

Access Control Identification

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: access_control_identification.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Identification

- **Is the means by which a user provides a claimed identity to the system**
- **The act of a user professing an identity to a system**
- **Ensuring that a subject is the entity it claims to be**
- **User identification enables accountability**
- **Usually takes the form of Logon ID or User ID**
- **Logon ID characteristics**
 - They must be unique
 - Not shared
 - Non descriptive of job function
- **ID Public Information**
 - User name ID
 - Department ID
 - Account ID
 - Employee number
 - Terminal ID
- **ID Private information**
 - Static passwords
 - Dynamic passwords
 - Cognitive passwords
 - Smart Tokens
 - Memory Tokens
 - Biometrics

❖ Authentication

- **Proving the identity**
- **Verification that the users claimed identity is valid**
- **Authentication is what you are authorized to perform, access, or do**
- **The entity could be individual user, machine, or software component**
- **Something U knows (TYPE I)**
 - User ID
 - Passwords
 - PINs
 - Cryptographic keys
- **Something U has (TYPE II)**
 - Memory tokens

- **Smart tokens**
- **Something U Are (TYPE III)**
 - **Biometric**
 - **Fingerprint**
 - **Characteristic-based (biometrics, behaviour)**

❖ **Authorization**

- **Right to Perform the tasks or the access requested**
- **Determines whether a user is trusted for that operation**

❖ **One-time Passwords**

- **Tokens**
 - **Introduction**
 - A software or hardware object used to verify an identity in an authentication process
 - The entity that currently holds the token has exclusive access to the resource
 - User-controlled, physical device used to verify an identity
 - **General usage**
 - An object that is used to control access and is passed between cooperating entities
 - Usually, the entity that currently holds the token has exclusive access to the resource.
 - **Synchronous**
 - Synchronous is based on TIME or EVENT driven mechanisms
 - Time-based
 - Event-based
 - **Asynchronous**
 - Asynchronous is based on challenge response
 - **Not vulnerable to**
 - Electronic eavesdropping
 - Guessing
 - Wiretapping
 - Sniffing
 - Mismanagement
 - They provide two-factor authentication
- **Single Sign-On (SSO)**
 - **Definition**
 - Users identify only once to a system
 - Make the use of multiple passwords transparent to the user
 - Pro's
 - ◆ More efficient user log-on process
 - ◆ The ability to use stronger passwords
 - ◆ Easier administration changing or deleting the passwords
 - ◆ Uniform security controls
 - Con's
 - ◆ Once user has logged on, they can freely roam the network
 - ◆ Single point of failure is a security risk due to concentration of risk in one place
 - **Kerberos**
 - Was developed at MIT
 - KDC knows secret keys of Client and Server
 - Use Symmetric Key Cryptography

- It authenticates clients to other entities on a network
- A secret key is shared between the KDC and the user
- The session key is shared between two users
- Ticket granting Service TGS grants temporary Ticket (symmetric key)
- Main components
 - ♦ KDC
 - Key Distribution Center (KDC)
 - The most important part of the system
 - Holds all of the secret keys
 - Provides both authentication and key distribution
 - Trusted by the entire Kerberos domain
 - ♦ Principals
 - Users, applications, services, etc.
 - All principals share a secret key with the KDC
 - ♦ Ticket
 - Generated by KDC and given to principal
 - ♦ Realms
 - Allows an administrator to logically group resources
 - ♦ Terms
 - TGS - Ticket Granting Service
 - AS - Authentication Server
 - KDC - Kerberos-trusted Key Distribution Center
- Kerberos Process
 - ♦ The user and the KDC share a secret key
 - ♦ The requested service and the KDC share a different secret key
 - ♦ The user and the requested service do not share a secret key
 - ♦ The user authenticates to the KDC
 - ♦ KDC's Ticket Granting Service (TGS) sends a ticket
 - ♦ Ticket to be used between the user and the requested service
 - ♦ User sends the ticket to the requested service
- Kerberos weaknesses
 - ♦ Replay is possible within time frame
 - ♦ TGS and Auth server are vulnerable as they know everything
 - ♦ Initial exchange passed on password authentication
 - ♦ Keys are vulnerable
 - ♦ Session keys Vulnerable to password guessing
- **SESAME**
 - Secure European System for Applications in a Multi-vendor Environment
 - Uses Needham-Schroeder protocol
 - Use a ticket for authorization called "Privilege Attribute Certificate"
 - Uses public key cryptography
 - Supports MD5 and CRC32 Hashing
 - Uses two tickets
 - ♦ 1) One contains authentication
 - ♦ 2) One contains the access rights to the client
 - SESAME weaknesses
 - ♦ Only authenticates by using first block of message
 - ♦ Initial exchange passed on password authentication
- **KryptoKnight**
 - Peer to peer relationship between KDC
 - Uses a trusted Key Distribution Center (KDC)

