Sun City Computer Club

Cyber Security SIG

February 16, 2017

SCCCCyber@gmail.com

Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

- DHS daily briefing
- Cyber Security Executive Order
- Your info on other smartphones
- Boarding pass photo
- Credit card photo
- Monitoring the monitor
- Smart Phone WAP cache
- MitM
- GPS jammer
- Samsung SmartTV
- Microsoft SMB 0-day patch delay
- uPnP on home routers on by default
- University attack 5000devices
- Full Screen Microsoft Tech Support scam

- ??

Current topics

Current topics

- 178 million IPs associated with malicious activity   60% of internet traffic
- SHA-1 hash collisions
- Ransomware “helpdesk” support
- Sprial Toys
- Airport servers   1 year
- 4th amendment & border
- Windows option to block non-store apps
- Used smartcars
- Israeli Defense Forces Android devices
- Honeypot Honeynet   blame game
- Dojo by Bullguard
- USB firewall
- ??

Firewall

Agenda

- Securing a home network

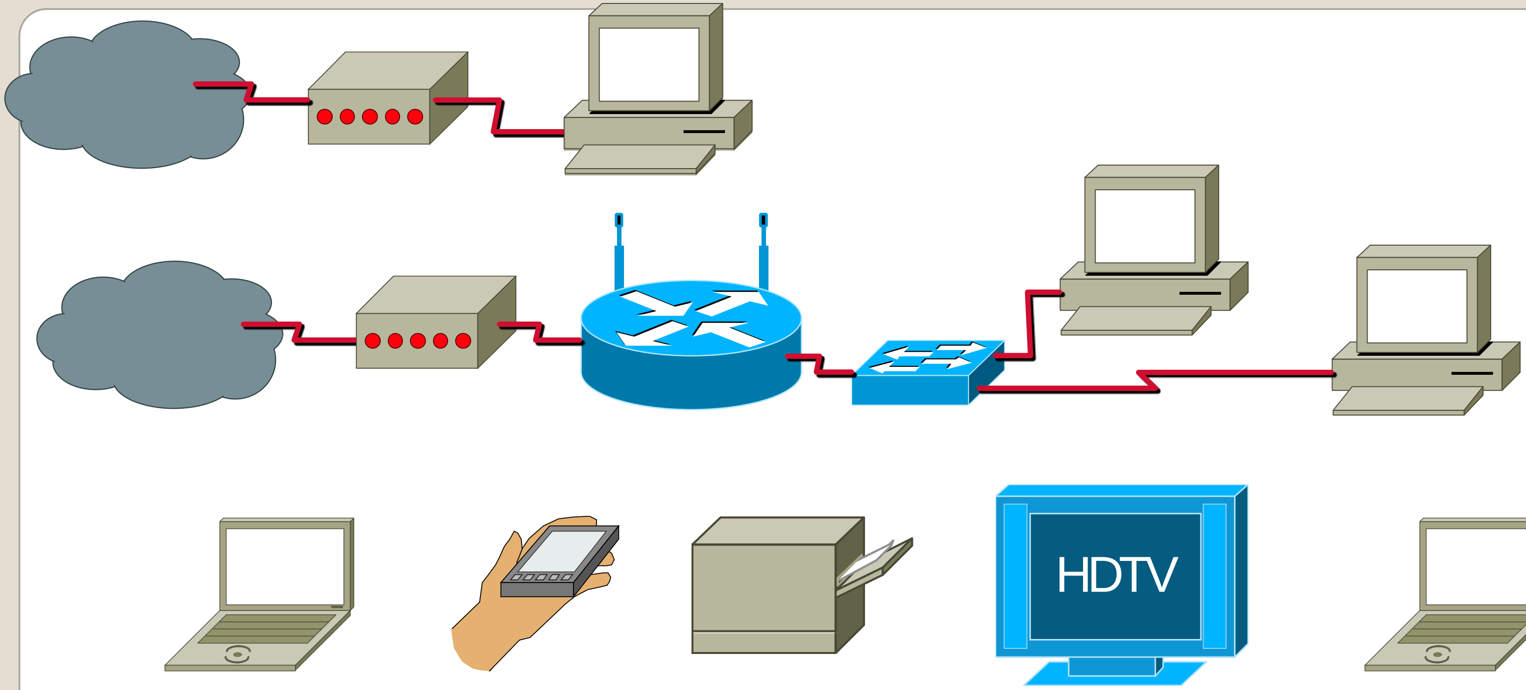
Design

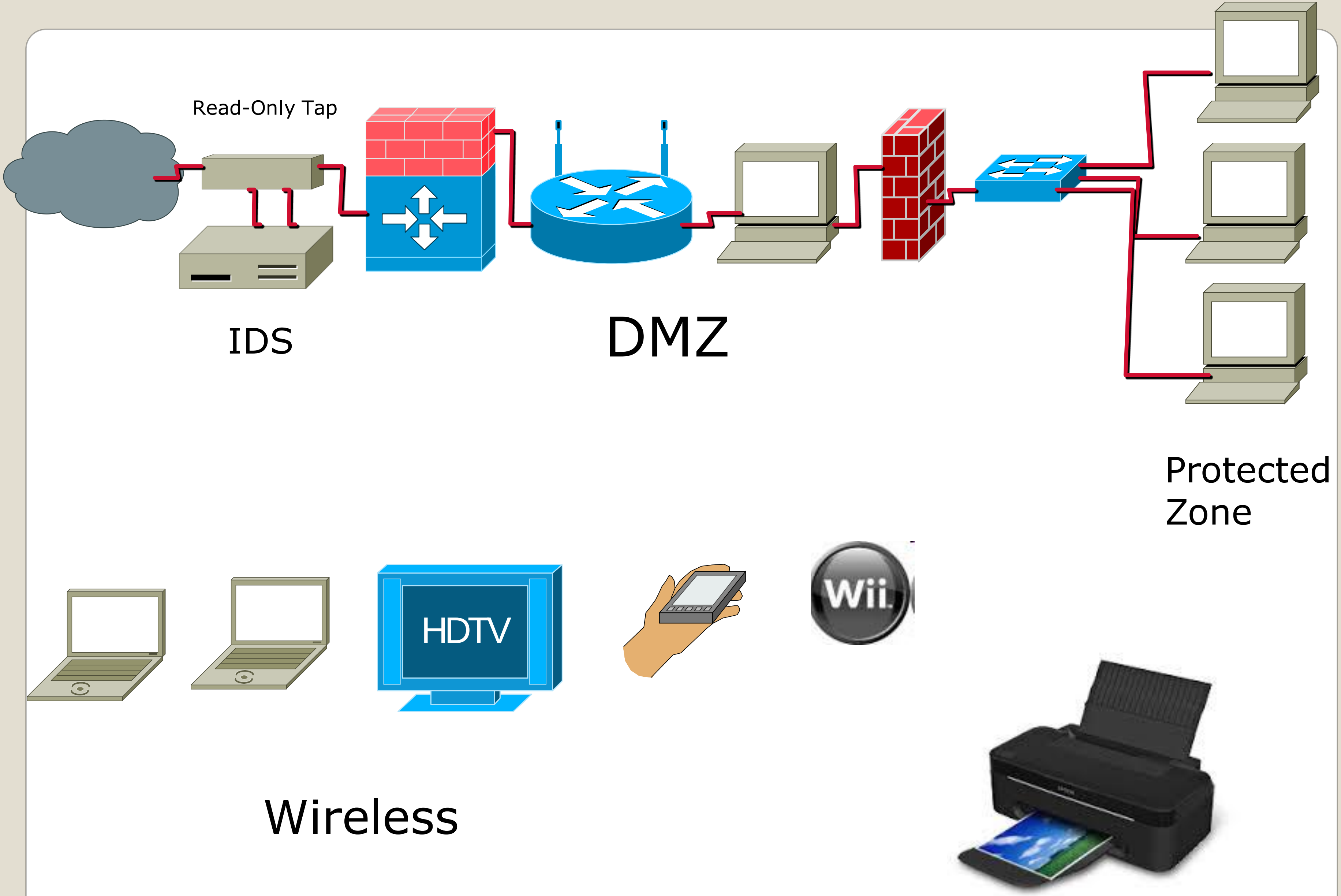
Configure

Instrument

Monitor

Home network


HDTV



Read-Only Tap

IDS

DMZ

Protected Zone

Wireless

- Privacy Issues
- Check on Internet traffic
- Intrusion Detection
- Intrusion Prevention
- Data Loss Notification
- Network Flow capture
- Read Only

Network Tap

- Filtering WEB Proxy Server
- Rogue Wireless Access Points
- Split DNS
- Other

DMZ Server

- Hardware and Software Firewalls
  filter BOTH ways
- Use Router Access Control Lists (ACLs)
- Default Deny   Access by Exception
- Choose Operating System   Virtual Machine Option
- Use Industry Best Practices
  http://cisecurity.org
- Network Address Translation (NAT)   DHCP reservation
- Banners
- Encryption

Configure

- IEEE 802.11 a/b/g/n ac
- Encryption WEP, WPA, WPA2, TKIP, EAP
- WPS protected setup
- Least Common Dominator
- SSID Name
- SSID Broadcast
- MAC Filtering DHCP Control Inventory
- Administrator Passwords
- Administrator Access HTTP Port Protected Zone
- Firmware Updates

Configure Wireless Access Points

- Hack from afar, Hack from not so far
- Speed and Distance
- Interference   Yours, Theirs
- Encryption for packet data only
- Dauthenticate

Wireless - radio

Instrument

- Logging to the Maximum
- Log to Central server in protected zone
- Host Based Intrusion Detection

  regmon, DiskMon, tripwire, rootkit, etc…
- Multiple Security Suites
- Simple Network Management Protocol SNMP off or secured

- Filter logs   Discard Benign
- Check Configurations often
- Keep Operating Systems, Applications and Firmware up to date
- Google for WAP GPS location
- Google for your assigned IP address
- Disassociate awareness
- Monitor the RF
- Monitor Internet Storm Center

  https://isc.sans.org

Monitor and Maintenance

- Questions, suggestions, comments?

SCCCCyber@gmail.com