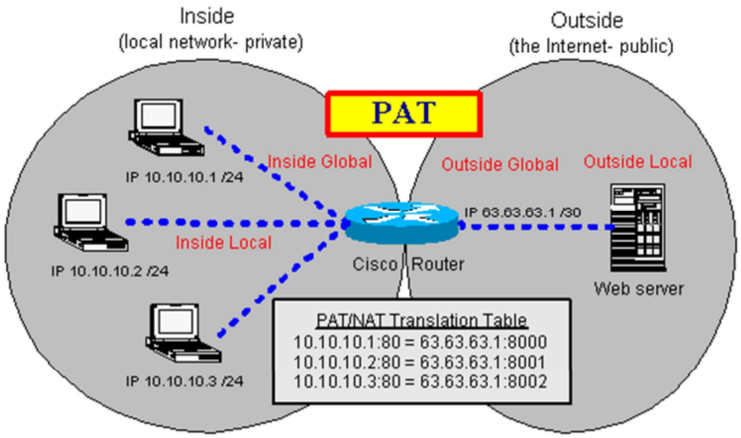
Network Access Control (NAC) Devices

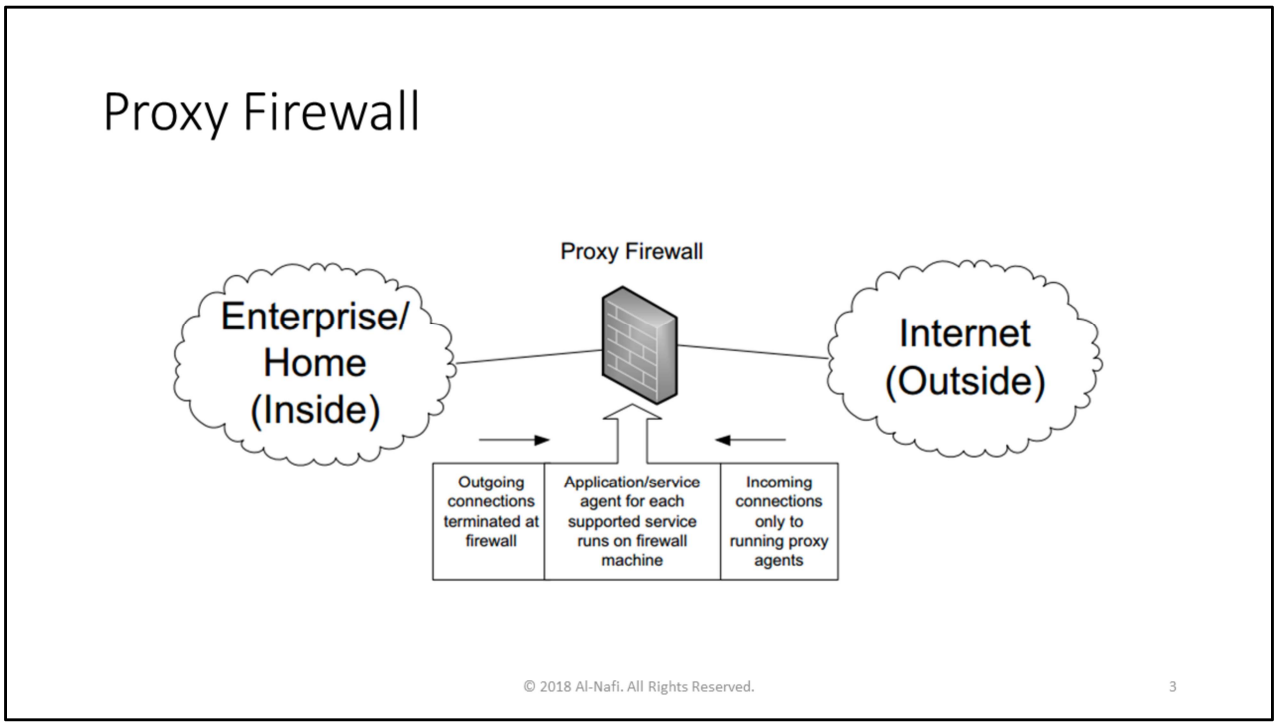
- Port Address Translation (PAT)
- Proxy Firewall
- Proxy Types
- Endpoint Security

Port Address Translation (PAT)



Port Address Translation (PAT)

An extension to network address translation (NAT), which translates all addresses to one externally routable IP address, is to use port address translation (PAT) to translate the source port number for an external service. The port translation keeps track of multiple sessions that are accessing the internet.

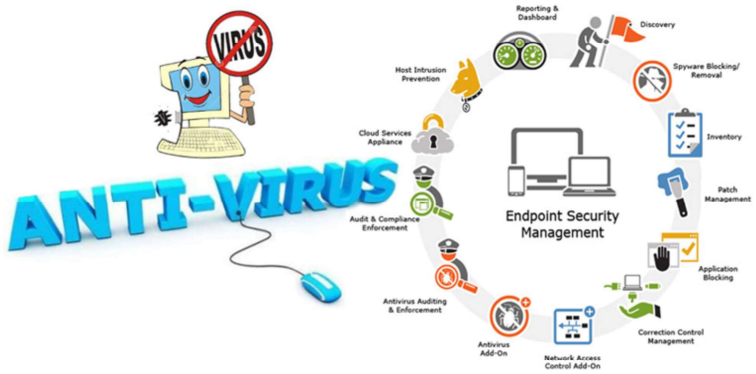


Proxy Firewall

A proxy firewall mediates communications between untrusted endpoints (servers/hosts/clients) and trusted endpoints (servers/hosts/clients). From an internal perspective, a proxy may forward traffic from known, internal client machines to untrusted hosts on the internet, creating the illusion for the untrusted host that the traffic originated from the proxy firewall, thus, hiding the trusted internal client from potential attackers. To the user, it appears that they are communicating directly with the untrusted server. Proxy servers are often placed at internet gateways to hide the internal network behind one IP address and to prevent direct communication between internal and external hosts.

Endpoint Security

Difference between Endpoint security and Antivirus?



 4

Endpoint Security

Workstations should be hardened, and users should be using limited access accounts whenever possible in accordance with the concept of “least privilege.”

Workstations should have the following:

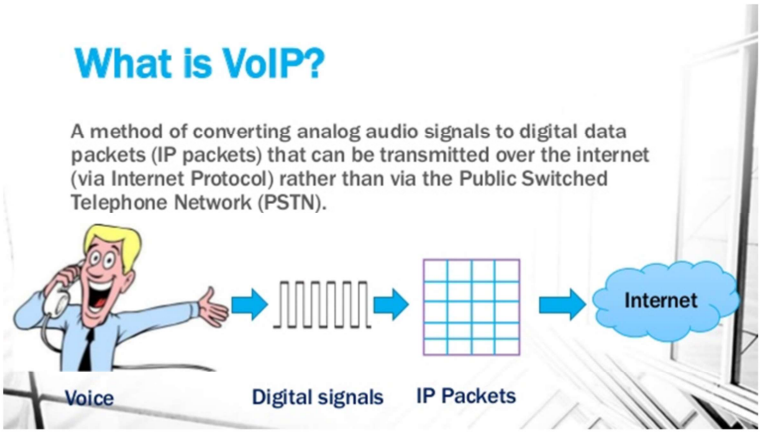
- Up to date antivirus and anti-malware software
- A configured and operational host-based firewall
- A hardened configuration with unneeded services disabled
- A patched and maintained operating system

While workstations are clearly what most people will associate with endpoint attacks, the landscape is changing. Mobile devices, such as smart phones, tablets etc., are beginning to make up more and more of the average organization’s endpoints. With this additional diversity of devices, there becomes a requirement for the security architect to also increase the diversity and agility of an organization’s endpoint defenses.

