Global Information Assurance Certification Paper

SecurID: A Secure Two-Factor Authentication
Steven Krychiw
February 28, 2001

INTRODUCTION

We are constantly being bombarded with media headlines informing us about wide spread hacking, viruses and data loss. Today companies need to protect their data. The need for strong password authentication is a start. The antiquated way of relying on single-factor passwords for protection is insecure. Company losses from computer crimes are rising (Table 1). A security breach could cause havoc and depending on your type of business, it could prove deadly. Information security is necessary and password fraud is partly to blame.

TYPE of CRIME	% Victimized	Avg. loss
Unauthorized insider access	55%	$143,000
Theft of Proprietary information	26%	$1,848,000
Telecom fraud	17%	$27,000
Financial fraud	14%	$1,471,000
System penetration by an outsider	31%	$103,000
Sabotage of data or networks	19%	$164,000
Denial of Service	32%	$116,000
Insider abuse of Net access	97%	$93,500
Telecom eavesdropping	13%	$76,500
Virus Infection	90%	$45,500
Active wiretapping	2%	$20,000
Laptop theft	69%	$87,000

TABLE 1. The above statistics are derived from the 1999 research conducted by the Computer Security Institute and the FBI. A total of 521 companies, organizations and educational institutions were surveyed.

The Single-Factor Password

A Corporate Security policy must be created and adhered to. If your company already has a Security Policy in place and if it is being followed, you reached the first important step in securing your information. Your current Security Policy should include a section on password creation and format. The single-factor password provides minimum protection and your password policy should be adjusted accordingly. You should consider the format and length of the password, and the frequency of changing them. Single-factor authentication is when your users rely on a string of characters to log onto their network device, domain or server. One problem is that this same password is used over and over again, every day. For whatever reason your users come up with, either because they find it easier not to constantly change their password or they don't want to forget them, they will usually keep the same password until asked to change them. Hopefully your administrator has setup the passwords to expire to at very least, every 3 months. Normally end users can remember their password. However, most users have a

tendency to write them down and post them on a sticky next to their computer. This unsecured practice can lead to unauthorized insider access. Another security risk of a single-factor password is that they are transmitted on your network in clear text.

Clear text can easily be captured on your network. There are several network security-monitoring tools available that can monitor and capture your network data. Network analyzers can be a software product run from an existing system or a dedicated hardware device. They can be active or passive. Passive, meaning they do not need to transmit data as part of their monitoring function. They can hang on your network without being detected while collecting clear text passwords and login ids. Passwords are not the only thing at risk. There are other services that can easily be snooped because they communicate in clear text. They are FTP, Telnet, SMTP, HTTP and IMAP. While no single security product can eliminate every risk, the secure two-factor password authentication SecurID card from RSA Security Inc. can help verify that the user who is logging in is not an imposter.

The SecurID Solution

RSA Security Inc located in Bedford Mass. provides several products for network security solutions. They provide RSA BSAFE for encryption requirements, RSA KEON for Public Key Infrastructure and RSA SecurID, which uses a token-based product for strong two-factor password authentication so companies can access their protected computer systems and resources while preventing unwanted intrusion.

The rate of new remote access solutions is increasing. New installations of VPN's, encryption devices and RAS servers can provide information protection. But you still have to protect against the one thing attempting to get at your resources, *the users*. This is where SecurID comes in.

SecurID is a good choice for securing network access. RSA's strong two-factor authentication is simple and secure. The first is based on something you know, which is a Personnel Identification Number (PIN). This is a 4-8 digit number (depending on how the administrator configures it) is kept private. The second factor relies on something the user possesses, the SecurID token. The numeric token code on the card changes every 60 seconds. This token code changes in conjunction with the ACE/Server database. The combination of the PIN + Tokencode = the Passcode. Because the token code changes every 60 seconds, the passcode is unique to each access session requested.

The SecurID Card

The SecurID Token card (Figure 1) contains a microprocessor, an accurate clock that uses Universal Coordinated Time (UCT), a battery, an LCD capable of displaying up to an 8-digit number and a unique 64-bit seed value. The token card is initialized with a 64-bit seed value. Every 60 seconds the microprocessor runs the RSA patented algorithm

combining the seed value and UCT time to generate a random number. The ACE/Server also knows the seed value associated to that card. When they both calculate at the same standard of time (UCT), the numbers they calculate should match.

Figure 1

This card comes in several forms. Two of the more popular forms are a credit card sized token card made from tempered steel and the hard plastic waterproof FOB that can be attached to your key chain. Two newer styles include a smart card and a software application that runs on Palm pilots. They all run a RSA's proprietary algorithm for hashing and encrypting the token code.

RSA's ACE/Server, the authentication engine, provides access security for several platforms in one fairly simple package. The ACE/Server can be installed on Windows NT, and UNIX based platforms from SUN Microsystems, IBM and HP. Depending on the server's hardware setup, a single ACE/Server can protect 100,000 users. The ACE/Server failover authentication works well when configured in a Master/Backup setup. When the Master goes offline, the backup server will authenticate users and store entries in the log. When the Master comes back online, the databases reconcile with each other. The communication between Master and Backup is done through TCP. The data stream between them is encrypted and the key changes every 10 minutes.

The ACE/Server authenticates both local and remote users. Authenticating users who want to access your network devices is accomplished by installing the ACE/Server Agent on your network devices (Figure 2). The ACE/Server communicates with the agents with a combination of UDP and Unicast. Their packets are encrypted as well. During the initial ACE/Server and Agent connection, a node secret is set between them. It doesn't matter if you have users connecting from VPNs, dial-ups, Intranets or Extranets. When those devices initiate an authentication request to gain access, the passcode request is encrypted and sent to the ACE/Server. Most market leading products have a built in two-factor authentication compatibility.

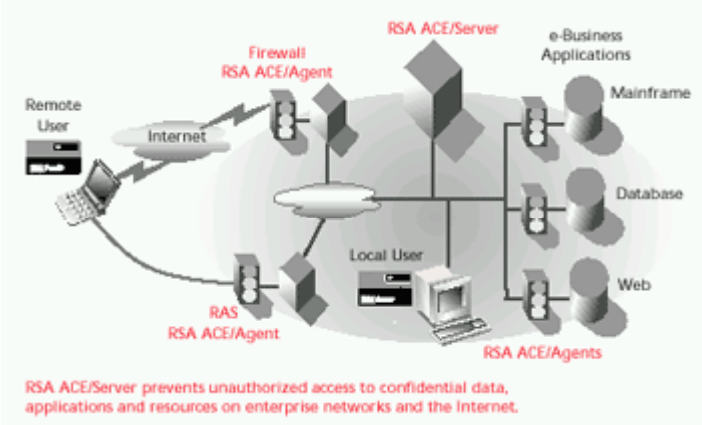

Figure 2

Token-based security systems have been around for about 10 years. The interface nicely with RADIUS (Remote Authentication Dial-In User Service) and TACACS(Terminal Access Controller Access Control System) protocols. There are over 100 RSA Security partners who have built in agents to support SecurID two-factor authentication in their products.

The ACE/Server allows administrators to create reports based on login attempt, users, groups and agents. These entries are automatically generated and added to a log file for auditing purposes. Consideration should be taken with your Security Policy and should include procedures on how you to collect network logs. Network auditing is just as important. Auditing consumes administration hours but is needed.

Conclusion

Two-factor password authentication is not the ultimate solution. It does provide very good authentication and authorization. It is still only one piece of your total security package. Limiting access to authenticating users is an important factor in protecting your enterprise information and resources. RSA's ACE/Server secure two-factor authentication offers a cost-effective way to minimize losses due to password fraud and unauthorized access.

Works Cited

RSA. "Strong Enterprise User Authentication: RSA ACE/Server" URL: http://www.rsasecurity/products/securid/whitepapers/ace4/ace4.pdf

Shostack, Adam. "Apparent Weakness in the Security Dynamics Client/Server". October 1996, URL: http://www.homeport.org/~adam/dimacs.html

Unknown. "Securing the Information Age... Minute by Minute". URL: http://www.oga.co.th/syncom/securid/security/security.html

Breton, Chris. “Mastering Network Security”. SYBEX Inc. 1999.

O’Shea M. Timothy. “A Token of Our Esteem”. Network Computing. September 1999.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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 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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor