Sun City Computer Club

Cyber Security SIG

March 5, 2020

Questions, Comments, Suggestions welcomed at any time

Even Now

- [Audio recording of this session as MP4 file](#)
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

- Blame Russia for Georgia cyber attacks
- Facial ID unlock celebrity phones at Madame Tussaud's?
- Clearview AI - hacked
     2200 partners U.S. Justice Dept, Immigration, NBA
- Tomcat – UPDATE
- Safari certificate lifetime change
- Ransomware publish victim's cloud backup information
- Microsoft subdomain vulnerability
- Facebook, Google, Twitter leave Pakistan

Current Issues

- HEB Pharmacy plastic bags w/ PII
  Name, DoB, Address, Phone Number,
  medication, price
- Android 7,8,9 *rooted*
- Malware less attacks increasing
- NSA metadata program
   $100M   4 years   2 leads
- GoodRx info sharing Google & Facebook

Current Issues

Nationwide®
is on your side

b. Discharge of any nuclear weapon (even if accidental);

Terms and Conditions

- Wi-Fi alliance trademark
- Protocol standard   IEEE 802.11
- 2.4GHz UHF
- 5 GHz SHF ISM
- Channels
- RADIO
- Encryption - data portion ONLY
- Sniffing MAC   re-use MAC
- WEP, WPA, WPA-2
- WPA3 display-less devices, weak passphrase

Wi-Fi Wireless   RADIO

- Infrastructure

  Stations   Wireless Access Points (WAP)
- Ad-hoc Station - Station
- Service Set - local, independent, extended, mesh
- Service Set IDentifier (SSID)   32-byte
- Basic Service Set BSS associated stations
- BSSID MAC address

Wi-Fi

- Industrial, Scientific, Medical bands
- 2.4GHz 11 channels US, 14 Japan, 13 EU
  3 non-overlap sets
    1,6,11   2,7,12   3,8,13   *4,9,14*
- 5 GHz (5.8) 23 non-overlapping channels
- NOT 5G Generation cellular
- Higher frequency, more attenuation
- 2.4GHz microwave, cordless phones, etc.
- 2.4GHZ 5MHz wide   5GHz 20MHz wide

Wi-Fi

- 802.11b 11Mbps 2.4GHz
- 802.11a 54Mbps 5GHz
- 802.11g 54Mbps 2.4GHz
- 802.11n 600Mbps 2.4GHz & 5GHz
- 802.11ac 1300Mbps 5GHz
- 802.11ax

Wi-Fi

- Hotspots Theirs   Yours
- Channels half duplex time shared
- Radio broadcast   "is this me/mine"
- MAC address
- CSMA/CD
- 802 protocol ethernet
- Encryption is data portion of packet ONLY

Wi-Fi

- Antennae to & fro Pringles can Yagi 200+ miles
- MIMO   ac
- 48 – 54 devices at my home
- Circuitry shrinkage
- Commodity devices
- Hide real SSID in thousands of SSIDs
- VPN

Wi-Fi

- WEP, WAP, WPA-2   LCD
- Hiding SSID
- Interior of floor plan   observe RF blockers
- Too much power neighbor leakage
- 2.4GHz   usage of 20MHz range

Wi-Fi

CHANNEL	SPECTRUM UTILIZATION	WIFI UTILIZATION		HIGHEST SIGNAL
1		████████	76.5%	Apex Leaders @ -49 dBm
2			0.0%	-
3			0.0%	Pitty in the city @ -70 dBm
4			0.0%	-
5			0.0%	-
6		████████	82.4%	CenturyLink0611 @ -57 dBm
7			0.0%	-
8			0.0%	-
9		████	36.5%	Luft @ -70 dBm
10			0.0%	-
11		████████	82.7%	-63 dBm
36		▌	1.2%	MTCDC Guest @ -83 dBm
40		██	14.5%	Red Sky @ -88 dBm
44		▌	2.0%	Apex Leaders @ -59 dBm
48		█	7.1%	Apex Leaders @ -62 dBm
52			0.0%	-
56			0.0%	-
60		▌	2.7%	MPGuest @ -71 dBm
64		█	7.1%	DeviceNet @ -66 dBm
100			0.0%	-
104			0.0%	-
108		▌	0.8%	MPGuest @ -71 dBm
112			0.0%	-

- Human & pet attenuation
- Ceiling mount, high shelf or bookcase
- Extender? Half way ther
- Mesh   dedicated back haul radio
- Ethernet wire up and over
- Powerline option

Wi-Fi

- Big B   little b
- Fast.com   DSLReports.com
- Latency   gaming, video conferencing
- Asymmetric connections
- One bad connection-> all bad connections
- One bad *upload* connection …
- Cabling

Wi-Fi

- ADMINISTRATOR passphrase!!
- Strong WPA-2 passphrase
- Segmentation
- Guest network
- MAC filtering
- Firewall - check logs
- Network Map   Network usage logs
- Inside IP of cable modem – block
- Lowest common denominator
- Disable external access until needed
- Update firmware

Security

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com