- NetSP is based on KryptoKnight
- Provide Authentication
- Provide Key Distribution
- Provide Data Privacy
- Provide Data Integrity
- Provide SSO
- **Scripting**
 - Many scripts run in the background to log that user
 - This method is extremely hard to maintain
- **Thin Clients**
 - Terminals with no operating system or hard drive
 - This forces the user to authenticate to the network

❖ Passwords

➤ Password Types

- **Good passwords can provide you with a good first line of defense**
- **Static**
 - Are normal password with or without expiration
 - Same each time and They are reusable
- **Dynamic**
 - Changes each time you logon
 - Password are good for one time only
- **Cognitive**
 - Use fact based and opinion based data as a basic for authentication
 - Example
 - ◆ What is your favorite actor, What is your favorite vegetable

➤ Several Schemes can be used

- **User Selected**
- **Generated**
- **Token generated**
- **Composition - Combination of two, totally unrelated words**
- **Passphrases - Good way of having very strong passwords**

➤ Management

- **Length Range**
 - Minimum length through a maximum length
 - All acceptable number of characters
- **Lifetime Consideration**
 - Cost of replacement (administrator time)
 - Risk of compromise
 - Distribution risk
 - Probability of guessing
 - Number of times used
 - Is the maximum acceptable period of time for which a password is valid
 - Password should be changed often if the cost of replacement is reasonable
 - Password should be changed quickly when a system is compromised
 - You should maintain a record of when a password was created and changed
- **Source**
 - Is the entities which can create or select a valid password

- The source passwords should be selected by the security officer
- Selected Password should be tested by an automated password system
- **Changing passwords consideration**
 - 60 days regular users
 - 30 days privilege users
 - 15 days security officers
 - User changes own passwords at expiration
 - Audit trail of password changes
 - By phone you must call back the user (only from office phone)
- **Ownership**
 - Is the set of individuals who are authorized to use a password
 - Access password should only be known to the person who own it
 - Each individual is responsible for providing protection for their passwords
- **Distribution**
 - Is set of acceptable methods for transporting a new password to its owner
 - An audit record containing the date and time of a password
- **Entry**
 - Is the set of acceptable methods by which a password may be entered
 - The number of allowed password entry attempts should be limited by the officer
- **Access Control Record Management**
 - It is necessary to clean up your user database once in a while
 - Here are a few steps
 - ◆ Remove obsolete userids bimonthly
 - ◆ Compare with payroll (everyone gets paid) and human resource for an up-to-date list of employees.
 - ◆ Suspend inactive use rids (accounts) after 30-60 days
 - ◆ Delete suspended userids 30-60 days after suspension
 - ◆ Remove redundant UID, accounts, role-based groupings from resource ACL
 - ◆ Remove redundant resource rules from UID, accounts, and role based groups.
- **Collusion**
 - Accure when one person controlling a component part collaborates with others to breach the security of a system

➤ **Password validation**

- **In order to identify and authenticate a system user two steps are suggested**
- **Public Information**
 - User name ID
 - Department ID
 - Account ID
 - Employee number
 - Terminal ID
- **Private information**
 - Static passwords
 - Dynamic passwords
 - Cognitive passwords
 - Smart Tokens
 - Memory Tokens
 - Biometrics

➤ **Problems With Passwords**

- **Guessing or finding passwords**
- **Giving passwords away**
- **Electronic monitoring (sniffing)**
- **Accessing the password file**

➤ **Improving Password Security**

- **Use password generators**
- **Put limits on log-in attempts**
- **Use password attributes**
- **Change passwords frequently**
- **Put restrictions on password reuse**
- **Protect password files**

❖ **Memory card, Smart card, key card**

➤ **Cryptographics Keys**

- **A private key that should be in the possession of one person**
- **Digital signature uses a private key to encrypt a hash value**
- **The act of encrypting the hash value is called "Digitally signing a message"**
- **Private keys and digital signature are other mechanisms used to authenticate an individual**

➤ **Tokens**

- **Introduction**
 - **A software or hardware object used to verify an identity in an authentication process**
 - **The entity that currently holds the token has exclusive access to the resource**
 - **2 types of token devices**
 - ◆ **Synchronous is based on TIME or EVENT driven mechanisms**
 - ◆ **Asynchronous is based on challenge response**
- **Token Benefits**
 - **Not vulnerable to**
 - ◆ **Electronic eavesdropping**
 - ◆ **Guessing**
 - ◆ **Wiretapping**
 - ◆ **Sniffing**
 - ◆ **Mismanagement**
 - ◆ **They provide two-factor authentication**
- **General usage**
 - **An object that is used to control access and is passed between cooperating entities**
 - **Usually, the entity that currently holds the token has exclusive access to the resource.**
- **Authentication usage**
 - **A data object or a portable, user-controlled, physical device used to verify an identity in an authentication process**

➤ **Memory Only Card**

- **This type of card is the most common card**
- **Memory card holds information but does not process it**
- **These cards can contain private information in the read-protected area.**
- **It has a magnetic stripe on the back**
- **Like the one used as Telecards for telecom payments**
- **Can offer two-factor authentication, the card itself (something you have) and the PIN (something you know).**

- These memory cards are very easy to counterfeit.
- There are more sophisticated cards. with some area read protected by a key

➤ **Smart Card or Memory card**

- **Smart Card or Memory card with some fixed logic (i.e. for encryption)**
- **Has appeared since the middle of the 1980's called smart cards or chip cards**
- **These cards are far more secure than the magnetic cards**
- **The basic smart card standard is the ISO 7816 series**
- **IC cards can be categorized by the capabilities of the chip:**
- **Smart card provides a two-factor authentication (PIN something you know) and The card it self (Something you have)**
- **Smart card are more expensive than memory cards**
- **There are several types of cards**

➤ **Overview of Smarcard from SCIA**

- **A smart card has built-in hardware and logic to process information**
- **Is a credit-card sized plastic card with an embedded computer chip**
- **The chip can either be a microprocessor with internal memory or a memory chip with non-programmable logic**
- **The chip connection is either via direct physical contact or remotely via a contact less electromagnetic interface**
- **Major rollouts such as the French National Visa Debit Card and France Telecom**
- **Types**

- **Contact micromodule which is embedded into a plastic substrate**
 - ♦ Micromodule embedded into the plastic substrate or card
 - ♦ Either a cold or hot glue process bonds the micormodule to the card
- **Contactless card requires only close proximity to a reader**
 - ♦ Derive the internal chip power source from this electromagnetic signal
 - ♦ The range is typically two to three inches for non-battery powered cards
 - ♦ The antenna is typically 3 - 5 turns of very thin wire (or conductive ink), connected to the contactless chip
- **Combi cards and Hybrid cards**
 - ♦ A Hybrid card has two chips, each with its respective contact and contactless interface
 - ♦ The two chips are not connected
 - ♦ It is now possible to access the same chip via a contact or contactless interface
- **There are microprocessor-cards**
 - ♦ The cards work following the ISO-7816 protocol
 - ♦ These are the safest
 - ♦ These cards have their own internal operating system
 - ♦ These cards are used when confidentiality is needed, like credit cards
 - ♦ Encrypted TV access cards
 - ♦ Health cards, and SIM cards for GSM, etc
- **The chips used in all of these cards fall into two categories**
 - ♦ **Microprocessor chips**
 - A microprocessor chip can add, delete and otherwise manipulate information in its memory
 - It can be viewed as a miniature computer with an input/output port, operating system and hard disk
 - Microprocessor chips are available 8, 16, and 32 bit architectures
 - Their data storage capacity ranges from 300 bytes to 32,000 bytes
 - ♦ **Memory chips**
 - Viewed as small floppy disks with optional security

- Memory cards can hold from 103 bits to 16,000 bits (2000 Bytes) of data
- They are less expensive than microprocessor cards
- They depend on the security of the card reader for their processing
- Ideal when security requirements permit use of cards with low to medium security
- **Wired Logic aka Intelligent Memory cards**
 - ◆ Contain some built-in logic
 - ◆ Used to control the access to the memory of the card
- **Processor cards contain memory and a processor**
 - ◆ They have remarkable data processing capabilities
 - ◆ Processing power is used to encrypt/decrypt data
 - ◆ Data processing also permits dynamic storage management
- **Applications**
- **Smartcard Attacks**
 - **Logical attacks**
 - Sensitive information is gained by examining the bytes going to and from the smartcard
 - One example is the so-called "timing attack"
 - This attack does require that the PIN to the card be known
 - **Physical attacks**
 - Temperature, clock frequency, voltage, etc, are altered in order to gain access to sensitive information on the smartcard
 - Another type involve an intense physical fluctuation at the precise time and location where the PIN verification takes place
 - Can be performed even though the PIN is unknown
 - **Trojan Horse attacks**
 - Trojan horse application that has been planted on an unsuspecting user's workstation
 - Trojan horse waits until the user submits a valid PIN from a trusted application
 - The countermeasure to prevent this attack is to use "single-access device driver" architecture
 - **Social Engineering attacks**
 - This type of attack is usually the most successful
- **They require a reader connected to each of the hosts.**

❖ **Characteristic-based (biometrics, behaviour)**

- **Definition**
 - **Take advantage of an individual's unique physical characteristics in order to authenticate that person's identity**
 - **Biometrics - something you are**
 - Identification
 - ◆ One-To-Many Relation
 - ◆ Physical Control
 - Authentication
 - ◆ One-To-One Relation
 - ◆ Logical or technical Control
- **Three main performance measures**
 - **False Rejection Rate (FRR) or Type 1 error**
 - The percentage of valid subjects that are falsely rejected.
 - **False Acceptance Rate (FAR) or Type 2 error**
 - The percentage of invalid subjects that are falsely accepted.
 - **Crossover Error Rate (CER)**

- The percent in which the FRR equals the FAR
- CER of 3 will be more accurate than CER 4

➤ **Order of Effectiveness**

• **Palm Scans**

- Include creases, ridges and grooves also includes the fingerprints of each finger
- This information is compared to a reference file

• **Hand Geometry**

- Hand geometry is the 'granddaddy' of all biometric technology devices
- Measure or record the physical geometric characteristics of an individual's hand.
- Measure length of fingers and thumb, widths, and depth
- Charge-coupled device (CCD) digital camera is used to record the hand's three-dimensional shape
- Profile or 'template' is constructed which the user will use to compare against subsequent hand readings
- Small reference templates file, generally under ten bytes
- Scanning devices usually fall into one of two categories
 - ◆ Mechanical
 - ◆ Image-edge detection
- Devices employed today take over 90 measurements of the length, width, thickness, and surface area of a person's hand and fingers
- Capturing one's hand measurements occurs with amazing speed, within one second
- Advantages to using hand geometry
 - ◆ Speed of operation
 - ◆ Reliability
 - ◆ Accuracy
 - ◆ Small template size
 - ◆ Ease of integration into an existing system
 - ◆ User-friendliness

