Global Information Assurance Certification Paper

Christopher Harper
GSEC Version 1.2e

Securing critical network resources with Two-Factor Authentication.

Introduction

In today's corporate environment, the need exists to ensure that only authorized individuals gain access to critical devices and services. With the availability of "ready to use" sniffers and password cracking tools, the standard username / password combination is no longer sufficient. A strong authentication system can be a successful replacement for traditional usernames and passwords.

This paper explores how several key platforms within an organization can benefit from using a strong authentication system. The examples are given with the intent of examining how a single solution can be used across multiple systems that are potentially very insecure with respect to authentication.

Three Examples

VPN access (a technology that seemingly everyone is deploying these days) gives an outsider access to the internal network. Think of the VPN as a tool which allows anyone to connect a cable into your internal network from anywhere in the world. The only thing (typically) authorizing this access is a username and password combination. With broadband Internet access, an authenticated VPN user can use the network in the same manner in which a locally connected user can. A well-implemented VPN involves proper authentication, strong encryption and good host security on the remote machines including virus protection and personal firewalls. This document speaks to the authentication issue only.

The need for strong authentication is not just for external access to network services. In a typical network, administrators remotely access routers, switches and even firewall devices using telnet. As a matter of function, the username and password is passed in clear text (as well as the entire session). Any curious observer using a packet sniffer could capture the password and use it to make his or her own changes to the router wreaking general havoc, or make serious modifications to the firewall to accommodate their Napster or PCAnywhere access.

Strong authentication can also be used to secure access to Windows domain controllers & individual domain or local accounts. Password cracking tools make it easy to obtain administrator access. An enterprising insider could find many interesting ways to exploit his newfound access.

What is strong authentication?

If weak authentication is a static password, which rarely changes and must be memorized by the user, strong authentication is a technology that dictates frequently changing, often one-time, passwords that are not memorized (or written down). This discussion uses as an example a very popular type of strong authentication. It is a product offered by RSA Security called SecurID. The SecurID system is an example of two-factor authentication. Some other products, which accomplish the same goals as this product, are as follows:

- Axent - Defender
- Datanet Systems - CryptoCard
- ActiveCard - ActiveCard One

The SecurID system involves the use of a hardware device that generates a component of the password that changes very often – typically every minute. This technology also dictates that the user memorize a portion of the password. Hence the two factors – TOKENCODE and PIN = PASSCODE. The hardware device is synchronized with a server that is typically located behind a firewall. Both devices produce the same code at any given moment. This server communicates with the device to which the user is to be authenticated to (i.e. router or firewall), and determines whether the credentials which the user presented are valid. The ACE server then informs the access device or host as to the validity of the user. The ACE Server will also detect if an intruder is trying to guess PINs, or TOKENCODEs, or replay valid PASSCODEs (the PIN and TOKENCODE combination) and take appropriate actions such as disabling the user account or asking the user for additional information.

A detailed technical explanation or implementation guide of the SecurID system is outside of the scope of this document, however here are the basic components and how they interact:

Token Device – Typically a hardware device containing a processor, which executes the proprietary algorithm developed by RSA (formerly Security Dynamics). This algorithm computed against the Seed (unique to each token) produces a unique 6 digit hash every 60 seconds. This number is known as the TOKEN-CODE.

PIN – This is a code which is memorized by the end user. This PIN will be combined with the hash displayed on the token to produce the password (PASS-CODE) for access.

Ace Server – This is the server component which contains the administrative utilities, an encrypted user and token database, audit logs, and configuration data. The database stores the unique Seed for each token device. This is used when producing the hash which is displayed on the token. The Ace server and token are synchronized such that the hash displayed on the token is known by the server at any given interval. The Ace server also stores the PIN for each end user.

Ace Agents – This is software which exists in many forms and lives on a device which will be authenticated to. This would be a firewall, a RAS device, a VPN device, etc. This agent securely passes the credentials presented by the user to the Ace Server for

verification. Ace determines whether the PIN and token-code combination (PASS-CODE) is valid, and returns an answer to the agent.

The SecurID system has many tools and processes which allow for lost or destroyed tokens, forgotten PIN numbers, creation of new PINs, and token deployement etc. For the purposes of this writing, it is important to understand that SecurID is a scalable, reliable, proven solution for two-factor authentication.

Which resources should be protected?

When determining which resources are to be protected by a strong authentication system, it is important to determine which systems in your environment are most susceptible to password compromise or employ the weakest password schemes. It is also important to factor in the significance of the system to be protected to the overall security of the organization. Ask yourself "What would happen if an unauthorized user or person gained access to this resource?"

Other considerations when deciding where two-factor authentication is appropriate:

- The administrative overhead – What is involved on behalf of the security team? – the help desk?
- The types of users who will be accessing the system – are they employees of your organization or a customer base?
- The cost of deployment
- The cost of maintenance

Deploying a large-scale token solution to users outside of your organization would obviously dictate a larger administrative burden, however, a bank could instill a high level of confidence in their high profile customers with such a deployment.

Many systems can benefit from using a strong authentication mechanism. Operating system access including Windows, Unix, and IOS, remote access devices and software, and web servers are included. In this paper, we examine three such technologies which exist in many organizations: A Check Point client VPN (Virtual Private Network), Cisco routers and firewalls, and local Administrator access to a Windows Server.

In the many environments where ACE is deployed for a single purpose, such as remote access, other components are often ignored. Deploying strong authentication across several platforms which can benefit from it, can provide a higher level of security, and help with further cost justification of the authentication system itself.

Access to a VPN (Virtual Private Network)

A very common and appropriate use of strong authentication is in a VPN environment. When a VPN user is authenticated, they often have access to most if not all of the network resources available. Weak passwords on VPN's make Swiss cheese of the

firewall. VPN's without additional authentication provide for encryption of traffic from a trusted outside host to the internal network. If an unauthorized user is accessing the network over a VPN, it just means that the unauthorized traffic is encrypted. Strong authentication can all but insure that the end user is who they claim to be.

Achieving SecurID functionality on an existing Check Point VPN is relatively straightforward. It involves accomplishing the following:

Establishing a Hybrid Mode configuration – This allows for options with regard to authentication to an otherwise purely IPSEC VPN configuration. Checkpoint has this process clearly documented.

Establishing connectivity between the firewall and the Ace Server – The Ace Agent is integrated into the installation of VPN-1 / Firewall-1, so this involves defining the firewall on the Ace Server and testing authentication.

Define a generic user on the firewall – VPN-1 allows the creation of a special user which can be used as a passthrough to an external authentication system. Defining "generic*" as a SecurID user, will allow all usernames to be passed to the Ace Server. This keeps the security administrator from creating two user databases. Using "generic* does have limitations, specifically, when a username is defined in the database it is not passed to generic*.

In practice, users will be prompted for their username and a valid PASSCODE (PIN+TOKENCODE) when attempting to gain access to the network via the VPN. Because the user must possess both the token and the memorized PIN, the administrator can be assured that the user is whom he/she claims.

Access to Cisco network equipment

Another perfect fit for strong authentication are Cisco switches and Pix firewalls. More often than not, Telnet is used to access and manage these devices and a single password is used for all of the equipment. In addition, this password rarely changes and is used by several administrators. Using strong authentication to identify users who gain access to these systems can improve overall security of an organization.

Though adding strong authentication does nothing to make Telnet more secure (the passwords would still travel the wire in the clear), it would individualize the passwords and they would change every minute. This makes sniffing the passwords less effective.

Implementing SecurID authentication to Cisco equipment is done using the Radius protocol. An ACE server can be configured to work as a RADIUS server, to allow for protection of devices that do not have built in support for ACE. Devices such as PIX can communicate with RADIUS servers for authentication.

Sample configurations are readily available, but what should be achieved is the control of authentication to the device. Configure access through the appropriate ports to use RADIUS authentication. (This is done mostly using aaa commands.) There are a few limitations when using this configuration. Such functions as "NEW PIN mode" and "NEXT TOKENCODE mode" are not supported when connecting to the device, which is typical in non-ACE agent mode.

One additional note regarding Telnet – the PIX OS v5.2 introduced support for SSH which allows access to the PIX through an encrypted tunnel. The SSH authentication can be done using RADIUS, making for a very secure connection to the PIX for remote management. Access from outside of the internal network can also be provided using the IRE VPN client in conjunction with strong authentication.

Administrative access to Windows servers

RSA SecurID can be used to protect local login access to the Windows 2000 (and Windows NT) desktop. There is a replaceable component of the Windows login process known as the GINA (Graphical Identification and Authentication DLL). The RSA Ace Agent replaces this DLL with SDGINA which allows strong authentication to be required for local (interactive) login to Windows servers. This would be appropriate for an environment where servers are physically secured in a computer room, but access to the computer room is not limited to administrators of the Windows servers. A non-administrator would no longer be able to "shoulder surf" for the administrator password.

In practice, a local group is configured with users who should be authenticated by SecurID. Users who "ctrl-alt-del" at the server keyboard are prompted for a valid Windows username and password. If they are found to be a member of the above group, they are prompted for a username and PASSCODE. Users who are not defined for strong authentication still logon using traditional methods. The ACE Agent will query the ACE Server and if the information supplied by the user is valid, they are allowed to login. It should be noted that this form of authentication is not appropriate for any accounts which act as the logon for a system service, as there is no means to provide the interactive authentication that ACE requires.

Of course, the ACE agent needs to be loaded on all servers and desktops where this functionality is required.

An optional failsafe password can be configured for use in the event of network problems which prevent communication with the ACE Server.

Using the system in this way would dictate that all administrators use the SecurID token when accessing the Windows servers. Through domain or active directory structuring, an enterprise can provide strong authentication services to all of it's users within an organizational unit and therefore increase the security posture of this unit.

Summary and final thoughts

As with any successful security implementation, planning, testing, piloting, documenting, and training are all vital to the process. The above descriptions are simply the high-level steps for implementation.

Deployment of a system such as this is not without shortcomings. In some configurations, the user may be given less than adequate information about the reason for a failed login. In addition, policy and procedures must be developed which address initial distribution of tokens, how to handle forgotten PINs and lost tokens, and the security weaknesses of software tokens. Also most hardware tokens have a "life" afterwhich they are no longer functional and must be replaced.

Strong authentication isn't a cure-all. Many other things are important such as encryption, access control, and host security. One of the most difficult challenges in security today is the password dilemma. Traditional passwords and their management are insufficient in terms of user identification. A two-factor authentication system such as the ones mentioned above are one answer to this problem. However, just as a firewall can't completely secure your network, neither can strong authentication. Security is a mindset that must be applied across the enterprise and adopted by individuals at all levels in the organization. But for some systems (such as the ones mentioned above and others), it can be very successful.

References:

"Cisco Security Associate Design Guide for RSA SecurID". Oct 4 2000. URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/csap/sarsa_rg.htm

"Cisco Remote Access Servers and Pix Implementation Guide". URL: http://www.rsasecurity.com/support/guides/imp_pdfs/Cisco_Remote_Access_Servers_and_Pix_FW.pdf

DiPietro, Joe. "Hybrid Mode IKE for SecuRemote Authentication". V1.4. Sept 6 2000. URL: http://support.checkpoint.com/kb/docs/public/securemote/4_1/pdf/hybrid-2-10.pdf

"RSA ACE/Agent v 1.1 for Windows 2000 Administration Guide". V1.0.

Welch-Abernathy, Dameon D. "Configuring SecurID-based Authentication". Dec 23 1999. URL: http://www.phoneboy.com/faq/0361.html

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS