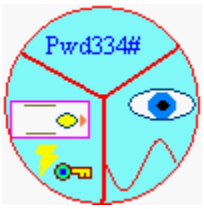
Global Information Assurance Certification Paper

Layered Authentication

We authenticate ourselves into our private worlds of data numerous times a day. Between e-mail, shopping, "logging in" or visiting a private website, we must give some sort of proof of who we claim to be. This proof takes the form of a few alphanumeric characters most of time, but can be the "James Bond"-esque form of a retinal scan. Whatever method we use, it's for a specific purpose; and the corollary, for each purpose only one method is used. Layered authentication is defined by using more than one method per application or access-requiring visit. This may seem a burden or as extraneous measures, but it does provide more dimension to an otherwise "flat" security model.

Trinity of authentication

Although you are probably already familiar with the three categories of authentication methods: "what we know", "what we have", and "what we are," we'll briefly go over it again here:



- What we know: mom's maiden name or some other easily guessable password.
- What we have: a physical token carried with you, i.e. Smartcard or RF token.
- What we are: thumbprint, raspy voice, chiseled jaw line, unique blood-vessel roadmap behind our baby blues.

Figure 1: The Three Categories of Authentication

A vast majority of corporations utilizes the first, "what we know," to judge the user as authentic. Strictly a password is needed in order to do anything from getting past the screensaver, to opening up an e-mail client, to buying their son's next birthday gift. As companies broaden, moving more tasks to their intranets, such as filling out timesheets or managing stock options, the authentication scheme is still the same –"what we know."

The "what we have" is more often used in walking up to a object, whether it be the front door, door to a data center or to an ATM. Ideally, we try not to even break stride in the authentication process, getting annoyed when a badge reader's LED doesn't flip green in less than 0.3 seconds. The third form, "what we are" is also known as "biometrics." In contrast to the first two categories, biometrics has been hindered by privacy issues and general social uneasiness, thus has yet to go mainstream. Ironically, even where the infrastructure is in place for other logging purposes, such as a camera installed at every ATM, it falls short of social acceptance, thus going wasted, in this author's opinion.

Several companies already may employ more than one method of authentication, such as requiring both a password and a Smartcard. However, each of these methods carries a specific purpose. For example, the company employee knows a password to log in to the network and carries a Smartcard to enter a physically secure area. Have you ever seen a door requiring a PIN number to ensure the owner of the necessary access card is the true owner?

Trinity Divine

Let's consider one plausible scenario where all three methods of authentication are employed:

You walk up to a workstation, enter you password to log in, -there you are, access granted by "what you know." You're opening up a web browser, checking on your company's stock price. You are but one user of many, surfing the web, wasting the company's time, which, in a round about way, explains the direction of the stock price. Before you know it, it's time for lunch. The screensaver takes five minutes to activate, but it only takes Fletch, your cubicle neighbor one minute to jockey your machine. He opens up a web browser to check his personalized stock portfolio.

Further expanding on this scenario, because you are a member of the web administrators group, you are granted access to update the company's web servers. Still jockeying the machine, with your logged-in session still open, Fletch goes to start up a dreamy application used to manipulate web pages, only to be reminded he does not have your Smartcard. Yes, access is layered throughout applications. Access granted to only those individuals able to show "what they have," not Fletch. Back from lunch, you unlock the screensaver and notice a browser open to http://www.CNNfn.com. As a naturally suspicious person, you decide to check the logs of the workstation's local Intrusion Detection Software (IDS). You are truly paranoid, so in order to open your favorite IDS monitoring package, a biometrics device has been employed here. The fingerprint reader attached to the machine identifies you as who you say you are. Logs display URLs, timestamps and information sent from your machine, so Fletch is caught. This scenario could be considered exaggerated. However, it is certainly possible.

Layered Approach

My wife is a geologist and an environmental engineer. So, over eggs and toast, before I can speak of code and servers, she will bring up "strata," or layers, of rock. As the good, interested husband, I'll ask how is it some chemicals, when spilled accidentally on the ground, can develop a plume so easily through porous sand, but not through clay. "Because it's a matter of 'what you are,' not 'what you know'," she'll retort. Cute, isn't she?

Similarly, because you can use some form of authentication to allow us into one layer, but demand another authentication process to delve *deeper down*, we add another dimension or aspect to our authentication model. In the previous example, you were prompted for different authentication methods only when different applications were opened. What if you were prompted for further credentials strictly when additional access is required? Here's an example: When you are a receptionist at a doctor's office, you require the ability to alter a patient's file, namely his or her personal information, i.e. phone number, address. However, the patient would rather keep their reasons for visiting private if possible. The nurse, with his Smartcard hanging from his neck, will require more information from the same application. The doctors, having a need for full disclosure of information, will be known by precisely "who they are." See the trinity of authentication –in a layered setting?

Keeping Britney Hidden

In another example, taking place at the author's work environment, we use all three methods in place to keep a collection of large sized files out of sight and out of mind. This collection happens to be an assortment of music videos.

Half a terabyte of storage utilized in our lab SAN can be regarded as strictly off limits to all folks, except for two: myself and a trusted co-worker. There are several very intelligent people working in the same engineering group, but none possess the necessary credentials required to get to the cache of videos filling that 500 Gig spinning at 10,000 rpm. Sitting in front of a lab workstation, the screen saver is child's play. It's a Windows 2000 Professional install, so via keyboard or network, it's considered unsafe as a box. After the box is initially built and "hardened," the Novell Client is installed.

> **Note:** This was used since NetWare servers serve the data in question. Although NetWare is the file server's OS of choice and Novell Directory Service (NDS) is already being used, there are equally functional alternatives for other platforms.

How To Access The Tiers Lower Than First

With our attention to Figure 2, we see that users, via password, log in to their account, activating their login scripts, granting access to their respective home directories. It was not coincidental that it took all three authentication methods to create a complete circle in the figure earlier in this document.

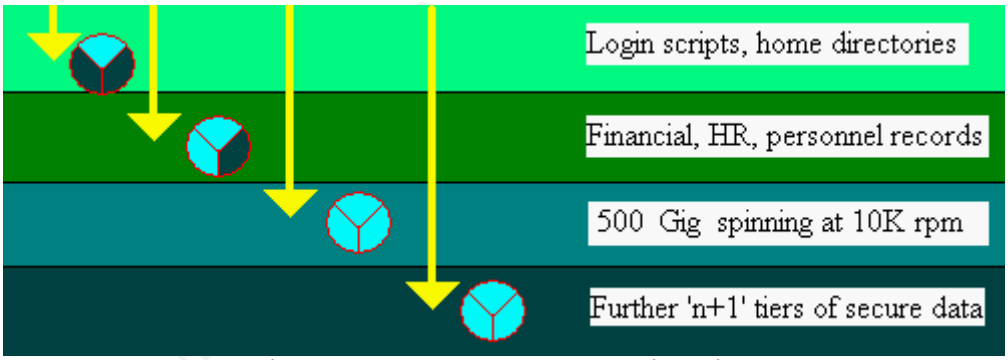


Figure 2: Layered Authentication

Once the user utilizes, for example, a Smartcard, the machine recognizes the user and grants access to deeper levels of secure data. Furthermore, a biometric device such as a fingerprint reader can give the user access to levels of secured data limited to a different audience. This third layer could be the point where all three methods illustrated in Figure 1 earlier have been used. Does this imply that the tertiary level is accessible only by those originally able to see "Financial or personnel records?" No, it does not; access is granted simply to those people given rights as deemed by the medium used for that particular level. This is no more complicated than giving rights to a particular administrative group or individual. Only in this case, rights to data of different degrees of concealment may determine the need for the variation of authentication method.

N+1 Tiers

You may choose to stop at three distinct levels (or "strata," if you will) of confidentiality, or you could certainly continue the tiers.
One important point to make is that you may grant authentication from one level to the next by an entirely different form (Smartcard to Password to Fingerprint) or you may choose to use different formats of similar devices between levels. For example, most all employees have fingers, voices and eyes, so that an assortment of biometric devices may be exercised to validate a user's identity.

Who Ships What to Allow This?

In an environment using a directory service, for instance Novell's NDS or Microsoft's Active Directory, software such as Novell Modular Authentication Service (NMAS) can take advantage of the centralized database (directory).

In the Novell space, it is the directory (NDS) that validates the user's credentials, thus determining the user's access; the layered authentication is dubbed "Graded Authentication." Though NMAS operates dependant on Novell Directory Service, it no longer requires a NetWare server present in the environment. This is because NDS may run solely on platforms such as Microsoft NT, UNIX, Solaris, Linux, etc.

In an environment that has no directory, there are literally dozens of vendors providing similar services of smartcard, token and biometric authentication devices. Although a database is necessary, this may be centralized and mirrored on several servers for the sake of high availability or distributed across multiple groups. Either way, this allows for any given employee's credentials to be contrasted with a known good from any machine at any time.

A comprehensive list of vendors can be found here:

Smartcard/Token vendors	http://www.infosyssec.net/infosyssec/secsmc1.htm
Biometric Technology vendors	http://www.infosyssec.net/infosyssec/biomet1.htm

Whatever the environment, vendors are quite competitive in their quest into this market. One vendor, eTrue, supplies cameras and fingerprint readers free-of-charge, in order to establish a service foothold into a company. An example of a success story: Keyware Technologies uses the uniqueness of biometric data (voiceprint, fingerprint, etc) to create an encrypted number. Standalone, this number is useless and is of no intrinsic value. Yet, stored on a Smartcard and compared to the same number created by the biometric variables at the transaction time - this combines two of the three methods for greater protection should the card be lost, as well as provides a solution to ease privacy issues. This happens to be the way the entire Belgian population (10 million strong) handle things such as Social Security, hospitalization and day-to-day purchasing.

Biometrics With Their Exclusive Cons Will Persevere

Biometrics poses a unique problem for administration and management. The handshaking between host and server over the wire, whether from a Smartcard, password or biometric device, is subject to eavesdropping and eventual compromise. Unlike a

Smartcard or a password, though, the personal features used for the biometric device can be neither rendered invalid nor replaced. The safeguarding of that handshake is entirely dependant on the software used to drive the hardware, such as a reader. If that software possessed encryption methods weak enough, traffic sniffed between host and server could be intelligible and perhaps manipulated and re-sent as bona-fide. It presents a difficult case for the true owner of the fingerprint to dispute how he or she was not the cause of some malicious act.

Nevertheless, last month biometrics is cited as one of the "Top Security Trends for 2001" by Security Advisor, echoing the results of the Yankee Group's March 30, 2001 findings in "Where the Investment Dollars Will Go in 2001." Yankee Group, a leading consulting group for technological research see the future of biometrics as "moving out of the labs and past government installations to become a mainstream technology for strong user authentication over IP networks" by end of year 2001 or beginning of 2002.

Above all it is most important to recognize the advantages and disadvantages of each method available. There can be an entirely new paper drawn up on the pros and cons of each method and then how to give weight to each, dependant on the individual company's needs.

Questions Needing Answers

No matter how good an idea or how simple an implementation is, solid planning and design are key to a smooth-running outcome.

Management and Systems Administration should start off by asking themselves the following questions:

Products and Design

1. What products are on the market?
2. What platforms will they run on?
3. Is our present infrastructure capable of handling them?

Implementation

1. What are we looking to control access to?
2. What measures are needed to safeguard implementation?
3. What training/awareness is necessary to implement this?
4. How will the employees respond to new devices (i.e. biometrics an issue)?

Management

1. How do we properly log, audit and track?
2. How can we prepare for potential abuse?
3. How can administration be proactive instead of reactive?

With any changes to the security infrastructure, especially as great as this, there must be representative changes made to the Security Policy. Unfortunately, documentation, whether it is for tracking systems, applications or the security policy itself, seems to lack priority at many installations. Security Policy is an oft-overlooked cornerstone to how tasks are carried out. Tasks including day-to-day administration as well as a new server installation are equally important in regards to how the Security Policy has laid out the methodology. A team led by John Wack at the National Institute of Standards and Technology has drafted a definitive, structured "How To" guide on

what it takes to create a Security Policy. The URL for that may be found in the list of Sources concluding this paper. Change management is a necessary part of a smooth operation and it starts at the very top.

Summary

We are quite accustomed to the concept of proving whom we are once and only once in order to gain access. This may be to check e-mail, shop on-line or fill out our timesheet. Should our identity be compromised along the way in completing one task, it may be used improperly for other, more sensitive tasks. The means to validate a user attempting access should reflect the perceived value of the assets being protected. Should a way to circumvent the authentication method be discovered or abused, one tactic to combat this is to make use of a completely different medium of establishing those credentials. In using the method of authentication most appropriate to the task at hand, the unauthorized person has a much harder time obtaining the means to gain access. All told, how easy or difficult it is to access data can be determined by our process to authenticate us. The bigger the challenge for abuse, the smaller the logs become. And when it becomes time to review them, we could all tolerate a little reduction.

Sources

Novell, Inc.: Novell Modular Authentication Service, Documentation
URL: http://www.novell.com/documentation/lg/nmas10/docui/index.html

ETrue. "eTrue's Biometric Internet Service"
URL: http://www.etrue.com/solutions/authentication.htm

Keyware Technologies. "Products and Services"
URL: http://www.keyware.com/smrtcrd/pages/products.html

Advisor Zone, Security. "Top Security Trends of 2001" April 6, 2001
URL: http://www.advisor.com/Articles.nsf/aidp/SMITT184

Wolansky, Mark W. "Stronger Authentication Methods: Biometrics and Public Acceptance" SANS Information Security Reading Room. April 18, 2001

John Wack. "Internet Security Policy: A Technical Guide" July 31, 1997
URL: http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

Yankee Group. "Where Internet Security Investment Dollars Will Go in 2001" May 11, 2001
URL:http://www.yankeegroup.com/webfolder/yg21a.nsf/press/8BD540DB9DC038E885256A1F0056A78F?OpenDocument

Last Updated: July 24th, 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 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 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
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 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
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 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