GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

SAN INSTITUTE

GIAC SECURITY ESSENTIAL CERTIFICATION

PRACTICAL ASSIGNMENT

Not all Two-factor Authentication Methods are Alike

By

John M. Black III
1/30/2002

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Contents:

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Abstract

Cyberspace requires authentication. Password authentication schemes can be compromised in numerous ways, leading companies to look for two-factor authentication. True two-factor authentication requires that the factors and the way in which they are compromised must be independent of one another. If so, then the level of confidence can be the multiple of their success rates, generating "strong" authentication. Some vendors have stronger two-factor authentication schemes than others.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Two-Factor Authentication:

Someone is known to you when you recognize their face. In cyberspace, since you cannot see the person at the other end of a computer cable, you need another method to identify someone. In cyberspace, there are a number of methods to do this and the process of confirming the identity of someone is called "authentication." But not all of these methods equally prove that the person on the other end is authentic. Some methods are more reliable than others.

All cyberspace authentication methods are based on three things about the person at the other end: something the person knows, something the person possesses, or something about the person. For example, the person at the other end of the cable may know a password that when sent gives you confidence that they are whom they say they are. Or the person may have a chip card -- "something they possess" -- that verifies their identity. Lastly, the person may send you something about their person, such as a thumbprint, using biometric technology.

More than one method can be used to authenticate someone cyberspace. If just one method is used, such as a password, it is called "single factor" authentication. When two methods are combined, such as passwords and smart cards, it is said to be "two-factor" authentication. When three are combined it is said to be "three-factor" authentication. Adding each one of these independent methods raises the level of confidence that the person out in cyberspace is who they say they are.

Joint Probability & Independence:

In adding additional factors, the probability of authenticating the person as genuine increases by a multiple of each factor's frequency of success. Success is defined as the probability that the authentication method has not been compromised. If the probability that a static password has not been compromised is 50% and the probability that a chip card has not been broken into is .01%, then the probability that the person is a fake using both methods to authenticate is 50% (password) times .01% (smart card) or just .005%. This is the joint probability of both methods being compromised.

In the example above, two-factor authentication dramatically reduced the probability of compromise from 50% to just .005%. This is one reason why two-factor authentication is said to be "strong" authentication. Both factors together are stronger than each alone, as a result of this multiple effect.

Note to use multiplication to calculate the probability of compromise, the authentication methods and the means that they are compromised must be independent of one another. Independence means that one event does not affect the other. For example, tossing one coin and then another does not affect the outcome of the first coin's results. For authentication methods, this means that the way in which the factors are compromised must be independent. For example, if a network "sniffer" is used to compromise both

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

methods, the password and chip card, then the probabilities of both being compromised cannot be their multiple. More will be said about this important point.

Password Compromise:

Using user ID and password is one of the most common forms of authentication. Unfortunately, password security can be easily compromised in a number of ways not the least of which is the user forgets the password. Users can tell or write down their passwords, making them susceptible to being discovered by others. Passwords are often sent through insecure communications networks. Finally, often the system file or database that holds the password is open to attack.

Social engineering refers to deceiving someone into giving away confidential information. Hackers use social engineering to deceive system users into telling their password. Common deceptions include masquerading as someone else, such as the user's Help Desk, or masquerading as something else, such as the user's system asking for re-authenticate.[1] In both cases users unwittingly reveal their password.

Passwords can also be compromised because of insecure network connections. Insecure network connections are those without strong encryption. In general, strong encryption relates to the key length of the cryptosystem being used to scramble the data. Common encryption standards such as the Data Encryption Standard (DES) are no longer thought to be secure because its short 56 bit key length can be decrypted. Most strong encryption protocols now use 128 bit key lengths to create virtual private networks. VPN protocols such as S/MIME, SSL, and IPSEC rely on strong encryption to protect authentication.

Tcpdump is a program that can filter and capture packets on an insecure IP based data networks. Just about any field in an IP datagram – including the actual data payload -- can be used to select records that are collected[2]. Tcpdump can be misused to "sniff" data off an insecure network. In fact, programs like tcpdump are referred to as "sniffers" and can easily capture passwords off of insecure data networks. Tcpdump is readily available to anyone -- or any hacker -- at www.tcpdump.org.

IDs and Passwords can also be compromised from insecure system hosts. Older NT operating systems are particularly open to attack by sophisticated hackers. Using a "null" session a hacker can log into your Windows NT system, and with the net use command read your Windows Registry to capture your user ID. If the system being compromised is your company's Primary Domain Controller, an attacker can capture a list of user names, including all the members of the Administration group[3]. Having these valid user IDs is the first step in cracking a system.

Even though the NT operating system uses password encryption, the design has several flaws. First, prior to storage and encryption, the LAN Manager cuts a single password

[1] GSEC Host Perimeter Defense, p.11.
[2] GSEC IP Behavior. p.4
[3] GSEC Information Assurance Foundations, p.10

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

into two seven-character words. Then hackers only have to crack two seven-character passwords, an easier task. Second, NT does not "salt" the password prior to encryption. A salt is a random character added to the password prior to encryption to prevent hackers from matching alike words from their cracking software.

Taking advantage of these two NT design flaws, L0phtCrack is cracking software that will decrypt NT passwords. L0phtCrack can use both dictionary and brute force attacks to decrypt NT passwords. Complex passwords can be cracked in a matter of days[4]. Alphanumeric passwords can be found in less than 24 hours[5]. The L0phtCrack website reveals that in one test of a high tech company, 18% of the passwords were cracked in less than ten minutes. Note only one password is needed to compromise a system. L0phtCrack can also be used to sniff passwords from the network.

Microsoft has responded with two new service packs to protect NT passwords. Two of the most important tools are passfilt.dll, which enforces the use of complex passwords, and SYSKEY, which provides 128 bit encryption of passwords in the Security Account Manager (SAM). Another recommended step is to disable the LAN Manager.

Just as NT passwords files can be compromise so too can UNIX password files. Like L0phtCrack, a UNIX based program called "Crack" can decrypt Unix DES-encrypted passwords. Crack encrypts words and then attempts to matches these with the encrypted passwords on the system. Crack has the ability to check millions of common passwords against those in the password file. Like L0phtCrack, Crack uses both dictionary and brute force attacks. Crack is freely available to anyone, including hackers, at www.users.dircon.co.uk.

Older version of UNIX stored all user IDs and passwords in the same unrestricted file. Attackers were able to copy this file and using Crack decrypt passwords off line. Now steps can be taken to protect UNIX passwords. Shadow password files can be used to prevent discovery of passwords. These files separate the passwords from the IDs and initiates restricted access to the passwords. Root access is required to read the shadow file. Passwd is a UNIX program that can do basic checks to force users to use strong passwords.

Two Factor Authentication:

Given that passwords can be easily sniffed from insecure networks and that password cracking software is readily available, most Fortune 500 companies have moved to two-factor authentication, especially for LAN access, believing that the probability is high that a hacker can crack any single-factor password authentication scheme. As discussed above, adding a second authentication factor greatly reduces the probability of system compromise.

[4] GSEC L0phtCrack, p.8
[5] GSEC L0phtCrack, p.12

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

One-time Passwords:

Most commercial two-factor schemes are something you know and something you have. For example, a person may have a "hard token" device, such as a smart card, which generates an access code every 60 seconds. The user knows the access code and sends it to the system for access. Because one-time password generators change the access code every 60 seconds, there is no password database subject to password cracking. Also, if the password is intercepted it cannot be used again. One-time password generators can be software based. For example, SKEY uses pre-computed one-time passwords that are given to users. Each time a user logs on he enters a different password.

Biometric Technology:

Biometric technology held great promise for strong authentication. Biometric authentication relies on unique body patterns such as fingerprints, iris patters, voiceprint, hand size, signature, and facial geography. Technology is used to measure and store these areas for later verification. But the application of the technology has been limited by reliability, of false matches and non-matches. Also, there is certain unease knowing that if the data is compromised the person looses his unique identifier for life. Another two-factor authentication scheme that avoids these biometric problems is Public Key Infrastructure (PKI).

Public Key Infrastructure:

PKI relies on asymmetric encryption, which uses a pair of keys rather than one. One key is the users public key while the other is their private key. Messages encrypted with the public key can only be decrypted with the private key. For communication, then, a user must know the other user's public key. The first user encrypts the message with the others public key, knowing only the receiver can decrypt it with his private key. By publishing everyone's public key secure communications is made possible.

PKI relies on an infrastructure to operate. A certificate authority creates the user digital certificates and authentication keys. A registration authority confirms the user's identity, signs-up participants, and issues the digital certificate. A validation authority stores, publishes, confirms, and revokes certificates. A directory access protocol defines how digital certificate data is stored and retrieved. A digital certificate protocol identifies certificate data fields. A digital certificate identifies the originating certificate authority, the user, the user's public key, and is signed to be recognized as genuine.

PKI provides more than strong authentication. With encryption, PKI ensures the privacy of communications. With verification codes, PKI ensures that the data has not been tampered with. With digital signatures, PKI ensures that neither party can repudiate the transaction. PKI implementations are designed to work with other security standards. S/MIME relies on PKI to digitally sign and encrypt email messages, and SSL provides a tunnel for secure access to web servers. Other VPN standards, such as IPSEC, can use PKI to manage IPSEC keys.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PKI can be implemented with either a hard token (smart card) or soft token. With a hard token implementation, the certificate is stored on the smart card. With the soft token implementation the certificate is stored on a personal computer or PDA.

Authentication Vendors:

Password:

Arcot is a vendor that specializes in security software of eCommerce[6]. Arcot for VPN product authenticates users with the ArcotID Digital Credential. This is a PIN-protected certificate that holds the user's private encryption key. According to Arcot, "The user's ArcotID (something you have), along with a personal PIN (something you know), combine to deliver strong authentication and verification of the end user." Furthermore, Arcot for VPN versatility is that it is not platform specific and the credentials can be downloaded to a kiosk. As this is a software-based product, it avoids some of the distribution and inventory overhead associated with tokens and smart cards.

But does this software-based scheme really provide strong authentication in all cases? Strong authentication is based on the two factors being independent of each other so that there is no single point of compromise. In this case the hacker must know the PIN and the passwords, which are stated to be two independent factors. But if the ArcotID Digital Credential is downloaded to a Kiosk, part of its claimed versatility, that could represent a single point of compromise. A hacker could install key-stroke capturing software on the Kiosk that would reveal to him the cashed credential's PIN and the reusable passwords.

One-time Password Generator:

RAS Security also specializes in security products for eCommerce. RAS SecurID is a two-factor authentication product based on something you know, a PIN, and something you have, an authenticator token. The authentication token, called the RSA SecurID authenticator, generates a new, unpredictable password every 60 seconds. The PIN and token code are given together for secure access. Each authenticator token uses a unique 64-bit symmetric key to generate a new access code every 60 seconds, and only the RSA ACE/Server knows which number is valid at that moment in time for that user.[7]

Unlike the Arcot authentication scheme, even if there is a potential single point of compromise, such as an airport kiosk, the RAS SecurID cannot be compromised after 60 seconds. A hacker with key-stroke capturing software will be unable to authenticate to the RAS ACE/Server as the dynamic access code changes every 60 seconds. Even if the hacker stole the SecurID authenticator token, he would need the PIN to generate the access code. In short, the SecurID product meets the standard of independence, as both "something you have" and "something you know" would need to be compromised. SecureID can be said to be "strong" two-factor authentication.

[6] www.arcot.com/products
[7] www.rassecurity.com/products

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Smart Card with PKI:

ActivCard competes with both Arcot and RAS Security. ActivCard Gold too provides two-factor authentication based on something the user knows and has. To authenticate a cardholder inserts their ActivCard Gold smart card and enters a PIN into the terminal reader, and using SSL the reader sends the credentials for secure access. With PKI integration the ActivCard Gold smart card stores the private and public key, and the digital certificate on the smart card. The private key is generated and processed in the microchip on the card and is never exposed outside this secure platform.[8]

Because there is no single point of compromise, ActivCard provides strong two-factor authentication. Users must have the smart card and know the PIN to activate the authentication sequence. The smart card is immune to forgery or tampering as it locks if the wrong PIN is repeatedly inserted. The reader never knows and does not have the private key, and the access request transmission is encrypted with SSL. With PKI there is a timestamp to prevent wiretap and replay of the authentication request. In short, ActivCard Gold integrated with PKI is a near perfect two-factor authentication scheme.

Compromise Matrix:

Vender authenticate schemes can be compared using a matrix, identifying points of vulnerabilities:

	Off Line Processing	Open Line transmission	Encrypted Line	Kiosk	PC without Encryption	PC with Encryption
Acrot for VPN	no	yes	no	yes	yes	no
RAS SecureID token	no	yes	no	no	no	no
ActivCard Gold with PKI	no	no	no	no	no	no

A "yes" in the box above implies a possible single point of compromise.

Summary:

Cyberspace requires authentication. The most common authentication method is static password. Password authentication schemes can be compromised in numerous ways, leading companies to look for two-factor authentication. Two-factor authentication schemes include something you know, something you have, or something you are. To be two-factor authentication, the factors and the way in which they are compromised must

[8] www.activcard.com/products

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

be independent of one another. If so, then the level of confidence can be the multiple of their success rates, generating "strong" authentication. Some vendors have stronger two-factor authentication schemes than others. For example, Arcot's VPN product may not be strong authentication at kiosks, since hacking software loaded onto the kiosk could possibly compromise the product. RSA's SecureID provides strong authentication as the dynamic access code changes every 60 seconds, so even if the code was intercepted it cannot be reused after 60 seconds. ActivCard's Gold smart card product integrated with PKI has no single point of compromise and qualifies as strong authentication.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Published Sources:

Austin, Tom. PKI: A Wiley Tech Brief. John Wiley & Sons, Inc., 2001.

Pisani, Robert. Statistics. New York: WW Norton & Company, 1998.

Winters, Chester M. Audit and Control of Data Communication Networks. Wellesley Hills, MA: Management Advisory Service & Publications, 1989.

Weber, Ron. Information Systems Control & Audit. Upper Saddle River, NJ: Prentice Hall, 1999.

Datamonitor PLC. Public Key Infrastructure 1999-2003. London: Datamonitor, 1999.

Online Sources:

Berlind, David. "Now is the time for two-factor security." October 25, 2001 Techupdate.zdnet.com

Rash, Wayne. "Biometrics: Not a sure thing." November 29, 2001. Techupdate.zdnet.com

Rash, Wayne. "Smart Cards Elevate Enterprise Security." February 5, 2002. Techupdate.zdnet.com.

Hulme, George, "RSA Boosts Two-Factor Authentication Management." June 1, 2001. Informationweek.com

http://www.datacard.com

http://www.activcard.com

http://www.arcot.com

http://www.rassecurity.com

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.