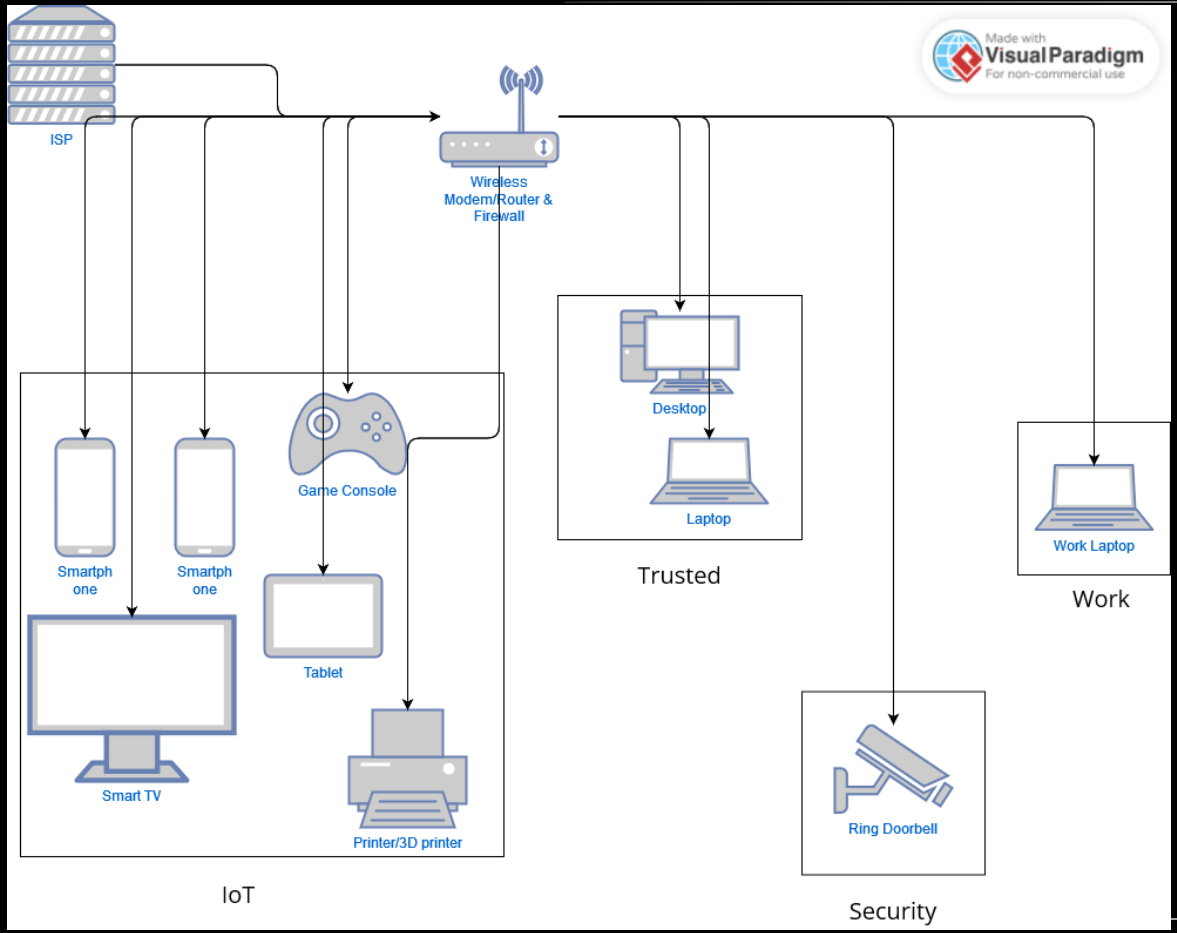
Planning

- Group devices into categories or levels of trust.
- Think about the level of permissions each device should have.
  - Should they know about all devices on my network
  - Should they reach the internet
  - etc

Planning Cont.

- Examples:
  - IoT – least amount of trust
  - Security – high amount of trust
  - Management – management interfaces of networking devices
  - Trusted – Desktop or laptop computers that need to access to management interfaces

What would this look like?



Things to Note

- Just putting devices into VLAN’s does not make them more secure
- Firewall rules will need to be setup
- You will probably need more hardware
- Take notes of your configurations
- There is no 1 correct way

Hardware Involved

- Modem
- Router*
- Switch (Managed)
- Wireless Access Points (WAP’s)

Software Involved

- Router’s
  - Default
  - OPNSense
  - Pfsense
  - OpenWRT.
  - DD-WRT

Software Involved Cont.

- Switches
  - Default
- Wireless Access Points
  - Default
  - OpenWRT

Configuration

- ToDo:
  - explain simple firewall rules
  - Explain VLAN’s and how to configure from Router to switch.
  - Explain VLAN’s with wireless access points