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.

Biometric Selection: Body Parts Online

The purpose of this paper is to provide information that will assist a biometric implementer evaluate and select biometric technology. The scope of this paper is limited to the selection of biometric technology as an authenticator in a networked environment. Biometrics as a physical access, e-commerce, and monitoring technology is beyond the scope of this paper. As a security consultant and systems integrator, I will attempt to point out the "fine print issues" of this technology, as well as, dispel biometric misconcep...

Copyright SANS Institute
Author Retains Full Rights

AD

Biometric Selection: Body Parts Online

© SANS Institute 2002, Author retains full rights.

Steven M. Walker CISSP, ABCP
GSEC Practical Assignment 1
Revision 1
Certification Sought GSEC
7/26/2002

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

Abstract

The purpose of this paper is to provide information that will assist a biometric implementer evaluate and select biometric technology. The scope of this paper is limited to the selection of biometric technology as an authenticator in a networked environment. Biometrics as a physical access, e-commerce, and monitoring technology is beyond the scope of this paper. As a security consultant and systems integrator, I will attempt to point out the "fine print issues" of this technology, as well as, dispel biometric misconceptions, cover generally available biometric technology, and explore selection considerations. Biometric technology has great promise and application, but only as a component of an organization's overall risk management program. As with all security mechanisms and countermeasures, improper selection, planning and implementation will leave an organization vulnerable to threats.

The Hype

Suffice it to say that information security has been a white-hot topic since 9/11. Security itself is so broad and misunderstood that IT managers and staff are being pressured to adopt the latest hot technology that promises to protect critical information assets while saving management from liability claims. Technology vendors promise a short ROI, quick deployments, user transparency, total reliability, and minimal additional resources (not likely). Failed security projects such as Public Key Infrastructure (PKI)[1], Single Sign-on (SSO)[2], Distributed Computing Environment (DCE)[3] litter the landscape because of nondescript objectives, incomplete requirements, lack of executive commitment, assumed capabilities, and exaggerated vendor promises.

Biometrics is one such hyped technology. Digitized body parts (physical attributes) stored online and compared real-time with an individual will identify terrorists as they pass by a camera, authenticate users, identify customers to e-commerce websites, and provide fine-grained access control to data objects. Properly implemented biometric technology can be part of a total solution that supports these functions. However, the devil is in the details, and biometric technology alone can't do any of these functions. In the production world it takes an infrastructure of complementary technologies, processes, policies, and resources to utilize biometric technology.

---

[1] Chen, Anne. Nov 5, 2001. Prescription for PKI Success. http://www.eweek.com/article2/0,3959,148423,00.asp

[2] Flynn, H. April 10, 1998. SSO Magic Quadrant. http://www.gartner.com/reprints/platinum/m034848.html

[3] Ediger, Bruce. October 19, 1999. 10 Reasons OSF DCE Sucks. http://www.users.qwest.net/~eballen1/anti_dce.html

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

Dispelling Misconception

Lets start this section by listing some common biometric misconceptions.

1. Biometric authentication is the strongest authentication mechanism available.
2. Biometric authentication is the most reliable authentication mechanism.
3. Biometric authentication is immune to circumvention.
4. Biometric technology provides a complete solution for authentication and access control.

Misconception 1

Biometric authentication as a stand-a-lone technology is not secure, and does not meet "Security Best Practices". Biometric technology is essentially the capture and storage of an individual's unique physical attributes (iris, retina, finger prints, hand geometry, palms, voice, face, signature and keyboard dynamics are the most common). These digitally stored attributes are nothing more than files stored in a database and used for comparison functions, just as entered passwords are compared to their database stored counterparts (Actually, passwords are hashed and compared against stored password hash values).

The main utility of this technology is to provide either identification or verification during the authentication process. In security there are 3 commonly referenced factors by which a user can authenticate [4]:

1. Something you know (ID, PIN, Password, Passphrase)
2. Something you have (Certificates, and tokens including One-Time-Passwords, smart cards, key cards, USB fobs, challenge/response)
3. Something you are (Biometrics)

"Best Security Practices" dictate that network authentication use minimally 2, and preferably 3 factors as part of a strong authentication scheme. Stand-alone biometric technology (1 factor authentication) is not very secure, as the same biometric

[4] Liu, Simon., and Mark Silverman, A Practical Guide to Biometric Security Technology. http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm

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

mechanism provides both identification/verification, and is susceptible to playback and forgery attacks. However, coupling biometrics with other factors, e.g. passphrase, or token does make for a very secure authentication mechanism, provided the authentication event is encrypted over the network, and input mechanisms are resistant to forgery. For this reason biometrics today are more commonly implemented in conjunction with a password/passphrase as opposed to replacing passwords/passphrases [5].

Misconception 2

Biometric reliability is variable among technology types and vendor chosen. The range is broad from low to high reliability. Biometric reliability is made up of accuracy and availability aspects. Reliability metrics assume a properly configured biometric system, backend system integration, and accurate enrollment of users. To discuss reliability, one has to understand 3 measurements used by vendors to describe and benchmark their product:

1. Type I Error - a.k.a. False Rejection Rate (FRR); Measurement of authorized users who are denied authentication and subsequent system access. Good guys can't get in. If 1 of 1000 authentication attempts rejects a legitimate user then the FRR = .1%

2. Type II Error – a.k.a. False Acceptance Rate (FAR); Measurement of unauthorized users that are granted access. Bad guys can get in. If 2 of 1000 authentication attempts accepts an illegitimate user then the FAR = .2%

3. Crossover Error Rate (CER) [6] – Rating stated as a percentage at which point Type I errors = Type II errors. Think of biometric authentication as a moving window. Too narrow a window, legitimate users are more frequently denied access, while illegitimate users more infrequently granted access. Too large a window, and legitimate users are more infrequently denied access, while illegitimate users more frequently granted access. Number of good guys denied = number of bad guys allowed. All biometrics systems have a sensitivity adjustment that allows manipulation of sensitivity thresholds to reach a point where FRR=FAR. The smaller the CER the more accurate the system.

[5] Scheier, Robert. January 10, 2002. Biometrics: Improving but not perfect. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci798104,00.html?FromTaxonomy=%2Fpr%2F286152

[6] Tipton, Hal., Donald R. Richards, Donald R. 1999. Handbook of Information Security Management: Biometric Identification. Boca Raton: Auerbach Publications http://www.cccure.org/Documents/HISM/033-037.html

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

Now that we understand error types and metrics, the next step is to realize that CER very from mechanism-to-mechanism and vendor-to-vendor. Note the Table 1 below. Notice the large differences in CER [7].

Biometric Crossover Accuracy:

Biometric	Crossover Accuracy %
Retinal Scan	.0000001%
Iris Scan	.000763%
Fingerprints	.2%
Hand Geometry	.2%
Signature Dynamics	2%
Voice Dynamics	2%
Keyboard Dynamics	5.4%

TABLE 1

Notice the lower 3 table entries. In the production world, 2 failures out of 100 authentications are not tolerable for a network of moderate size. Each user may have to authenticate 4 or 5 times a day if not more. Given a 1000 user network, 1000 * 5 = 5000 daily authentications, 5000 * (range of 2-5% CER) = 100 to 250 authentication errors/day.

The other side of reliability is availability. The CER listed in Table 1 are error rates when everything is working perfectly. What happens when the fingerprint reader gets oily, or the iris camera gets dusty or is knocked out of position? Type 1 Errors occur. The maintenance and the upkeep of the biometric input mechanisms need to be considered and evaluated. CER could easily double or triple if input mechanisms are not properly maintained. Additionally, the lack of contingency planning could significantly affect availability. What happens if the reader, scanner, or camera breaks? What will be the

[7] Advanced Digital Microsystems, Comparison of Biometrics. http://www.admsyst.com/comparison_bio.htm

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

lost productivity to the user and the organization? Does the biometric software allow for alternate authentication should the input mechanism be disabled? Backup units, training, and maintenance need to be accounted for when evaluating technology reliability. The major points to take away here are that order-of-magnitude reliability differences exist between biometric mechanisms, and the CER will escalate when maintenance procedures on input devices are not routinely followed.

Misconception 3

Circumvention of biometric systems are only now being thoroughly tested and with surprising results. In the minds of most people biometric authentication is considered very secure. There is no password to guess or read in clear text over the wire. No tokens, or written passwords to lose or leave in the office. Just your hand, finger, eye, etc. are needed and you won't forget those. What people do seem to forget is that biometric templates (files that contain a user's biometric data) are usually sent clear text from the user's desktop to the authentication server responsible for the biometric comparison. Biometric templates contain a series of numbers determined by a vendor's proprietary algorithm and are not as easily discernable as clear text passwords. However, any file that can be seen (sniffed) on a network can be captured and replayed. I can prove I am Sam if I have Sam's authentication credentials. In this respect, biometric authentication transversing the network in clear text is no more secure than sent clear text passwords. Unless appropriate countermeasures for network sniffing are implemented (VPN, encryption, time stamps, etc) biometric authentication is subject to sniffing and replay attacks.

Forgery of biometric mechanisms is only now being understood and tested [8]. Rubber and latex fingerprints of legitimate users have been forged and used by illegitimate users to circumvent fingerprint systems. In fact, a user's dusted fingerprints have been lifted with adhesive tape (same way law enforcement does) and applied to a scanner with light pressure to gain unauthorized access. Pressure was applied using a baggie filled with a little water. Facial pictures of legitimate users have been used to fool Iris and facial recognition systems. It is not as difficult to fool a biometric system as was once thought.

Misconception 4

As pointed out previously, biometric technology captures an individual's unique attribute(s), and stores it for later comparison. Beyond that function authentication and access control backends actually control the administration, configuration, policy management and access control rules to systems and applications. Some biometric vendors provide fairly complete out-of-the-box solutions, while others provide a toolkit for use in integration into existing environment. Solutions range from authentication only, to

[8] Leyden, John. May 22, 2002. Biometric sensors beaten senseless in tests. http://www.theregister.co.uk/content/archive/25400.html

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

system access control, and a few provide granular access control (applications, directories, folders, files, data objects). Systems integrators can write hooks or utilize Application Programming Interfaces (API) to force current applications to make calls to the biometric system for authentication. Of course this requires a lot of skill, time and resources (=money). Some biometric vendor's provide a framework for biometrics; this means that every system (unless gateways/proxies are used) will require some retrofitting (agents, slave servers & processes, API) to take advantage of biometric mechanisms. So beyond the biometric technology itself is the utility, value and comprehensiveness of the backend systems. Biometric technology should be evaluated in total with the required solution, and not as a stand-a-lone technology. I am often asked which are better fingerprint or voice systems, and other such technology comparisons. The real battleground for success or failure (after 2 or 3 factor authentication on the front end) is the backend systems. How easily can they be modified and adapted to the environment? What functions can they perform? How will the system be administered and what are the points of control? These questions are far more important in the long run to the success of a biometric project, than the type of biometric being used.

Common Biometric Technologies

Table 2 is a chart of common biometric technologies. In researching these comparative approaches I discovered that different authors have slightly different opinions. The technology group that is considered the most accurate consists of Palm Scan, Hand Geometry, Retina, and Iris Scan. While the order accuracy varies from author-to-author, these 4 technologies have the lowest CER [9] [10]. Fingerprints are in the middle tier along with voice recognition. Keystroke and signature dynamics comprise the lower tier. Facial recognition (depending on author) is placed in the middle or lower tier. From vendor-to-vendor, advancements are being made daily to accuracy, reliability and usability of their respective systems. Use charts like Table 2 to begin your research not as a decision making tool.

Biometrics are supposed to be based something you are. Keyboard dynamics (tracks how you type a passphrase) and signature dynamics (characteristics of a signature) are based on an individual's supposed unique behavior. Personally, I believe that falls outside of a true biometric definition. Because of the use of

[9] Rhodes, Keith A. April 25, 2002. National Preparedness: Technology to Secure Federal Buildings. Page 10-11. http://www.cccure.org/Documents/Biometric/secure.pdf

[10] Harris, Shon. 2002. All-In-One CISSP Certification Exam Guide. Page 127-134. New York: McGraw-Hill/Osborne

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

thresholding (exact comparison match of 2 templates not required - just close enough), and because of relatively high CER, keyboard and signature dynamics should not be considered unless the environment being secured is of low value. Medium to high security environments should consider lower CER technologies with lower thresholds.

Common Biometric Technologies

Characteristic	Method	CER	Performance factors	User acceptance
Fingerprints	Patterns of fingertips are captured and compared	Medium	Dryness, dirt, worn, aged fingertips	Medium
Palm Scan	Patterns, shape of palm are captured and compared	Low	Hand injury, age, jewelry	
Hand Geometry	Dimensions of hand and fingers are measured and compared	Low	Hand injury, age, jewelry	High
Retina	Patterns of blood vessels on retina are captured and compared	Low	Glasses, difficult to use	Low
Iris	Patterns of iris are captured and compared	Low	Poor Lighting, movement	High
Face	Facial features are captured and compared	Medium	Lighting, age, glasses, hair, environment	Medium
Signature Dynamics	Rhythm, acceleration, and pressure flow of signature are captured and compared	High	Changing or erratic signatures	High
Keyboard Dynamics	Speed, pressure, of typed passphrase	High	Changing or erratic signatures	High
Voice	Cadence, pitch, and tone of vocal tract are captured and compared	Medium	Noise, colds, weather, age, equipment, environment	High
	* Lower the CER the better the accuracy			

Table 2

With each type of technology listed in Table 2, the user must go through an enrollment process that captures the biometric data and stores it in a reference template for later authentication comparisons. Enrollment times and procedures vary with technology type

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

and the vendor's approach, as well as, the size of the reference template. The range for reference templates size is from 9 bytes – 3k bytes. Enrollment time is a down side of biometrics. In medium to high security environments the enrollment processes needs to be supervised, increasing time and cost of implementation. It is essential that the binding of biometric data to the right individual be highly scrutinized. Sam's fingerprint bound to Steve will allow Sam to impersonate Steve if only 1 factor authentication is used. Also, if 2 factor authentication is used but poorly implemented, such as an ID that is company standardized e.g. first initial, last name, it would still be easy for Sam to impersonate Steve. That is why this author believes that biometrics should substitute for a user's Identification not verification. However, it is still common for biometric data to substitute for the verification, which means that the enrollment (setting up identity and verification mechanisms) must be scrutinized and that care be taken to ensure the secure correct binding.

Biometric Selection Considerations

Biometrics is the most expensive method of verifying a person's identity and implementation obstacles, such as enrollment time, throughput, and user acceptance must considered during the selection process. Costs are coming down, but costs are coming down on other security measures such as certificates, smart cards, and other tokens.

The first step in biometric selection is to determine what your objectives are and why you need biometrics [11]. Are current authentication methods not meeting legal, policy, or productivity requirements? Are authentication tokens being routinely forgotten or lost by employees negatively impacting productivity? Does your environment require medium to high security? Does your back-end authentication system support alternative front-ends such as biometrics. What problem(s) are you trying to solve e.g. eliminate passwords, ID's, smart cards, tokens, increase productivity, reduce risk, tighten security?

Many times there are quality alternatives to biometrics such as One-Time Password tokens, certificate authentication, and Kerberos, which are often cheaper, faster, and more accurate implementations. Hybrid systems that fuse biometric front-ends, to existing authentication infrastructure (Kerberos, PKI, LDAP, NDS) are being strongly considered.

After justifying objectives, and obtaining management's commitment to funding and resources, you can begin to go down the evaluation trail. You will need to draw up your

[11] Wayman, James L., Lisa Alyea, 2000. Picking the Best Biometric for Your Applications. Page 269 – 275. http://www.engr.sjsu.edu/biometrics/nbtccw.pdf

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

environment (# of users, systems, locations, applications, network, wan, workgroups, etc.) and your requirements.

Your requirements should be broken down into several categories from which you will create questions to submit to vendors as a Request for Information (RFI) or Request for Proposal (RFP). Requirement categories will vary from company-to-company, but should still cover the following:

Scope: What will biometrics be used for? Desktop, network, remote, application, database authentication. Will Single sign-on be a requirement? What does the project encompass? What is the timeframe? How many people, systems, locations will be included? What policy, regulation or standard is being addressed?

Performance: How long should an authentication event take? How many concurrent authentications can the system support? How many records can the database hold without losing significant performance? Throughput rates for both enrollment and operation have to be determined.

Enrollment: How long will the enrollment process take? A supervised user will submit biometric data (fingerprint, iris scan, etc.) and fill out employee information (name, employee number, SSN, address, phone, etc.). A supervisor will verify information and authorize storage and creation of user account/record. Some information can also be imported from other sources and only missing information filled in. Once stored, the user will try to authenticate. If successful, the user has been enrolled. This can be a very time consuming process and may have to be done centrally and carefully scheduled to reduce impact to production operations. What will be the reference template size? Will multiple user templates be required? How will enrollments be conducted? What resources are required? What special training is needed for supervisors and users?

Database: Can existing LDAP or relational databases be utilized to store account profiles and templates or does a new database need to be added to the IT infrastructure? What can the database scale to and still be performant? What is the recovery and backup capability of the reference template database? Are auto-recovery functions available?

User Acceptability: Is there a track record of user acceptance of the biometric mechanism. How much and what kind of training is required? What allowances are made for disabled users? What user maintenance is required? Will eyeglasses or jewelry have to be removed when authenticating?

Functional Requirements:

Policy enforcement: What policies do your organization want enforced? Session timeouts, inactivity timeouts, password reuse, failed login lockouts, etc.?

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

Audit & Reporting: What audit records are legally required? How long should they be kept and backed-up? What reports are needed? How are reports and audit logs secured? Are reports configurable? What kinds of report filters are available? Is there a warning when audit logs approach maximum size? How are accesses to audit logs restricted?

Administration: What is desired centralized or decentralized administration? What range of administration is desired, users, accounts, systems, agents, slave servers, database, policy configurations, etc. Is separation of duties important or does the security administrator have full rights and control of everything?

Integration: Integration will allow current systems and applications make calls to the biometric system for authentication, resulting in access control to that system or application. What integration is desired (with applications, existing systems, databases, directories, ERP systems, e-mail, PKI, access control software, websites, SSO authentication systems, VPN, etc.)?

Maintenance & Support: Is 7x24x365 phone support a necessity? Is onsite problem resolution available? What are repair time commitments? How are patches delivered and what is the notification method? Is there remote access fix capability, and if so is it secure? What maintenance is done automatically by the system and what has to be done manually?

Diagnostics & Calibration: Are diagnostics available in the event of a problem? Is there a flow chart of troubleshooting steps? Is calibration required beyond enrollment? What training is required to diagnose and calibrate systems?

Technological: What platforms need to be supported? What high availability, backup, and restoration options are available? What thresholds can be set? What input mechanisms are required/recommended? What is the meantime-between-failure of these input mechanisms? What happens if authentication server or reference template database fails? What is an acceptable FAR? FRR? CER? What standards does the system support? Is the system open or proprietary? Does the system support role based, discretionary, or mandatory access controls?

Once you know your environment, objectives and requirements, vendors are queried for a solution. RFI and RFP are normal information vehicles. During your evaluation of responses you will develop a short list of vendors that have promised you a solution. Now you need to see the solution, first in a demo (perhaps at the vendor's lab), secondly, a pilot at your location. You want to check off on items you have listed as functional requirements. The big gotcha here is that anything is possible through integration and programming, so the vendor may have said yes to every question. You want to select a product that requires the least amount of programming. Rate your functions as met: 1) out of the box, 2) toolkit required, 3) custom programming required.

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

If you make it to the pilot stage, bring in a cross section of users to test with. For example 20% of the world's population does not have a fingerprint suitable for digital scanning. The majority of these people are Asian women. If you never tested Asian women in your pilot you might be in a lot of trouble rolling out the solution. You also need to check for user acceptance of the technology chosen. For example, blindness, glasses, color contact lens, could all be significant factors needing testing in a retina or iris scan solution. Testing usually covers the legitimate users getting access to the system. Try to fool the system by having illegitimate users try to trick the system by smudging the fingerprint scanner, or moving during iris scans, or during the enrollment process.

Look at implementation options as well; there is more than one way to implement products today. Biometric data could be stored on a smart card that the user carries. The card is placed in the card reader, and the user authenticates real time against the template in the card. The software on the desktop controls the authentication so there is no sending of the template over the network. Biometrics can be used to unlock private keys and digital certificates stored on the desktop securing their use for authentication. There are a lot of choices, and each choice has it's own cost and resource requirement. The good news is you are not limited by the lack choices. Just be sure you use 2 or 3 factor authentication and you will be in pretty good shape if you implement with "Best Security Practices" in mind.

The biometric industry does not have many standards. There are some standards for fingerprint format and compression, and there is some work being done on the BioAPI. The BioAPI is released in version 1 and attempts to standardize how biometric calls are made. It has not been widely adopted as of yet. Most biometric implementations today rely on the vendor's proprietary mechanisms. Once standards get established vendors will most likely write to the standard, until then, if the company is financially strong and the product has value, your risk may be minimal.

Summary

Biometric technology is ready for prime time when used in conjunction with other technologies. When part of a 2 or 3 factor authentication scheme biometrics strengthens the authentication process. Biometric authentication traffic between client and server should be encrypted and time stamped to avoid playback, and input mechanisms should be evaluated with accuracy, maintenance, and resistance to forgery in mind. When you select biometric technology look for the lowest CER, narrowest operational threshold, and maximum user acceptance within the budget. Fully understand the backend aspects of the solution. With a good evaluation process, understood objectives, documented requirements, and management commitment a biometric project has a very good chance of success.

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

Appendix A

Glossary [12]

Access control Access control refers to the rules and deployment mechanisms that control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist.

Account An 'account' is the term used most commonly to describe a user's profile which permits access to computer systems. Sometimes the account refers simply to the means of gaining network access to printers and the filing system; in other instances 'accounts' can be application systems' specific and incorporate a range of optional privileges controlling a user's level of access.

Agent A piece of software performing some function on behalf of its user; usually independently, remotely, and unattended.

API Application Programming Interface is code that is added to an application that has preprogrammed instructions that can make program calls to other mechanisms.

Attribute A measurable characteristic.

Audit Log Computer files containing details of amendments to records, which may be used in the event of system recovery being required. The majority of commercial systems feature the creation of an audit log. Enabling this feature incurs some system overhead, but it does permit subsequent review of all system activity, and provide details of: which User ID performed which action to which files when etc. Failing to produce an audit log means that the activities on the system are 'lost'.

[12] http://www.yourwindow.to/information-security/

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

Authentication Refers to the identification and verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and / or data.

Availability Ensuring that information systems and the necessary data are available for use when they are needed.

Biometrics Systems that authenticate (verify the identity of) users by means of physical characteristics, e.g. face, fingerprints, voice, retina pattern, etc.

CER Crossover error rate is a comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.

Certificate A digital certificate is the electronic version of an ID card that establishes your credentials and authenticates you. To obtain a Digital Certificate one must apply to a Certification Authority, which is responsible for validating and ensuring the authenticity of requesting entity. The Certificate will identify the name of the entity, a serial number, the validity date ("from / to") and the entity's Public Key. In addition, the Digital Certificate will also contain the Digital Signature of the Certification Authority to allow any recipient to confirm the authenticity of the Digital Certificate.

Challenge

Response Sometimes referred to as a 'Challenge Handshake' or 'Challenge Protocol', Computer A attempts authentication to computer B. Computer A identifies itself to B. B issues a numeric challenge to A. A performs a mathematical operation on the challenge and generates a response and presents back to B. B receives proper response and completes authentication of A and grants access.

