Authentication on DoD Information Systems

Jean Liebig

20 July 2004

GSLC Practical Assignment
Version 1.0

ABSTRACT

Authentication is a critical element in defending our personal computers and networks against intrusion. In order to authenticate a user, we must be assured that the user is exactly who he says he is. Is it enough to trust that a user name and password hasn't been given out to a spouse or secretary or been compromised? Or do we need to take further steps in authentication? When we authenticate you as a user, we must assess one or more of "the three pillars of authentication:" something you know, something you have, or something you are.[1] The more of these we authenticate, the more we can be assured that you are who you say you are - an authorized user on the information system. The US Department of Defense (DoD) has just recently moved beyond only assessing something you know and now looks at a combination of the three pillars.

INTRODUCTION (Selection Criteria)

A couple of decades ago, it was good enough to turn off the computer, lock the door, and go home at night, knowing that the information on your computer was relatively safe. The only way an intruder could get to your information would be to physically break into your office to steal it. Even though physical security is still a serious consideration in protecting information systems, it is no longer necessary to have physical access to the computer to steal information. Most information systems are connected to the World Wide Web and therefore can potentially be accessed from anywhere in the world.

In the military, we store a significant amount of sensitive information on our personal computers and networks. Sensitive data can include personnel records, medical records, legal records, logistical data, etc. As information technology and security professionals, it is up to us to put policies and procedures in place to protect the information from unauthorized individuals.

One of the most basic and common ways we protect our information is to authenticate the user trying to access the information and/or information system. Traditionally, a user name and password has been used to perform this authentication. But as technology continues to accelerate and cracking passwords is more feasible, password requirements have become very stringent and other technologies are augmenting or replacing the password authentication. The military is implementing more advanced authentication methods utilizing something you have (the Common Access Card or CAC) and something you are (biometrics).

[1] Reid, Paul. "Biometrics for Network Security". Prentice Hall PTR, 2004, p. 9.

DISCUSSION AND APPLICABILITY

Something you know

Passwords and Personal Identification Numbers (PINs) are the most common examples of authenticating users by something they know. We have passwords or PINs for almost every electronic device we encounter, to include our work, home, and handheld computers, Internet service providers, voice mail accounts, ATM machines, websites, office buildings, cars, homes, and the list goes on. "For most of us, the number of passwords and PIN codes we currently have is somewhere between 5 and 8. For some, that number can be as high as 12-15."[2] But do we really memorize all of those individual passwords? Do we write them down someplace safe or make all of our passwords the same?

"Passwords are popular because of their low cost; however, poor password use and management have left many systems vulnerable and are a common reason in the majority of system penetrations."[3] As technology improves and computers process faster, cracking passwords has become easier. Two methods used to guess a password are:

- "The cracker has some personal information about the user. Frequently people use the names of their cats, dogs or spouses as their passwords.
- A brute force attack is one in which all possible words of a certain length are attempted until a correct one is found. Crack dictionaries which contain a list of common words and phrases can easily be found on the Internet."[4]

Networking software and add-on applications allow system administrators to set restrictions and policies to enforce better password practices, such as the length, composition, and life of a password and the limits for where, when, and how many times a user can attempt to log in. Example criteria for a strong password policy include:

- Use eight or more characters (variable length is best)
- Use upper- and lower-case letters, numbers, special characters, and non-printable characters (when possible)
- Do not use dictionary words or user names, forward or backward
- Do not use character replacement in dictionary words (i.e., replace a with @)
- Do not use simple keyboard patterns
- Change the password periodically (every 3-6 months)
- Do not allow repeat passwords (i.e., rotating the same three passwords)
- Do not use the same password with only a couple of character changes
- Make it easy to remember so there is no need to write it down
- Limit unsuccessful login attempts (i.e., no more than five or account is locked)

[2] Reid, Paul. "Biometrics for Network Security". Prentice Hall PTR, 2004, p. 3.
[3] US Air Force. "Identification and Authentication". AFMAN 33-223, 21 November 2003, p. 4.
[4] Shekhar, Raj. "Choosing Strong Passwords". News Forge, 1 March 2003.

Passwords are a good form of authentication, but alone they are not good enough to protect sensitive systems and sensitive data. Passwords can easily be shared or compromised, so you can never truly be sure the user is exactly who he says he is.

Something you have

The military's implementation of a stronger authentication method includes the issuance of Public Key Infrastructure (PKI) certificates on Common Access Cards (CACs). The CAC is the replacement for the military identification cards. It is "a Department-wide smart card ... for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals."[5] The CAC has the potential to be used for accessing military networks, government websites, controlled offices, buildings, or installations.

The CAC not only contains the individual's picture, name, rank (if applicable), affiliated service component, and other personal data, but it also has a bar code, magnetic strip, and a small integrated circuit. The circuit contains the PKI certificate used to log into networks and websites that are PK-enabled. This PKI certificate is specific to the individual and his current email address and requires a PIN number to authenticate.

PKI technology is based on asymmetric cryptography, using two different keys. These keys are generated at the same time, and are mathematically related such that if either key is used to encrypt, the other key must be used to decrypt. The algorithms used to generate these key pairs also ensure that if one key, called the public key, is known, the other key, called the private key, cannot be easily determined. The public key is widely distributed, while the private key is never shared outside the direct control of the subscriber.[6]

The PKI certificate has many security purposes including authentication. The individual can insert his CAC into the CAC reader and enter the PIN to log onto the network. When he pulls the CAC out of the reader, his workstation is automatically locked. In email, the individual can use his private PKI certificate to digitally sign emails sent to others, leaving no doubt that he sent that email. He can also use his private PKI certificate to decrypt emails that were sent to him encrypted with his public certificate. He can use other individuals' public certificates to send encrypted emails to them. Finally, he can use his private certificate to authenticate to PK-enabled web servers.

Although the military has been using PKI with software certificates for a number of years, the CAC is a more assured form of authentication because it combines something you know with something you have. Chances are much less likely that you will leave your only identification card with your coworker, spouse, or secretary, because you must have it with you.

[5] US Department of Defense. "Public Key Infrastructure (PKI) and Public Key (PK) Enabling". DoD Instruction 8520.2, 1 April 2004, p. 13.
[6] US Department of Defense. "The DoD PKI And PK-Enabling Frequently Asked Questions". 3 May 2004, p.2.

A few drawbacks of using the CAC with the PKI certificate have been encountered. First, if an individual changes rank, name, or any other personal information, the CAC must be reissued. This means the individual gets a brand new PKI certificate, and he will encounter difficulties decrypting previously stored encrypted messages. Next, there has been a significant learning curve for getting users to not leave their CAC in the CAC reader at their computer. When they return to work the next day, they can't access the military installation because their CAC is still on their desk in their office. Finally, individuals can't use PKI from home or the road, unless they have a CAC reader and the military network supports PKI from afar. Many of these challenges will be resolved with time, practice, and new technologies.

Something you are

The field of biometrics encompasses a fascinating technology that has actually been around for many years. Many of us have seen the movies that depict individuals using handprints or iris scans to access the top secret laboratories in some villain corporation. But biometrics only recently entered the commercial computing industry, available to the average consumer. "Biometrics are automated methods of recognizing an individual based on their physical or behavioral characteristics. Some common commercial examples are fingerprint, face, iris, hand geometry, voice, and dynamic signature."[7]

For a biometric system to be effective, first individuals must be enrolled in the system. Then when the users wish to be authenticated, their current biometric is compared with what was originally enrolled. The biometric system is initially populated (enrollment) when an individual's biometric is recorded by the acquisition device, the collected data is mathematically averaged by the software, and a reference template is created and stored in the system or on the smart card. Acquisition devices can include cameras, scanners, or voice recorders. After enrolling with the system, the individual can either identify himself to the system and authenticate with his biometric (verification) or the individual's biometric can be compared with the database to determine the identity of the individual (identification).[8]

When choosing to implement a specific biometric system, we must be fully aware of the potential for false positives (the user is not who he says he is, but is granted access) and false negatives (the user is who he says he is, but is not granted access). False positives can be detrimental to the security of the information system, while false negatives can be very annoying to the authorized individuals. A balance must exist between how secure the system is with a low false positive rate and how usable the system is with a low false negative rate.

[7] Blackburn, Duane M. "Biometrics 101, Version 3.1". FBI, March 2004, p. 1.

[8] US General Accounting Office. "Information Security, Technologies to Secure Federal Systems". GAO-04-467, March 2004, p. 26.

As the cost of biometrics and biometric systems decrease and the authentication accuracy improves, the military is becoming increasingly interested in using biometrics to augment authentication for access to networks, secure offices, buildings, or installations. They are also interested in the applications of biometrics to quickly access portable information systems on the battlefield. "By 2010, [DoD] will use biometrics in its classified and unclassified systems to improve physical and cyber security.... DoD might require that military, civilian, and contractor personnel provide biometric identifiers, such [as] fingerprints and iris scans, to enter buildings or gain access to data."[9]

Standardization is one of the most important issues with identifying a single biometric system to implement across the entire military. If biometrics are to be used with the CAC and PKI, the Air Force, Army, Navy, and Marine Corps must all support the chosen biometric and biometric system. First, with the decreasing staffs in the network operations centers, it must be easy to implement and support at the installation level and at the unit level. Second, it must be socially acceptable. Through a thorough education program, we must convince the military, civilian, contractor, and foreign national populace that biometrics can increase the security of our information systems. Third, implementing biometrics must be user friendly, convenient, accurate, and efficient to the individual users. They will not support the new system, if it takes significantly longer to authenticate with a biometric than with a password. Fourth, backup biometrics must be identified and supported. If an individual is missing the required biometric, whether it is a hand, finger, eye, or voice, alternate solutions must be in place to gain support and acceptance from all. And fifth, biometrics must be supported whether you are physically located on the network or you are attempting to authenticate through some remote method. As the military becomes more mobile, this is a necessary requirement.

Even though the accuracy of biometric systems has improved significantly over the past few years, some obstacles still require refinement in the collection and comparison of biometric data. "Minute changes in positioning, distance, pressure, environment, and other factors influence the generation of a [reference] template."[10] Furthermore, the quality and cleanliness of capture devices can affect the accuracy of the biometric data. Fingerprints are of special concern because scanners can retain latent images from the last person who used the scanner. "Fingerprint scanners have been tricked into accepting latent prints that were reactivated simply by breathing on the sensor or by placing a water-filled plastic bag on the sensor's surface."[11] Obstacles such as these must be considered and overcome before we can entrust biometrics to authenticate users to our information systems.

[9] Onley, Dawn S. "DoD Reveals Biometrics Plan". Washington Technology, 2 September 2003.
[10] US General Accounting Office. "Information Security, Technologies to Secure Federal Systems". GAO-04-467, March 2004, p. 29.
[11] Ibid

SUMMARY

Authenticating a user depends on analyzing something you know, something you have, something you are, or a combination of the three. As the military evolves from basic password authentication to authenticating by CAC/PKI with a PIN and eventually to authenticating by CAC/PKI with biometrics, they continue to improve the accuracy of authentication. It was once easy to leave your password with another individual so he can check your email, maintain your calendar, or access your files. It is a greater imposition to leave your CAC with others, as you need to have your CAC with you. As the military develops and implements biometrics with the CAC, it will be virtually impossible for you to allow others authentication on your behalf. With time and technology improvements, the military will overcome the obstacles of implementing the CAC and biometrics to develop an authentication process that can be trusted by all. We will eventually find ourselves using combinations of the PIN, CAC, and biometrics to authenticate access to military installations, buildings, offices, computer networks, and the Internet.

REFERENCES

Blackburn, Duane M. "Biometrics 101, Version 3.1". FBI, March 2004. URL: http://www.biometricscatalog.org/biometrics/Biometrics_101_v5.pdf

Onley, Dawn S. "DoD Reveals Biometrics Plan". Washington Technology, 2 September 2003. URL: http://www.washingtontechnology.com/news/1_1/daily_news/21601-1.html

Reid, Paul. Biometrics for Network Security. Prentice Hall PTR, 2004.

Shekhar, Raj. "Choosing Strong Passwords". News Forge, 1 March 2003. URL: http://www.newsforge.com/software/03/02/26/1639212.shtml?tid=2

US Air Force. "Identification and Authentication". AFMAN 33-223, 21 November 2003. URL: http://www.e-publishing.af.mil/pubfiles/af/33/afman33-223/afman33-223.pdf

US Department of Defense. "Public Key Infrastructure (PKI) and Public Key (PK) Enabling". DoD Instruction 8520.2, 1 April 2004. URL: http://www.dtic.mil/whs/directives/corres/pdf/i85202_040104/i85202p.pdf

US Department of Defense. "The DoD PKI And PK-Enabling Frequently Asked Questions". 3 May 2004. URL: http://iase.disa.mil/pki/faq-pki-pke-may-2004.doc

US General Accounting Office. "Information Security, Technologies to Secure Federal Systems". GAO-04-467, March 2004. URL: http://www.gao.gov/new.items/d04467.pdf