For mobile devices such as smart phones and tablets, consider the following:

- Encryption for the whole device, or if not possible, then at least encryption for sensitive information held on the device
- Device virtualization/sandboxing
- Remote management capabilities including the following:
    - o Remote wipe
    - o Remote geo locate
    - o Remote update
    - o Remote operation
- User policies and agreements that ensure an organization can manage the device or seize it for legal hold

Voice over Internet Protocol (VoIP)

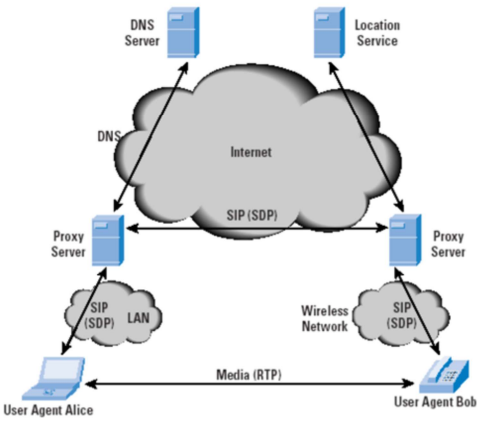


Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a broadband internet connection instead of a regular (or analog) phone line. VoIP is simply the transmission of voice traffic over IP-based networks. VoIP is also the foundation for more advanced unified communications applications such as web and video conferencing. VoIP systems are based on the use of the Session Initiation Protocol (SIP), which is the recognized standard. Any SIP compatible device can talk to any other. In all VoIP systems, your voice is converted into packets of data and then transmitted to the recipient over the internet and decoded back into your voice at the other end. To make it quicker, these packets are compressed before transmission with certain codecs, almost like zipping a file on the fly. There are many codecs with diverse ways of achieving compression and managing bitrates, thus, each codec has its own bandwidth requirements and provides different voice quality for VoIP calls.

VoIP systems employ session control and signaling protocols to control the signaling, set-up, and tear-down of calls. A codec is software that encodes audio signals into digital frames and vice versa. Codecs are characterized by different sampling rates and resolutions. Different

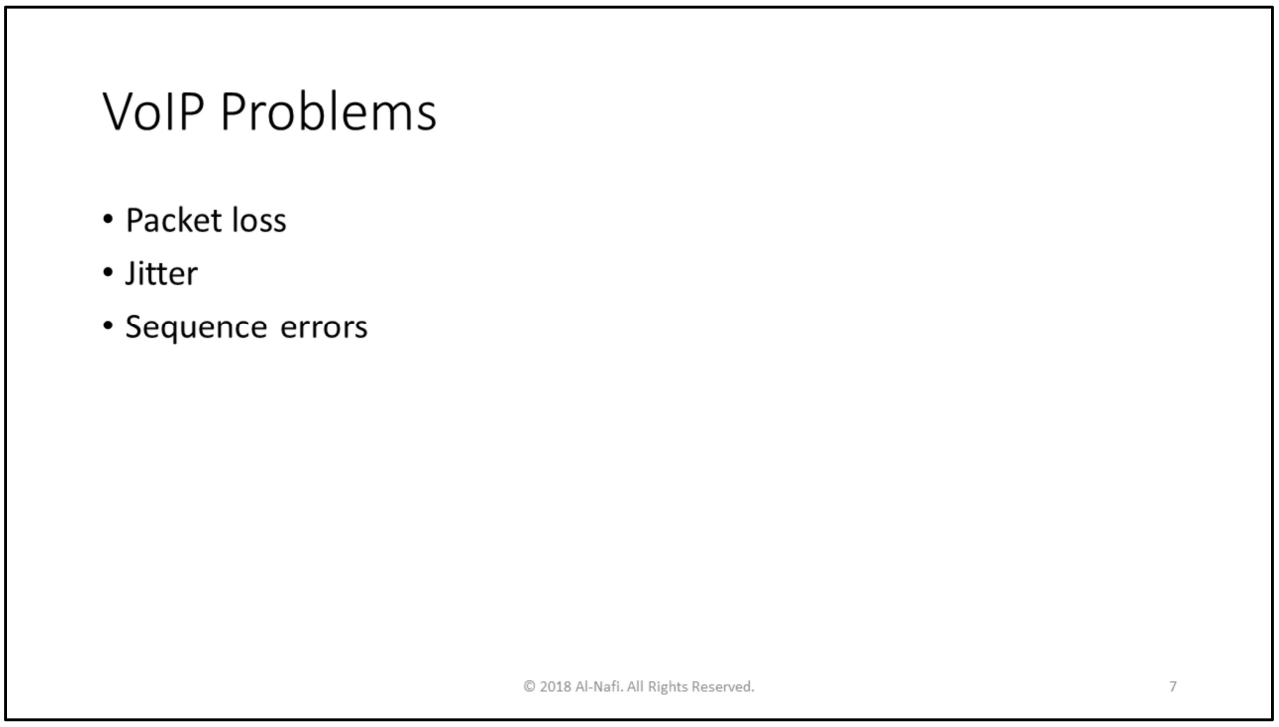
codecs employ different compression methods and algorithms, using different bandwidth and computational requirements.

Session Initiation Protocol (SIP)



Session Initiation Protocol (SIP)

As its name implies, SIP is designed to manage multimedia connections. SIP is designed to support digest authentication structured by realms, like HTTP (basic username/password authentication has been removed from the protocol as of RFC 3261). In addition, SIP provides integrity protection through MD5 hash functions. SIP supports a variety of encryption mechanisms, such as TLS. Privacy extensions to SIP, including encryption and caller ID suppression, have been defined in extensions to the original Session Initiation Protocol (RFC 3325).



VoIP Problems

Packet loss: A technique called packet loss concealment (PLC) is used in VoIP communications to mask the effect of dropped packets. There are several techniques that may be used by different implementations:

Zero substitution is the simplest PLC technique that requires the least computational resources. These simple algorithms generally provide the lowest quality sound when a considerable number of packets are discarded.

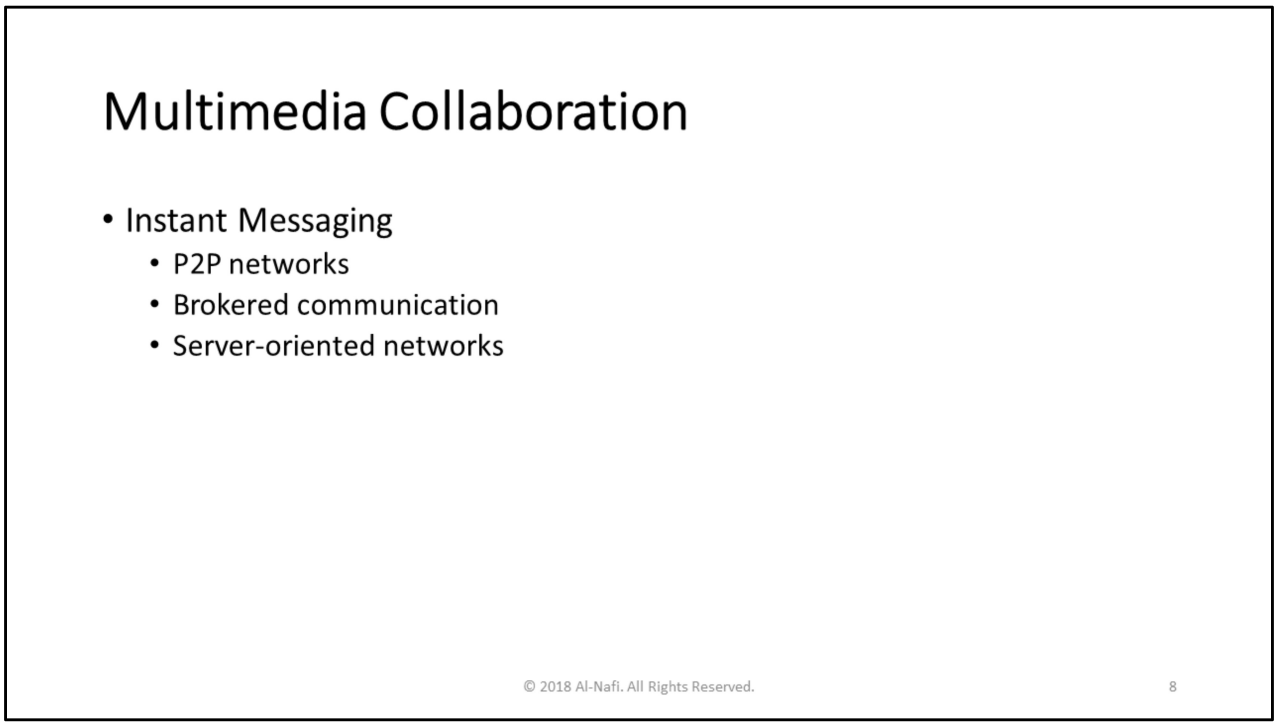
Filling empty spaces with artificially generated, substitute sound. The more advanced algorithms interpolate the gaps, producing the best sound quality at the cost of using extra computational resources. The best implementation can tolerate up to 20 percent of packets lost without significant degradation of voice quality. While some PLC techniques work better than others, no masking technique can compensate for a significant loss of packets. When bursts of packets are lost due to network congestion, noticeable degradation of call quality occurs.

In VoIP, packets can be discarded for many reasons, including network congestion,

line errors, and late arrival. The network architect and security practitioner need to work together to select the right PLC technique that best matches the characteristics of an environment, as well as to ensure that they implement measures to reduce packet loss on the network.

Jitter: Unlike network delay, jitter does not occur because of the packet delay but because of a variation of packet timing. As VoIP endpoints try to compensate for jitter by increasing the size of the packet buffer, jitter causes delays in the conversation. If the variation becomes too high and exceeds 150ms, callers notice the delay and often revert to a walkie-talkie style of conversation. Reducing the delays on the network helps keep the buffer under 150ms even if a significant variation is present. While the reduced delay does not necessarily remove the variation, it still effectively reduces the degree to which the effect is pronounced and brings it to the point where it's unnoticeable by the callers. Prioritizing VoIP traffic and implementing bandwidth shaping also helps reduce the variation of packet delay. At the endpoint, it is essential to optimize jitter buffering. While greater buffers reduce and remove the jitter, anything over 150ms noticeably affects the perceived quality of the conversation. Adaptive algorithms to control buffer size depending on the current network conditions are often quite effective. Fiddling with packet size (payload) or using a different codec often helps control jitter as well.

Sequence errors: Routed networks will send packets along the best possible path at this moment. That means packets will, on occasion, arrive in a different order than transmitted. This will cause a degradation in the call quality.



Peer-to-Peer (P2P) Applications and Protocols

Peer-to-peer (P2P) applications are often designed to open an uncontrolled channel through network boundaries (normally through tunneling). Therefore, they provide a way for dangerous content, such as botnets, spyware applications, and viruses, to enter an otherwise protected network. Because P2P networks can be established and managed using a series of multiple, overlapping master and slave nodes, they can be very difficult to fully detect and shut down. If one master node is detected and shutdown, the "bot herder" who controls the P2P botnet can make one of the slave nodes a master and use that as a redundant staging point, allowing for botnet operations to continue unimpeded.

Instant Messaging

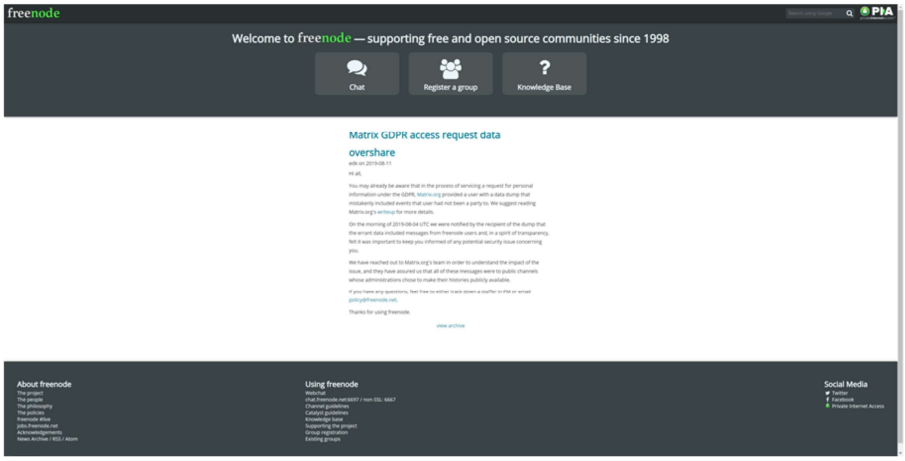
Instant messaging systems can generally be categorized in three classes:

- P2P networks
- Brokered communication
- Server-oriented networks

All these classes will support basic "chat" services on a one-to-one basis and

frequently on a many-to-many basis. Most instant messaging applications do offer additional services beyond their text messaging capability, for instance, screen sharing, remote control, exchange of files, and voice and video conversation. Some applications even allow command scripting. Instant messaging and chat is increasingly considered a significant business application used for office communications, customer support, and “presence” applications. Instant message capabilities will frequently be deployed with a bundle of other IP-based services such as VoIP and video conferencing support.

Internet Relay Chat (IRC)



Internet Relay Chat (IRC)

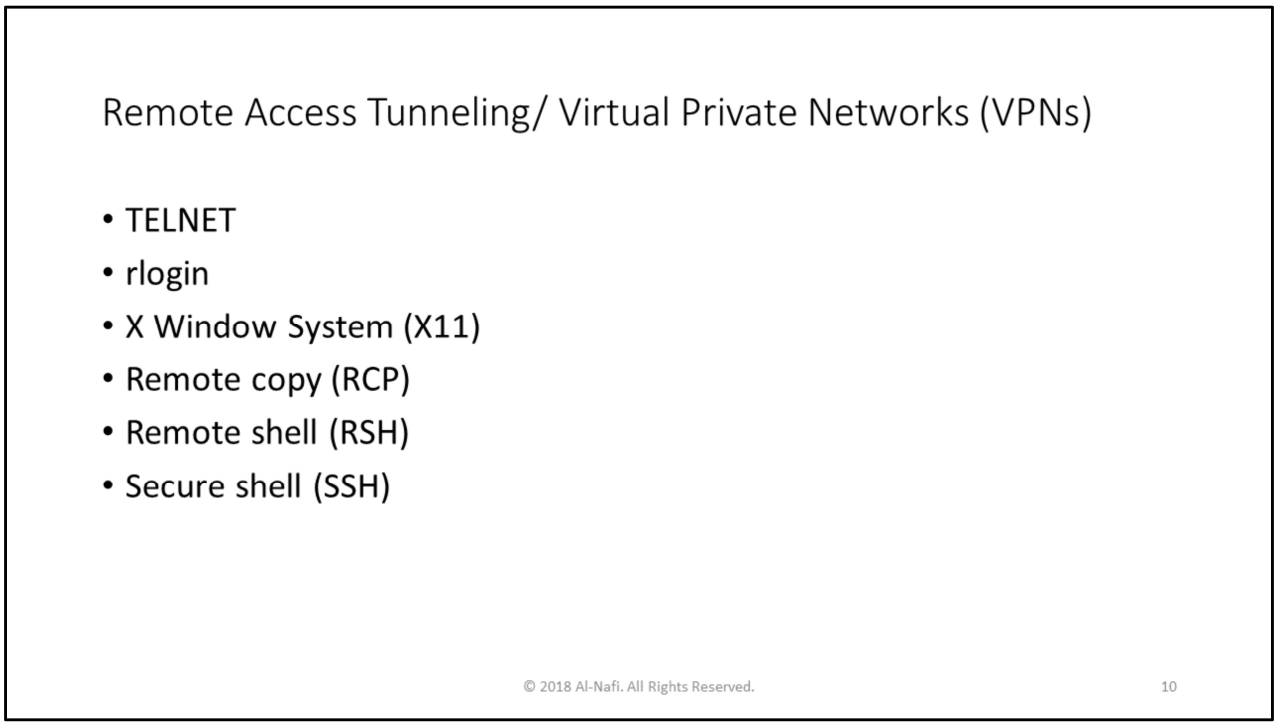
Internet Relay Chat (IRC) is a client/server-based network. This is a common method of communicating today. IRC is unencrypted and, therefore, an easy target for sniffing attacks. The basic architecture of IRC, founded on trust among servers, enables special forms of denial-of service attacks. For instance, a malicious user can hijack a channel while a server or group of servers has been disconnected from the rest (net split). IRC is also a common platform for social engineering attacks aimed at inexperienced or technically unskilled users. While there are many business and personal benefits and efficiencies to be gained from adopting instant messaging/chat/IRC technologies, there are also many risks.

Authenticity: User identification can be easily faked in instant messaging and chat applications by the following:

- Choosing a misleading identity upon registration or changing one's nickname while online.
- Manipulating the directory service if the application requires one.
- Manipulating either the attacker's or the target's client to send or display a

wrong identity.