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

Database A collection of files, tables, forms, reports, etc., held on computer media that have a predictable relationship with each other for indexing, updating, and retrieval purposes.

DCE The OSF Distributed Computing Environment (DCE) is an industry-standard, vendor-neutral set of distributed computing technologies. It is the only middleware system with a comprehensive security model. DCE provides a complete Distributed Computing Environment infrastructure. It provides security services to protect and control access to data, name services that make it easy to find distributed resources, and a highly scalable model for organizing widely scattered users, services, and data.

FAR False-acceptance rate is the percentage of imposters incorrectly matched to a valid user's biometric. Type I Error.

FRR False-rejection rate is the percentage of incorrectly rejected valid users. Type II Error.

Enrollment The initial process of collecting biometric data from a user and then storing it in a template for later comparison.

Identification The process by which the biometric system identifies a person by performing a one-to-many (1:*n*) search against the entire enrolled population.

Kerberos Authentication protocol that provides SSO for a wide variety of distributed systems, utilizes symmetric key encryption.

LDAP Lightweight Directory Access Protocol is a standard way to store and access information stored in directories and databases.

NDS Novell Directory Service is Novell's LDAP compliant directory.

OTP One-Time-Password is a token that generates a new password value every X seconds. The password a user enters will never be used again to capture of the password would not do any harm.

Passphrase A sentence or phrase that is used as a password for authentication purposes.

PKI Public Key Infrastructure is a system for publishing the public-key values used in public-key cryptography. There are two basic

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

operations common to all PKI: *Certification* is the process of binding a public-key value to an individual, organization or other entity, or even to some other piece of information, such as a permission or credential. *Validation* is the process of verifying that a certification is still valid.

Playback Authentication information is recorded and playback for later use. A technique used to gain unauthorized access.

Reference

Template A mathematical representation of biometric data. A template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition.

SSO Single Sign-on is a mechanism that the user will authenticate one time and get access to all entitled resources.

Token Portable personal physical security item such as an OTP device, smart card, USB fob, that is required in the authentication process.

Verification The authentication process by which the biometric system matches a captured biometric against the person's stored template (1:1).

© SANS Institute 2002, Author retains full rights.

References

Bibliographies and References cited in this paper:

1. Chen, Anne. Nov 5, 2001. Prescription for PKI Success. http://www.eweek.com/article2/0,3959,148423,00.asp .

2. Flynn, H. April 10, 1998. SSO Magic Quadrant. http://www.gartner.com/reprints/platinum/m034848.html

3. Ediger, Bruce. October 19, 1999. 10 Reasons OSF DCE Sucks. http://www.users.qwest.net/~eballen1/anti_dce.html

4. Liu, Simon., and Mark Silverman, A Practical Guide to Biometric Security Technology. http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm

5. Scheier, Robert. January 10, 2002. Biometrics: Improving but not perfect. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci798104,00.html?FromTaxonomy=%2Fpr%2F286152

6. Tipton, Hal., Donald R. Richards, Donald R. 1999. Handbook of Information Security Management: Biometric Identification. Boca Raton: Auerbach Publications http://www.cccure.org/Documents/HISM/033-037.html

7. Advanced Digital Microsystems, Comparison of Biometrics. http://www.admsyst.com/comparison_bio.htm

8. Leyden, John. May 22, 2002. Biometric sensors beaten senseless in tests. http://www.theregister.co.uk/content/archive/25400.html

9. Rhodes, Keith A. April 25, 2002. National Preparedness: Technology to Secure Federal Buildings. Page 10-11. http://www.cccure.org/Documents/Biometric/secure.pdf

10. Harris, Shon. 2002. All-In-One CISSP Certification Exam Guide. Page 127-134. New York: McGraw-Hill/Osborne

11. Wayman, James L., Lisa Alyea, 2000. Picking the Best Biometric for Your Applications. Page 269 – 275. http://www.engr.sjsu.edu/biometrics/nbtccw.pdf

12. http://www.yourwindow.to/information-security/

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

Last Updated: May 21st, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced