Remote Access Services

Lecture 6

Prepared by:
Jonel M. Baculod
Gerami M. Benedicto

College of Engineering and
Information Technology

What is Remote Access

- ability for an authorized person to access a computer or network from a geographical distance through a network connection.
- enables users to connect to the systems they need when they are physically far away. This is especially important for employees who work at branch offices, are traveling or telecommute.

A **remote access strategy** gives organizations the flexibility to hire the best talent regardless of location, remove silos and promote collaboration between teams, offices and locations.

Types of Remote Access

Cable broadband shares bandwidth across many users and, as a result, upstream data rates can be slow during high-usage hours in areas with many subscribers.

DSL (Digital Subscriber Line) broadband provides high-speed networking over a telephone network using broadband modem tech. However, DSL only works over a limited physical distance and may not be available in some areas if the local telephone infrastructure doesn't support DSL technology.

Cellular internet services can be accessed by mobile devices via a wireless connection from any location where a cellular network is available.

Types of Remote Access

Satellite internet services use telecommunications satellites to provide users internet access in areas where land-based internet access isn't available, as well as for temporary mobile installations.

Fiber optics broadband technology enables users to transfer large amounts of data quickly and seamlessly.

What is VPN?

A **virtual private network** (VPN) gives you 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. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

Desktop Sharing

- refers to the technologies that allow remote access of your computer or mobile device by another user on a separate device. Typically, the other user deploys a VNC (Virtual Networking Client) to view or even control your desktop from a remote location. You may also have heard desktop sharing being referred to as ‘screen sharing’ or ‘remote support’.

Privileged Access Management

- consists of the cyber security strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment. By dialing in the appropriate level of privileged access controls, PAM helps organizations condense their organization's attack surface, and prevent, or at least mitigate, the damage arising from external attacks as well as from insider malfeasance or negligence.

What are privileged accounts?

Standard user accounts have a limited set of privileges, such as for internet browsing, accessing certain types of applications (e.g., MS Office, etc.), and for accessing a limited array of resources, which is often defined by role-based access policies.

Guest user accounts possess fewer privileges than standard user accounts, as they are usually restricted to just basic application access and internet browsing.

A **privileged account** is considered to be any account that provides access and privileges beyond those of non-privileged accounts. A privileged user is any user currently leveraging privileged access, such as through a privileged account. Because of their elevated capabilities and access, privileged users/privileged accounts pose considerably larger risks than non-privileged accounts / non-privileged users.

Examples of privileged access used by humans:

Super user account: A powerful account used by IT system administrators that can be used to make configurations to a system or application, add or remove users or delete data.

Domain administrative account: An account providing privileged administrative access across all workstations and servers within a network domain. These accounts are typically few in number, but they provide the most extensive and robust access across the network. The phrase “Keys to the IT Kingdom” is often used when referring to the privileged nature of some administrator accounts and systems.

Local administrative account: This account is located on an endpoint or workstation and uses a combination of a username and password. It helps people access and make changes to their local machines or devices.

Examples of privileged access used by humans:

Secure socket shell (SSH) key: SSH keys are heavily used access control protocols that provide direct root access to critical systems. Root is the username or account that, by default, has access to all commands and files on a Linux or other Unix-like operating system.

Emergency account: This account provides users with administrative access to secure systems in the case of an emergency. It is sometimes referred to as firecall or break glass account.

Privileged business user: Is someone who works outside of IT, but has access to sensitive systems. This could include someone who needs access to finance, human resources (HR) or marketing systems.

Examples of privileged access used by humans:

Application account: A privileged account that's specific to the application software and is typically used to administer, configure or manage access to the application software.

Service account: An account that an application or service uses to interact with the operating system. Services use these accounts to access and make changes to the operating system or the configuration

SSH key: SSH keys are also used by automated processes.

Secret: Used by development and operations (DevOps) team often as a catch-all term that refers to SSH keys, application program interface (API) keys and other credentials used by DevOps teams to provide privileged access.

Vendor Privileged Access Management

This technology adds additional controls and processes to coveted privileged credentials in order to prevent them from being compromised while also limiting the damage if they ever are compromised.

What is cable broadband?

Cable broadband connects your home to a fibre cabinet in your area. However, instead of using copper wires, cable broadband uses coaxial cables to connect to the cabinet, giving you a much faster internet connection than the traditional copper phone line cables used for ‘superfast’ broadband connections (up to 60Mbps).

What is DSL?

Digital Subscriber Line (DSL) is a modem technology that uses existing telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. DSL provides dedicated, point-to-point, public network access. This DSL connection is typically between a network service provider (NSP) central office and the customer site, or on local loops created either within buildings or campuses.

What is Cellular internet service?

A cellular network or mobile network is a type of wireless connection facilitated by cellular towers. To have access to the cellular network, your mobile devices will have to be connected through a cellular provider.

What is Satelite

Satellite internet is wireless internet beamed down from satellites orbiting the Earth. It’s a lot different from land-based internet services like cable or DSL, which transmit data through wires. Since it’s the only internet service that’s available nationwide, satellite internet is often the only way to get online for many rural homes and businesses, although it does still come with a few disadvantages (more on that later).

Fiber optics broadband

Fiber optic Internet is an Internet connection that transfers data fully or partially via fiber optic cables. “Fiber” refers to the thin glass wires inside the larger protective cable. “Optic” refers to the way the type of data transferred – light signals.

Fiber optic internet is a complex technology that allows the transmission of information in the form of light rather than electricity. There are many pieces that make up this advanced technology, but two key components are optical fibers and the so-called “last mile” of the fiber-optic network.

VPN/ LAN/ WAN

Local Area Network - A LAN is a group of computers that are connected together locally. There is no access from an outside computer, but connections to the internet are permitted.

Wide Area Network - A WAN is a connection to and through the internet.

Virtual Private Network - A VPN is a secure connection from outside the LAN, through the internet. A VPN creates a tunnel that uses encryption algorithms to secure the information from outside to inside the network.

Remote access protocols?

Point-to-Point Protocol (PPP) enables hosts to set up a direct connection between two endpoints.

Internet Protocol Security (IpSec) a set of security protocols used to enable authentication and encryption services to secure the transfer of IP packets over the internet.

Point-to-Point Tunneling (PPTP) is one of the oldest protocols for implementing VPNs. However, over the years, it has proven to be vulnerable to many types of attack. Although PPTP is not secure, it persists in some cases.

Layer Two Tunneling Protocol (L2TP) is a VPN protocol that does not offer encryption or cryptographic authentication for the traffic that passes through the connection. As a result, it is usually paired with IPsec, which provides those services.

Remote access protocols?

Remote Authentication Dial-In User Service (RADIUS) is a protocol developed in 1991 and published as an Internet Standard track specification in 2000 to enable remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that was originally common to Unix networks that enables a remote access server to forward a user's password to an authentication server to determine whether access to a given system should be allowed. TACACS+ is a separate protocol designed to handle authentication and authorization, and to account for administrator access to network devices, such as routers and switches.

What is SSO?

Single sign-on (SSO) is a technology which combines several different application login screens into one. With SSO, a user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications.

- is often used in a business context, when user applications are assigned and managed by an internal IT team. Remote workers who use SaaS applications also benefit from using SSO.

Types of SSO

Security Access Markup Language (SAML): SAML is an open standard that encodes text into machine language and enables the exchange of identification information. It has become one of the core standards for SSO and is used to help application providers ensure their authentication requests are appropriate. SAML 2.0 is specifically optimized for use in web applications, which enables information to be transmitted through a web browser

Open Authorization (OAuth): is an open-standard authorization protocol that transfers identification information between apps and encrypts it into machine code. This enables users to grant an application access to their data in another application without them having to manually validate their identity—which is particularly helpful for native apps.

Types of SSO

OpenID Connect (OIDC): OIDC sits on top of OAuth 2.0 to add information about the user and enable the SSO process. It allows one login session to be used across multiple applications. For example, it enables a user to log in to a service using their Facebook or Google account rather than entering user credentials.

Kerberos: Kerberos is a protocol that enables mutual authentication, whereby both the user and server verify the other’s identity on insecure network connections. It uses a ticket-granting service that issues tokens to authenticate users and software applications like email clients or wiki servers.

Types of SSO

Smart card authentication: Beyond traditional SSO, there is also hardware that can facilitate the same process, such as physical smart card devices that users plug into their computer. Software on the computer interacts with cryptographic keys on the smart card to authenticate the user. While the smart cards are highly secure and require a PIN to be operated, they have to be physically carried by the user—running the risk of being lost—and they can be expensive to operate.

What is IPsec?

IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from.

L2TP

Layer 2 **Tunneling Protocol** (L2TP) is a computer networking protocol used by Internet service providers (ISPs) to enable virtual private network (VPN) operations. L2TP is similar to the Data Link Layer Protocol in the OSI reference model, but it is actually a session layer protocol.

A User **Datagram Protocol** (UDP) port is used for L2TP communication. Because it does not provide any security for data such as encryption and confidentiality, an encryption protocol such as Internet Protocol security (IPsec) is often used with L2TP.

This term is also known as **Virtual Dialup Protocol**.

PPTP

Point-to-point tunneling protocol (PPTP) is a set of communication rules that govern the secure implementation of virtual private networks (VPN), which allow organizations a method of extending their own private networks over the public Internet via "tunnels."

PPTP offers the following advantages:

Lower transmission costs: No additional service used, other than the Internet.

Lower hardware costs: Allows ISDN cards and modems to be separated from RAS servers, which results in fewer devices to purchase and manage.

Low administrative overhead: Administrators only manage the remote access server (RAS) and user accounts, rather than managing different hardware configurations.

Enhanced security: PPTP connection is encrypted and secured over the Internet and works with other networking protocols, like IP, Internetwork Packet Exchange (IPX) and NetBIOS Extended User Interface (NetBEUI).

SLIP

Serial Line Internet Protocol (SLIP) is a simple protocol that works with TCP/IP for communication over serial ports and routers. They provide communications between machines that were previously configured for direct communication with each other.

SLIP frame has a very simple format, comprising of payload and a flag that acts as an end delimiter. The flag is generally a special character equivalent to decimal 192. If this flag is present in the data, then an escape sequence precedes it, so that the receiver does not consider it as the end of the frame.

PPP

The **Point-to-Point Protocol** (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP is comprised of three main components:

A method for encapsulating multi-protocol datagrams.

A **Link Control Protocol** (LCP) for establishing, configuring, and testing the data-link connection.

A family of **Network Control Protocols** (NCPs) for establishing and configuring different network-layer protocols.

RAS

Remote Access Server (RAS) is a type of server that provides a suite of services to remotely connected users over a network or the Internet. It operates as a remote gateway or central server that connects remote users with an organization's internal local area network (LAN).

- includes specialized server software used for remote connectivity. This software is designed to provide authentication, connectivity and resource access services to connecting users.

- is deployed within an organization and directly connected with the organization's internal network and systems. Once connected with a RAS, a user can access his or her data, desktop, application, print and/or other supported services.

Remote access server is also the name of a Windows 2000 Server component that provides enterprise IT infrastructure access to remote users.

3 forms of dialin permission:

No call back: Gives the user permission to dial in to the network using the RAS server.

Set by caller: Terminates the connection after the user dials in to the RAS server. The RAS server dials the user back at the phone number the user specifies. This function is called callback.

Preset to: Also uses callback, but the server always calls the user back using a phone number preset on the server.

RDP

Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client users, devices and a virtual network server. It enables a remote user to add a graphical interface to the desktop of another computer. Based on the ITU-T.120 protocol set, RDP is compatible with multiple types of local area network (LAN) protocols and topologies.

RDP supports up to 64,000 separate data channels with a provision for multipoint transmission.

RDP provides support for the following services:

- Mouse and user keyboard data encryption
- Audio, printer, port and file redirection
- Clipboard sharing between a remote server and a local client
- Remote desktop applications run on client machines using a remote desktop connection
- Remote Desktop Services (RDS), which provides RDP functionality via Windows 2008 R2 with Service Pack 1 (SP1)

TACACS

Terminal Access Controller Access Control System (TACACS) is an authentication protocol used for remote communication with any server housed in a UNIX network. TACACS provides an easy method of determining user network access via remote authentication server communication. The TACACS protocol uses port 49 by default.

- uses allow/deny mechanisms with authentication keys that correspond with usernames and passwords. Cisco, which designed and launched the TACACS protocol, is also its owner.