- The continued growth of social-networking services and sites like Facebook, Vine, KiK, Twitter, LinkedIn and others present amply opportunity to create false identity and to try and dupe others for criminal purposes.



Remote-Access Services

The services described under this section are present in many UNIX operations and, when combined with Network File System (NFS) and Network Information Service (NIS), provide the user with seamless remote working capabilities. However, they also form a risky combination if not configured and managed properly.

These services include the following:

- TELNET
- rlogin
- X Window System (X11)
- Remote copy (RCP)
- Remote shell (RSH)
- Secure shell (SSH)

Conceptually, because they are built on mutual trust, they can be misused to obtain access and to horizontally and vertically escalate privileges in an attack. Their authentication and transmission capabilities are insecure by design; therefore, they have to be retrofitted (as X11) or replaced altogether (TELNET and rlogin by SSH).

TELNET is a command line protocol designed to give command line access to another host. Although implementations for Windows exist, TELNET's original domain was the UNIX server world, and in fact, a TELNET server is standard equipment for any UNIX server. (Whether it should be enabled is another question entirely, but in small LAN environments, TELNET is still widely used.)

TELNET:

- Offers little security, and indeed, its use poses serious security risks in untrusted environments.
- Is limited to username/password authentication.
- Does not offer encryption.

Once an attacker has obtained even a low-level user's credentials, they have a trivial path toward privilege escalation because they can transfer data to and from a machine, as well as execute commands. As the TELNET server is running under system privileges, it is an attractive target of attack in itself; exploits in TELNET servers pave the way to system privileges for an attacker. Therefore, it is recommended that security practitioners discontinue the use of TELNET over the internet and on internet facing machines. In fact, the standard hardening procedure for any internet facing server should include disabling its TELNET service that under UNIX systems would normally run under the name of telnetd, and using SSHv2 for remote administration and management where required.

Remote Log-in (rlogin), Remote Shell (rsh), Remote Copy (rcp) In its most generic form, rlogin is a protocol used for granting remote access to a machine, normally a UNIX server. Similarly, rsh grants direct remote command execution while rcp copies data from or to a remote machine. If a rlogin daemon (rlogind) is running on a machine, rlogin access can be granted in two ways:

- Using a central configuration file
- Through a user configuration

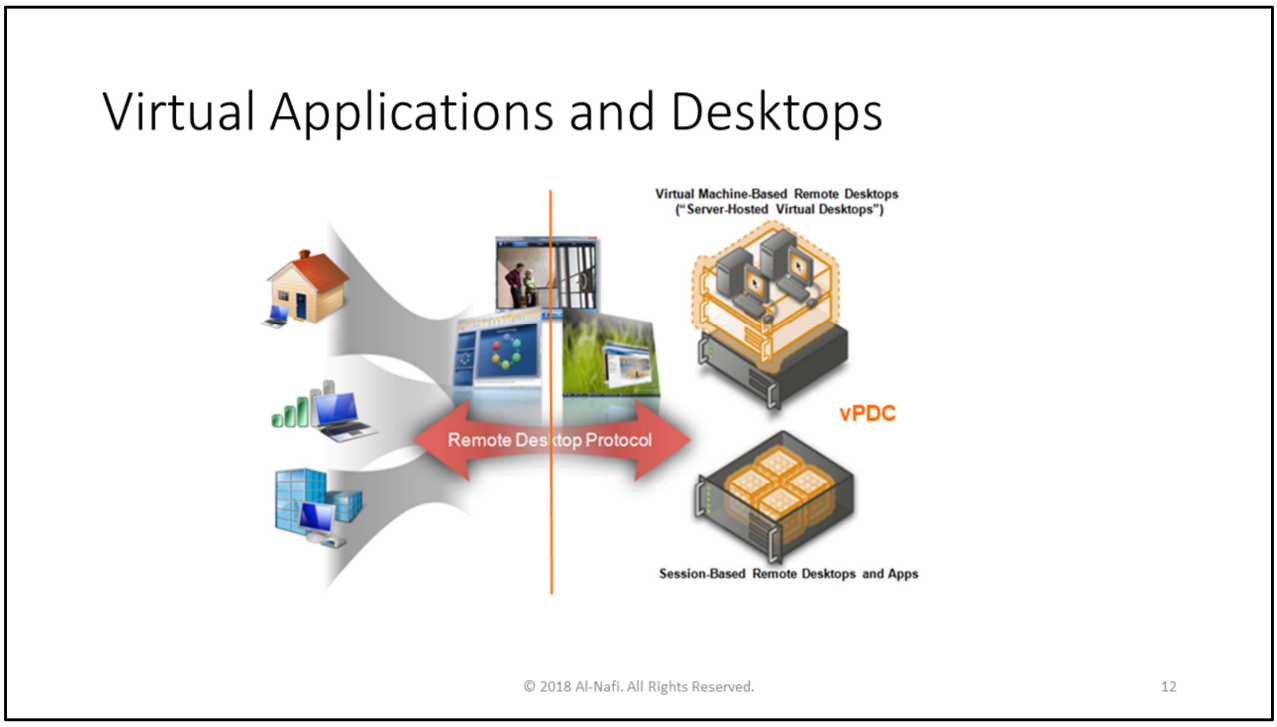
By the latter, a user may grant access that was not permitted by the system administrator. The same mechanism applies to rsh and rcp although they are relying on a different daemon (rshd). Authentication can be considered host/IP address based. Although rlogin grants access based on user ID, it is not verified; i.e., the ID a remote client claims to possess is taken for granted if the request comes from a trusted host. The rlogin protocol transmits data without encryption and is hence subject to eavesdropping and interception.

The rlogin protocol is of limited value—its main benefit can be considered its main drawback: remote access without supplying a password. It should only be used in trusted networks, if at all. A more secure replacement is available in the form of SSHv2 for rlogin, rsh, and rcp.

Screen Scraper

Screen Scraper

A screen scraper is a program that can extract data from output on a display intended for a human. Screen scrapers are used in a legitimate fashion when older technologies are unable to interface with modern ones. In a nefarious sense, this technology can also be used to capture images from a user's computer such as PIN pad sequences at a banking website when implemented by a virus or malware.

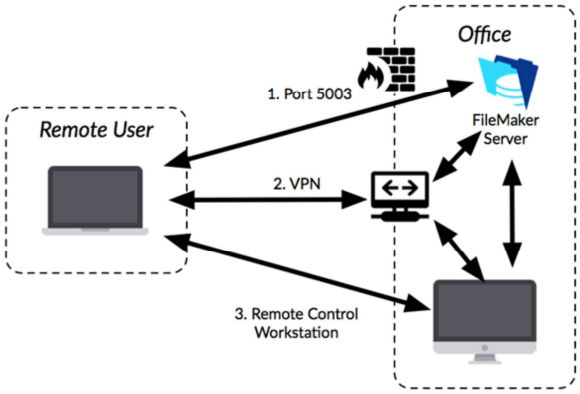


Virtual Applications and Desktops

Virtual Network Terminal Services

Virtual terminal service is a tool frequently used for remote access to server resources. Virtual terminal services allow the desktop environment for a server to be exported to a remote workstation. This allows users at the remote workstation to execute desktop commands as though they were sitting at the server terminal interface in person. The advantage of terminal services such as those provided by Citrix, Microsoft, or public domain virtual network computing (VNC) services is that they allow for complex administrative commands to be executed using the native interface of the server, rather than a command-line interface, which might be available through SSHv2 or telnet. Terminal services also allow for the authentication and authorization services integrated into the server to be leveraged for remote users, in addition to all the logging and auditing features of the server as well.

Remote Access



Virtual Private Network (VPN)

A virtual private network (VPN) is point-to-point connection that extends a private network across a public network. The most common security definition is an encrypted tunnel between two hosts, but doesn't have to be. A tunnel is the encapsulation of one protocol inside another. Remote users employ VPNs to access their organization's network securely.

Depending on the VPN's implementation, they may have most of the same resources available to them as if they were physically at the office. As an alternative to expensive dedicated point-to-point connections, organizations use gateway-to-gateway VPNs to securely transmit information over the internet between sites or even with business partners.