• **Iris Scan**

- The iris is the colored portion of the eye that surrounds the pupil
- The iris unique patterns, rifts, colors, rings, coronas, and furrows
- The human iris has more than 400 measurable variables of which the Iridian Technologies process uses about 240 [Iridian].
- 240 points of reference are digitized
- Then stored into a 512-byte record
- The subject looks at the video camera from a distance of 3-10 inches can be done from distances up to 40 inches
- The scan excludes the lower portion of the iris because of inherent moisture and light reflection
- The entire enrollment process is less than 20 seconds, and subsequent identifications take 1 - 2 seconds
- Eyeglasses and contact lenses present no problems to the quality of the image, and the system further tests for a live eye rather than, say, a lens
- Does offer advantages of accuracy and ease-of-use over other biometrics.
- One potential disadvantage is that there must be a certain level of light for successful imaging

• **Retina Scan**

- Retinal Scan technology maps the capillary pattern of the retina, a thin (1/50th inch) nerve on the back of the eye
- To enroll, a minimum of five scans is required, which takes 45 seconds

- The subject must keep his head and eye motionless within ½" of the device, focusing on a small rotating point of green light
- Then stored into a 35-byte record
- This compares to 30-70 points of reference for a finger scan.
- Unfortunately a retinal scan is considerably more intrusive than an iris scans and many people are hesitant
- **Fingerprint**
 - Intro
 - ♦ Every person's fingerprint is unique
 - ♦ Fingerprint authorization is potentially the most affordable and convenient method
 - ♦ The lines that create a fingerprint pattern are called ridges
 - ♦ The spaces between the ridges are called valleys
 - ♦ The unique fingerprints are compared by "Minutiae"
 - Ridge endings
 - Bifurcations
 - ♦ Scanner take a mathematical snapshot and save it as a minutia file
 - ♦ The minutia file that is stored in the database
 - ♦ The minutia file cannot ever be reconverted back to the original
 - ♦ Total time for fingerprint =
 - Finger scanning time +
 - User identification time +
 - Finger position time
 - Potential Issues
 - ♦ Privacy
 - ♦ False Rejection False Acceptance
 - ♦ Accuracy
- **Voice Pattern**
 - Advantages to using voice identification
 - ♦ Considered a "natural" biometric technology
 - ♦ Provides eyes and hands-free operation
 - ♦ Reliability
 - ♦ Flexibility
 - ♦ Timesaving data input
 - ♦ Eliminate spelling errors
 - ♦ Improved data accuracy
 - Requires that a "voice reference template" be constructed so that it can be compared against subsequent voice identifications.
 - To construct the "reference template" an individual must speak a set phrase several times as the system builds the template.
 - Voice identification systems incorporate several variables or parameters in the recognition of one's voice/speech pattern including pitch, dynamics, and waveform
 - A major concern for voice identification systems is how to account for the variations in one's voice
 - To help eliminate these types of variations during voice identification, a process comprising Hidden Markov Modeling is applied
 - Error rates that use this type of language modeling are from one to 15 percent
 - Five specific forms of voice identification
 - ♦ Speaker Dependent
 - Hold a vocabulary of between 30,000 and 120,000 words
 - ♦ Speaker Independent
 - As a trade off, the vocabulary is smaller and error rates higher.
 - ♦ Discrete Speech Input

- Make small pauses, as small as 1/10 of a second, between words
 - ◆ Continuous Speech Input
 - Can only recognize a limited amount of words and phrases
 - Also referred to as "word-spotting" systems
 - ◆ Natural Speech Input
 - This is the most desired form of voice identification
 - **Facial Scan**
 - Offers the lowest CER
 - Individuals can immediately distinguish among people just by looking at their face
 - Facial feature identification is considered to be one of the most natural biometric technologies
 - The process of facial identification incorporates two significant methods: detection and recognition.
 - Detection involves locating the human face within an image captured by a video camera
 - Recognition is comparing the captured face to other faces that have been saved and stored in a database
 - Facial feature identification involves either eigenfeatures (facial metrics) or eigenfaces
 - Eigenfeature system approach strives to determine the distances between such facial features as the nose, eyes, bone structure, mouth, and eyebrows
 - These eigenfeatures are then compared against saved eigenfeatures in a database
 - Most facial feature identification systems today only allow for two-dimensional frontal images of one's face.
 - Thermal imaging systems employ an infrared camera to capture the pattern of blood vessels under the skin of one's face
 - Advantages to this system are that it can be used in complete darkness and is not as effected by facial changes and position.
 - **Handwritten Dynamic signatures**
 - Signature identification, also known as Dynamic Signature Verification (DSV)
 - Currently, off-the-shelf digitizers cost as little as \$99
 - Signature identification involves the method of trying to differentiate between the parts of the signature that are habitual (consistent) and those that alter with each signing (behavioral)
 - Signature identification systems analyze two different areas
 - ◆ The specific features of the signature
 - ◆ Specific features of the process of signing one's signature
 - Features that are taken into account
 - ◆ Speed, pen pressure, directions, stroke length
 - ◆ The points in time when the pen is lifted from the paper
 - **Keystroke Pattern**
 - Keystroke dynamics requires, as with most biometric technologies, a "reference template"
 - Is considered one of the most unusual and innovative biometric technologies
 - Keystroke dynamics looks at the way a person types at a keyboard
 - Keyboard dynamics measures two distinct variables:
 - ◆ "dwell time"
 - Which is the amount of time you hold down a particular key
 - ◆ "flight time"
 - Which is the amount of time it takes a person to between keys
 - Keyboard dynamics systems can measure one's keyboard input up to 1000 times per second
- **Biometric Issues**

- Enrollment Time - Acceptable rate is 2 minutes per person
- Throughput Time - acceptable rate is 10 people per minute
- Acceptability Issues - privacy, physical, psychological
- Network crashes, power failures, hardware failures, and software problems are all possible ways in which a biometric system could become unusable

➤ **Vulnerabilities of Biometrics Systems**

- **Physical robustness of the user facing devices**
 - Security of physical connectivity between authentication points and the host system
- **Security of third party networks**
- **Security of back end authentication engine and associated interfaces**
- **Security of processes within host controller**
- **Inherent biometric device performance**
- **Overall authentication procedures**
- **Conclusions**
- **The Zephyr**
 - User Criteria
 - System Criteria
 - Order of effectiveness
 - Order of acceptance

❖ **Line of Defenses**

➤ **First line of defenses**

- **Policies and procedures against peoples bad behavior**
- **Internal controls, especially preventive controls**
- **Passwords and user identification**
- **Firewalls against network compromises**
- **Separation of duties against errors, omissions, irregularities**
- **Training awareness and education**
- **Physical security controls e,g keys locks guards**
- **Network monitors against spoofing attacks**
- **Quality assurance against poor quality or poor integrity**
- **Fault tolerant and redundancy against data loss and DOS**
- **Dial-back technique against unauthorized dial access**
- **Backup files against loss of data**
- **Limited unsuccessful attempts prior to login**
- **Perimeter barriers against property damage, physical intrusion**
- **Integrity verification software against poor quality data**
- **System isolation techniques against virus and other attacks**
- **Split knowlege procedures against compromise of system integrity**
- **Security containers to place objects**

➤ **Second line of defenses**

- **Audit trails and logs against unauthorized actions**
- **Monitoring against unauthorized actions**
- **Attack detection software against harmful attacks**
- **Penetration testing against circumventing security features of a system**
- **Exterior protection such as walls and ceilings against unauthorized entry**

➤ **Last line of defenses**

- **Software testing against design and programming defects**
- **Insurance against disasters natural and man-made**
- **Security containers to place objects**
- **Backup files against loss of data**
- **Configuration management practices against improper release**
- **Quality and integrity control against poor quality**
- **Contingency planning against unforeseen events and conditions**
- **Employee vigilance against anything is not mentioned in first and second line**