Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Proximity Authentication

The author discusses protecting data by denying direct physical access onto a user's computer; that is, protect sensitive data terminals from being used by unauthorized users. The emphasis is on how to identify users - to make sure that they are who they claim to be, to a certain level of certainty - and gives an overview of Users Authentication Methods, both software and physically based. Included is a case study of the Ensure Technologies' XyLoc product. One of the goals for any security policy is to strike a balance...

Copyright SANS Institute
Author Retains Full Rights

AD

Proximity Authentication

Ali Merayyan
July 16, 2001

1. Introduction

As a result of the World Wide Web (WWW), the Internet, and the low price, computers became an important tool at home and work. They are being used as a research tool, shopping tool and a publishing tool. As an outcome of these services, people started to utilize the computers for most of their daily tasks. Which meant that people started to store private, personal, and valuable data on their computers. At work, sensitive data become very accessible to workers on their desktop. The availability of information and computers made the private/sensitive data vulnerable and tempting to unauthorized people to access that data. Furthermore, users have the habit of logging-in when they start their day and stay logged-in all day regardless if they are by the computer or not. Which makes the computer vulnerable to unauthorized access, "The weak link in securing access to PCs and data is undoubtedly the user"[1] With the use of physical/biometric devices it will be easier for the user to login and logout each time they walk-to or walk-away from their computer.

Protecting this data takes two forms:

1) Protecting valuable data from people trying to access it using the Internet. Which is protecting the data from people trying to gain access to the computer using the Internet and collect whatever valuable data the user have stored on his/her personal computer. Of course the best method to protect computers from being access by unauthorized users over the Internet is to have the computer not connected to the Internet, but this solution is too far drastic and there are less drastic measure including firewalls, intrusion detection, etc. This form of protection is beyond the scope of this paper.

2) Protecting data from people trying to access it using the user's computer itself. Which is protecting sensitive data terminals from being used by unauthorized users. For example, a computer setting on a registrar's desk with the registrar's identification has access to student's records. Gaining access to that terminal provides access to student's records. The best method to prevent access to computers that hold sensitive data is to have these computers locked up in a room and to provide access to these rooms to a limited number of users, which is not a realistic approach all the times. The registrar has to deal with students and should have access to their records to answer their inquiries; he/she can't be running back and forth into a locked computer. Also, it is recommended that the BIOS of the computer be modified in such fashion to prevent users from booting the computer into a different operating system using a diskette or the CD-ROM.

In this paper, I will discuss the second form of data protection. I will be talking about how to identify users, to make sure that they are who they claim to be, to a certain level of certainty.

1.1 Users Authentication Methods Overview (I am who I claim to be)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

There are several ways to authenticate users. Each of which has weak points and strong points. Some of these method have been used for quit a while some are just being utilized in the computing field. These methods could be categorized into two groups:

A. Software based: This is the oldest and the most utilized form of authentication. In this method, the user provides a user name, and a password. The system hashes the password (some implementations adds a salt to the typed password some don't) and compares it to the hashed password for that user in the password file. If the entered one and the stored one match, the user is allowed to log in. To provide a higher level of protection in this method, the user provides a given sequence of digits (Personal Identification Number – PIN) in addition to the name and password to identify himself/herself. As a result, the intruder would need this information triplet to be able to gain access, which makes more difficult. There are some problems with this method:

    a) Users select password that is easy to guess. Even though if the user select a not so easy password, they tend not to change the password for a quite long time which will give hackers the chance to crack the password. It is possible for system administrator to assign one-time use password and/or assign system's generated password. But by doing so, it will be very difficult for users to remember these passwords and it will be highly inconvenient.
    b) Users tend to write the password down and keep it around the computer, which defeats the use of system's generated passwords.
    c) Some login software still transmit password in clear text over the network. System administrator should disable these programs and steer users toward applications that uses encrypted communications between the client and the server.
    d) Password files that contain the hashed/encrypted passwords on some system are readable by all.
    e) Any person who has the name, password and PIN can pose as a legitimate user. This could be a voided by using some biometric feature of the user which makes it impossible for impostors to gain access to the system.

    Some of these issues can be fixed by using encryption before transmitting the password over the network and shadowing the password file to make the hashed password file readable only by the system.

B. Physically based: In this method the user uses a physical device to authenticate his/her identity to the computer. There are two forms of physical information that could be used to authenticate users:

    I. Biometric information: Some of the user's physical features (face, finger print, etc.) are used to identify him/her. The user has to be physically present by the scanning device to be identified. This is the most convenient method since the user doesn't have to carry extra devices to authenticate himself/herself to the computer and it is very difficult for others to claim to be who they are not. This technology entered the computing field recently, which makes a bit pricey and not mature enough.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Furthermore, even though the actual user scan is not saved on the computer just interesting point of the scan, the question that comes to mind, is it possible in the future for any entity to interpolate the original scans (i.e. finger print) from the stored data?

The identification process goes through four steps:

i. Scanning step: Scan the person's face, finger, or retina, etc. This step uses almost the same idea in all the different technologies.
ii. Feature extraction step: In this step the important point of the scan get extracted. This where the algorithm differ greatly.
iii. Comparison step: Comparing the extracted data to the stored data.
iv. Matching step: Matching the extracted data to the stored data and letting the user through.

Examples of the technology:

i. Facial Scan: The face of the person is used to identify him/her. This technology uses one of the following methods to identify/verify the identity of a person: eigenfaces, feature analysis, neural network, and automatic face processing.
ii. Finger Scan: The person's fingerprint is used to identify him/her. This technology uses the knowledge acquired using figure printing. It looks for certain points in the figure prints to identify that person.
iii. Iris Scan: The Iris features of a person's eye are used to identify him/her. Iris recognition is based on visible (via regular and/or infrared light) qualities of the iris. A primary visible characteristic is the trabecular meshwork (permanently formed by the 8th month of gestation), a tissue which gives the appearance of dividing the iris in a radial fashion. Other visible characteristics include rings, furrows, freckles, and the corona, to cite only the more familiar.[4]
iv. Retina Scan: The retina features of a person's eye are used to identify him/her. In this technology the pattern of the blood vessels on the back of the human eye are used to identify/verify the person. It was found that these patterns are unique from one person to another.
v. Hand Scan: The whole handprint is used to identify the person.
vi. Voice Scan: A spoken words are used to identify the person.
vii. Signature Scan: The way the person sign his/her name is used to identify him/her.

II. Physical Devices: A key chain, a ring or a smart card is used to authenticate users to the system. These devices could hold an encrypted PIN number (smart cards) that get passed to the system or the serial number (dumb devices) of the devices is used to authenticate the user. These devices make it convenient for the user since he/she doesn't have to remember a PIN number to login into their systems. But the user is forced to carry a device with his/her person all the time. Of course, these devices could be lost or stolen which adds another security risk. These devices communicate with the host computer using one of the following two methods:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

i. Using a reader/scanner device attached to the host computer: The user has to attach a scanner/reader to the computer and each time the user needs to gain access to the computer they need to slide the access device into the reader/scanner to be authenticated. Some people might consider this process a burden on the user and consider it a draw back.

ii. Using a wireless signal to communicate with a device attached to the host computer (called proximity devices).

2. Proximity Authentication – Ensure Technologies' XyLoc product case study

One of the goals for any security policy is to strike a balance between how secure the system is and how convenient it is for the users to use the system. Such a convenience makes it easier to get users to comply with the security policies. This convenience can be accomplished using a proximity device.
Proximity devices allow the computer to recognize an authorized user approaching and unlock itself for their use. This kind of authentication system consists of three components:

a) A device attached to the computer using a USB port, called the lock (Figure 1.) The lock is responsible for detecting the presence of an authorized key and instructing the software to unlock the computer. This device keeps on scanning within a certain range looking for authorized keys. The manager sets how far the key needs to look for authorized keys (lock range). Also, the software can detect the presence and the absence of the lock (got unplugged for some reason), and locks the machine. To get back into the machine, the user needs to plug the lock back in or over-ride the screen saver with a valid password.

Figure 1: XYLOC Lock– Source: Ensure Technologies' web site.

b) A device (badge, key chain) on the user's person, called the key (Figure 2.) The key transmit radio frequency to announce the user to the lock, then the lock communicates with the software to unlock the computer and grant the user who is carrying the key access. The key is in continuous communication with the key using radio frequency. Each key has a pre-set serial number that the manager uses to inform the software which keys are authorized to access the machine and what is the user's level of access.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figure 2: XYLOC Key Card – Source: Ensure Technologies' web site

c) A software package. On systems that don't have a protected file system and don't provide some kind of locking mechanism, the software encrypts the file system and provides login software to lock the system. If the system has a protected file system and locking mechanism, it communicates with the login software to be able to lock and unlock the system.

After installing the software and the hardware the system manager can configure the following setting:

I. Add authorized keys to access the machine. A key can unlock more than one machine and a machine could be unlocked by more than one key. Each key can be assigned an administrator, user, or a guest privileges. With administrator rights, the key/user would have a complete access the configuration parameters. With user rights, the key/user would have access to his/her authentication method, Xyloc password, lock range and password. With guest rights, the key/user has no access to the configuration manager.

II. Lock range. It defines how close the user needs to be to the machine for it to get unlocked. This range is very useful when setting too many machines within close proximity. The software administrator sets the range to "short" if he/she installing machines within cubical setting.

III. Login/Unlock Authentication method. These are the options the key/user has to access the computer. It defines how the user owning the key interacts with the system to gain access. With this setting the manager can select one of the following:

   a. AutoLogon (Keystroke confirm): with this method when the user enters the lock range, the user gets instructed to press a key to confirm that the right key/user id has been selected by the software to login.
   b. Hands-Free AutoLogon: With this method, when the user enters the lock range, the machine gets unlocked with out the need for the user to do anything. This method could be a security hole if a key got lost, stolen, or more than one person uses the same key.
   c. Select User Name: The lock finds all keys within range and instructs the user to select a user name to login with. This setting is useful if there are more than

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

on user using the same machine and they all stay within close proximity of the machine.

d. Must Enter Password: The user is required to enter a password an addition to the recognition of the key. This method defeats the convenience factor but it adds to the security factor, where the person with key needs to have a valid password.

e. Select User and Enter password: For this configuration, the user would have to enter the user name and password to be able to login to the machine even though the key was validated. This method adds another level of security where the user holding the key needs to have a valid user name and password to be able to gain access to the machine.

IV. Allow password override: This property allows the user to login into the machine if the key/lock are not functional. This property creates a security hole were an unauthorized user without a key can override the lock and login using a stolen password. On the other hand if the lock/key are not working and this property is not set the user would not be able to gain access to the machine and the administrator would have to remove the software component to allow users access to the machine.

2.1 Security Features

I. XyLoc Secure Login: Windows 95, 98 are not secure by nature. Ensure technologies includes XyLoc Secure Login software to allow the users of these systems encrypt their file systems and allow only authorized users to access the system. This software automatically disables the safe mode boot option to disallow unauthorized users from bypassing the login screen. Also, it is recommended that the user takes out the Floppy and CD-Rom from the boot sequence and password protect the BIOS.

II. Encryption: The lock and key are in continues radio communications using the challenge response schema. These communication lines are encrypted to prevent spoofing and code-grapping. Also, the software encrypts certain XyLoc configuration files that reside on the hard-drive for security.

III. Frequency Hopping: The system uses 900 MHz unlicensed frequency and it is known that there are so many devices using this band. To over come interference, the system utilizes some sort of automatic channel switching method. This frequency switching to some extent insures availability. But it is not a bulletproof method, since it is possible to introduce a noise that covers the whole band rather than sub-bands which is in fact can be considered a denial of service attach. Also, this frequency hopping could be considered a form of security since the two devices are not communicating using the same frequency all the time, it will be harder for a person to listen to a specific frequency and capture the communication packets. I am not sure if the company is using some sort of proprietary frequency hopping or they are using Frequency Hopping Spread Spectrum (FHSS).

IV. Bandwidth Utilization: Since it is possible to have more than lock-key pair in close proximity, the system uses Time Division Multiple Access (TDMA) method to allow more than one lock-key pair the use of the bandwidth. Also by limiting the range of each lock, it is possible for adjacent systems to reuse the same sub-band.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

3. Conclusion

The idea is noble and it does make it convenient to secure the system while the owner is a way, it has some issues though. I see the strength of the system in replacing the screen saver after the initial user log in. I don't feel that the system should be used to replace the user-id, password pair to authenticate the user and it should be used with some other form of authentication as a backup method for lost or stolen keys. If the system was configured with "Must Enter Password" setting and the key or lock get lost or stolen, the only way to allow login is to remove the software. One of the advantages of such a system is the quickness of locking and unlocking the user's machine. With screen savers, either the user has to lock the system himself/herself or just set a time of inactivity for the screen saver to lock the system. With the time limit, the system doesn't get lock the minute the user walks away from the computer and this is where this proximity device shines. Also, I wonder why the company is not using the unlicensed 2.4 GHz and Spread Spectrum technology that gives more channels and provide a more secure communicate channels.

References:

1) Brostoff, George. "Proximity authentication ensures security of NT/2000 environments." July 2000. URL: http://www.serverworldmagazine.com/compaqent/2000/07/proximity.shtml
2) Unknown. "Finger-Scan Technology." URL: http://www.finger-scan.com/finger-scan_technology.htm
3) Unknown. "Facial Scan Technology: How it Works." URL: http://www.facial-scan.com/facial-scan_technology.htm
4) Unknown. "Iris Recognition: The Technology." URL: http://www.iris-scan.com/iris_technology.htm
5) Unknown. "Retina Scan Technology." URL: http://www.retina-scan.com/retina_scan_technology.htm
6) Unknown. "Hand Scan Technology." URL: http://www.hand-scan.com/technology.htm
7) Unknown. "voice-scan.com." URL: http://www.voice-scan.com/
8) Unknown. "signature-scan.com." URL: http://www.signature-scan.com/
9) Microsoft Corporation. "Microsoft Smart Card Whitepaper." April 1998. URL: http://ecash.com/Press/microsft_smart_card_whitepaper.htm
10) Unknown. "Authentication 101 > Devices." URL: http://www.ankari.com/devices.asp
11) Pfleeger, Charles P. Security in Computing, 2nd Edition. Upper Saddle River: Prentice Hall, 1996. 254-264.
12) Young, A and et al. "Technologies to Support Authentication in Higher Education." August 21st. URL: http://www.ukoln.ac.uk/services/elib/papers/other/scoping/#22
13) Ensure Technologies™, "XyLoc Solo User Guide, 5.x"
14) Ensure Technologies™, "Frequently Asked Questions" URL: http://ensuretech.com/cgi-bin/dp/frameset.dt/products2/faq/faq.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**