Increasing Network Security

Introduction

Network and data security has been a growing concern in many organizations. With the emergence of wireless networking, security preemptives have been primarily focused on mitigating the man-in-the-middle attack and general weaknesses inherent in earlier 802.11 standard. Security threats in networks, however, are not just an issue with wireless networks, but also wired. The purpose of this article is to look into areas of security concerns beyond the wireless and provide advice on how they can be mitigated.

Is there a need for organizations to look into network security?

Every network in an organization is subject to security risks. Unauthorized access, eavesdropping of network data, and network tampering by authorized users, are some of the many security risks faced by network administrators everyday.

In order to understand the importance of network security, it is a good practice to look into the extent of damages that can occur when an organization's network is not protected. Take the example of damages that can be done to an organization by a user on the network. According to a press release by insurance broker Assurex Global, US defense contractor Lockheed Martin crashed its e-mail system for six hours after a disgruntled employee sent sixty thousand personal e-mail messages to coworkers, complete with a request for an electronic receipt. In this particular instant, Lockheed Martin, which posts forty million e-mails a month, was forced to fly in a Microsoft rescue squad to repair the damage done by one employee.

In a less serious case also mentioned in the press release, a Forbes Inc. computer technician deliberately caused five of the publisher's eight network servers to crash because of his termination from a temporary position. The result was a complete erasure of all information on the affected servers with no restoration possible. This single sabotage caused Forbes to shut down its New York operations for two days, costing the company losses in excess of US$10,000.

Securing Network Access

From the two scenarios described above, it is clear that network security is of utmost importance to any organization. If measures have been taken to prevent security breaches, the cost of damages can be substantially reduced. In the case of the Forbes scenario, if the network manager immediately terminates the staff's access to the network, the staff would not have been able to authenticate and gain access to the organization's servers or data, and sabotage would not have been possible.

Network authentication is the first step of defense in securing network access from intruders. It is the process by which someone or something must first be identified through mechanisms such as user name and password or PIN, signature certificate, public and private key infrastructure, or biometric devices, before authorized access to network is possible. In the case of private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. In networks that allow remote clients' access, authentication is also necessary in order to protect the network from unauthorized access.

To build an infrastructure that provides network access security, a managed switch that supports RADIUS, TACACS+, SSL, SSH, Access Control List, Virtual LANs, 802.1x, and port security, is highly recommended. A managed switch has more capabilities than unmanaged switch and includes additional managed features which may vary between manufacturers and models. A switch is a network device that channels incoming data from various input ports to specific output port of its intended destination. In order to appreciate the capabilities offered by different managed switches, this article will attempt to explain and illustrate some of the extended features mentioned above.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server in order to authenticate remote users. Once the remote users are authenticated, authorization for their access to the requested system or service is granted.

When a user wishes to access the company's network or services, the workstation will make a request for connection to the network. The managed switch acts as a RADIUS client authenticator and pass on the user information to the designated RADIUS server. The RADIUS server containing the centralized user profiles database identifies the requester, authenticates the user, and returns the information to the managed switch, which then authorizes user access to the requested service.

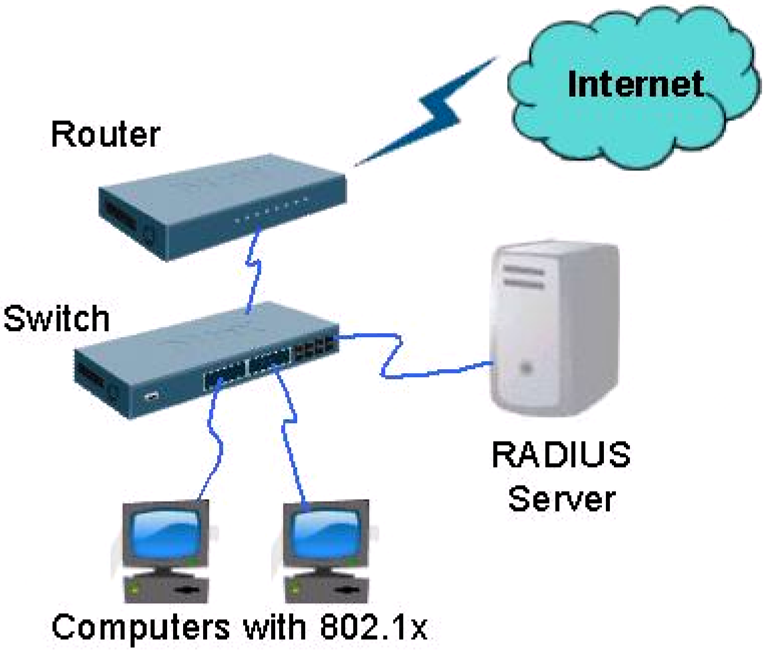

Diagram 1: Topology of Radius Network

TACACS+

Terminal Access Controller Access Control System (TACACS) is an authentication protocol that provides similar functions as RADIUS. Unlike RADIUS that uses the User Datagram Protocol, however, TACACS+ uses the Transmission Control Protocol (TCP) which provides greater reliability. RADIUS combines the authentication and authorization in a user profile to provide a single process access and connectivity while TACACS+ separates the two operations to provide greater complexity using the triple A model of authentication, authorization, and accounting (AAA). Authentication determines whether requester is allowed to access the network, authorization determines what user is allowed to do, and accounting tracks what the user do and when it is done.

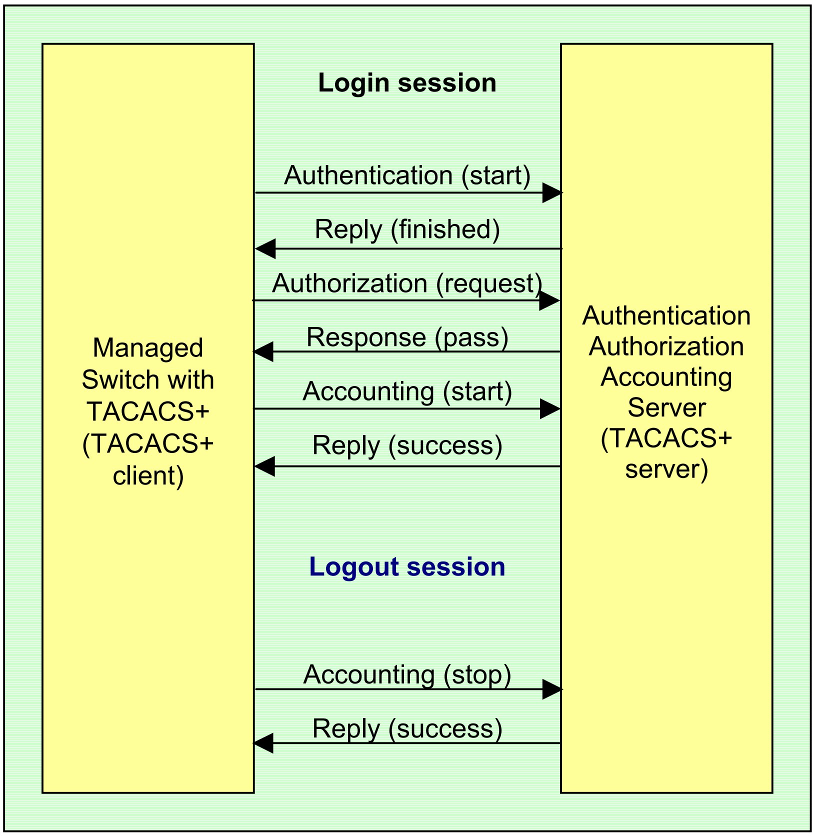

Diagram 2: TACACS+ Authentication and

SSL

Secure Sockets Layer (SSL) is a popular protocol used to perform secure transactions and message transmission on the Internet. Web sites such as those providing products for purchase or on-line banking services often use SSL. To establish a secure SSL session at a web site, users must first obtain a SSL digital certificate. A SSL digital certificate is an electronic file that uniquely identifies individuals and servers. Digital certificates allow SSL clients (web browsers) to authenticate the server prior to establishing a SSL session and are typically signed by an independent and trusted third party to ensure their validity. The ‘signer’ of a digital certificate is known as a Certification Authority (CA).

Security such as confidentiality, message integrity, and authentication is provided by SSL through the use of cryptography, digital signatures, and certificates. Using SSL, managed switches can be implemented to provide protection to secure data transmission between the remote clients and the servers.

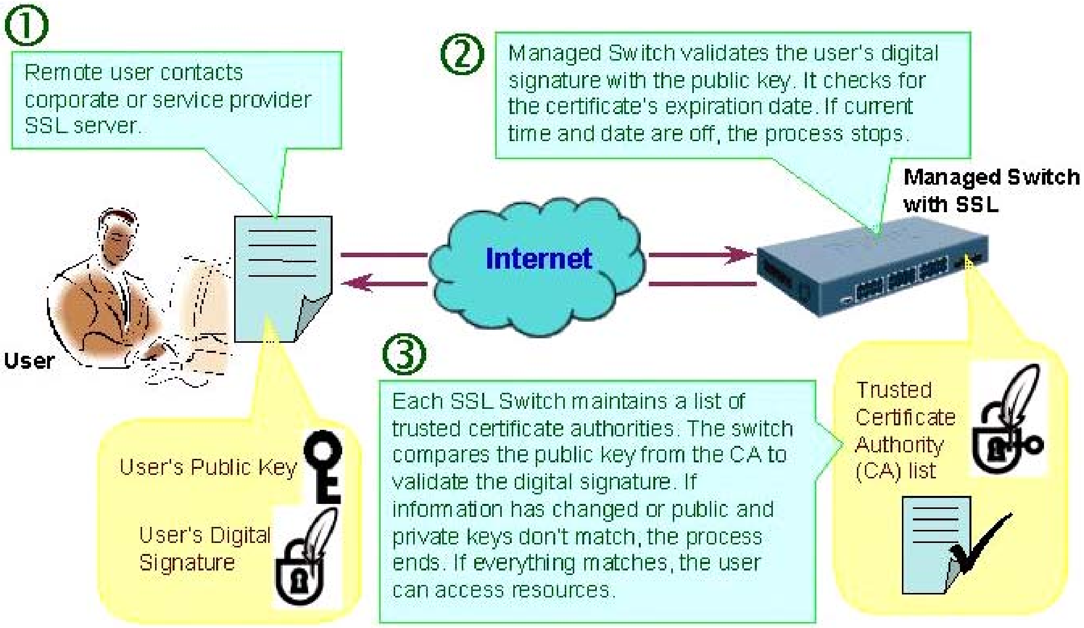
①
Remote user contacts corporate or service provider SSL server.
②
Managed Switch validates the user's digital signature with the public key. It checks for the certificate's expiration date. If current time and date are off, the process stops.
Managed Switch with SSL
Internet
User
③
Each SSL Switch maintains a list of trusted certificate authorities. The switch compares the public key from the CA to validate the digital signature. If information has changed or public and private keys don't match, the process ends. If everything matches, the user can access resources.
User's Public Key
User's Digital Signature
Trusted Certificate Authority (CA) list

Diagram 3: SSL Authentication

SSH

Secure Shell (SSH) is a Unix based shell command protocol for secure login and command execution on a remote computer. SSH is widely used by network administrators to control web and other servers remotely. Like SSL, SSH uses digital certificates and cryptography encryption to grant authentication and connection to the remote user. Managed switches may be incorporated in SSH network environment to provide extended protection in securing data transmitted between client/server.

Summary

There are many other areas of network security that are not covered in this article, such as Access Control List and Virtual LAN, which are also supported by various managed switches. Today, with key concerns of many organizations focused on network and data security, there is a need for network administrators and managers to build infrastructures that will provide secure networks. Whether it be remote access or access over the Internet, there are real threats that can harm private networks in organizations. Using protocols such as RADIUS, TACACS+, SSL, SSH, and switch management, network security can be significantly enhanced to reduce these threats.

- End -