PROTECTING REMOTE CONNECTIONS

The networks that organizations create are seldom used only by people at that location. When connections are made between one network and another, the connections are arranged and managed carefully. Installing such network connetions requires using leased lines or other data channels provided by common carriers, and therefore these connections are usually permananet and secured under the requirements of a formal service agreement.But when individuals-whether they be employees from home, contract workers hired for specific assignments, or other workers who are traveling-seek to connect to an organization‘s network(s), a more flexible option must be provided. In the past, organization‘s provided these remote connections exclusively through dial-up services like Remote Authentication Srvice (RAS).Since the Internet has become more wide-spread in recent years, other options such as Virtual Private Networks (VPNs) have become more popular.

Dial-Up

Before the Internet emerged, organizations created private networks and allowed individuals and other organization‘s to connect to them using dail-up or leased line connections. The connections between company networks and the Internet use firewalls to safeguard that interface. Although connections via dial-up and leased lines are becoming less popular they are still quite common. And it si a widely held view that these unstructured, dial-up connection points represent a substantial exposure to attack. An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points. A war-dialer is an automatic phone-dialling program that dials every number in a configured range (e.g., 555-1000 to 555-2000), and checks to see if a person , answering machine, or modem picks up. If a modem answers, the war dialer program makes a note of the number and then moves to the next target number. The attacker then attempts to hack into the network via the identified modem connection using a variety of techniques. Dial-up network connectivity is usually less sophisticated than that deployed with internet connections. For the most part, simple username and password schemes are the only means of authentication. However , some technologies such as RADIUS systems, TACAS, and CHAP password systems, have improved the authentication process, and there are even systems now that use strong encryption. Authenticating technologies such as RADIUS, TACAS, Kerberos, and SESAME are discussed below.

RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up connection. Typical dial-up systems place the responsibility for the authentication of users on the system directly connected to the modems. If there are multiple points of entry into the dial-up system, this authentication system can become difficult to manage.

The **RADIUS (Remote Authentication Dial-In User Service)** system centralizes the management of user authentication by placing the responsibility for authenticating each user in the central RADIUS server. When a remote access server (RAS) receives a request for a network connection from a dial-up client, it passes the request along with the user's credentials to the RADIUS server. RADIUS then validates the credentials and passes the resulting decision (accept or deny) back to the accepting remote access server. Figure 6-15 shows the typical configuration of an RAS system.

Similar in function to the RADIUS system is the Terminal Access Controller Access Control System (TACACS). TACACS is another remote access authorization system that is based on a client/server configuration. Like RADIUS, it contains a centralized database, and it validates the user's credentials at this TACACS server. There are three versions of TACACS: TACACS, Extended TACACS, and TACACS+. The original version combines authentication and authorization services. The extended version separates the steps needed to provide authentication of the individual or system attempting access from the steps needed to authorize that the authenticated individual or system is able to make this type of connection. The extended version then keeps records that show that the action of granting access has accountability and that the access attempt is linked to a specific individual or system. The plus version uses dynamic passwords and incorporates two-factor authentication.

Securing Authentication with Kerberos

Two authentication systems can be implemented to provide secure third-party authentication: Kerberos and Sesame. Kerberos-named after the three-headed dog of Greek mythology (spelled Cerberus in Latin), which guarded the gates to the underworld-uses symmetric key encryption to validate an individual user to various network resources.

Kerberos keeps a database containing the private keys of clients and servers-in the case of

a client, this key is simply the client's encrypted password. Network services running on servers in the network register with Kerberos, as do the clients that use those services. The Kerberos system knows these private keys and can authenticate one network node (client or server) to another. For example, Kerberos can authenticate a user once-at the time the user logs in to a client computer-and then, at a later time during that session, it can authorize the user to have access to a printer without requiring the user to take any additional action. Kerberos also generates temporary session keys, which are private keys given to the two parties in a conversation. The session key is used to encrypt ali communications between these two parties. Typically a user logs into the network, is authenticated to the Kerberos system, and is then authenticated to other resources on the network by the Kerberos system itself.

Kerberos consists of three interacting services, all of which use a database library:

1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.
2. Key Distribution Center (KDC), which generates and issues session keys.
3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services. In Kerberos a ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive service. The ticket consists of the client 's and network address, a receive services. The ticket validation starting and ending time ,and the session key, all, encrypted in the private key of the server from which the client is requesting services.

Kerberos is based on the following principles:

- The KDC knows the secret keys of all clients and servers on the network.
- The KDC initially exchanges information with the client and server by using
- these secret keys.

- Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications between the client and KDC, the server and KDC, and the client and server.
- Communications then take place between the client and server using these Temporary session keys.

Kerberos may be obtained free of charge from MIT at *http://web.mit.edu/is/help/* Kerberos/, but if you use it, be aware of some fundamental problems. If the Kerberos servers are subjected to denial-of-service attacks, no client can request services. If the Kerberos servers, service providers, or clients' machines are compromised, their private key information may also be compromised.

Sesame

The Secure European System for Applications in a Multivendor Environment (SESAME) is the result of a European research and development project partly funded by the European Commission. SESAME is similar to Kerberos in that the user is first autherticated to an authentication server and receives a token. The token is then presented to a privilege attribute server (instead of a ticket granting service as in Kerberos) as proof of identity to gain a privilege attribute certificate(PAC).The PAC is like the ticketing in Kerberos;however, a PAC

conforms to the standards of the European Computer Manufacturers Association (ECMA) and the International Organization for Standardization/International Telecommunications Union (ISO/ITU- T). The balances of the differences lie in the security protocols and distribution methods used. SESAME uses public key encryption to distribute secret keys.

SESAME also builds on the Kerberos model by adding additional and more sophisticated access control features, more scalable encryption systems, as well as improved manageability auditing features, and the delegation of responsibility for allowing access.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf