

Access Control Authentication

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: access_control_authentication.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.*

❖ Introduction

- **Authentication**
 - **Proving in some way that you are, who you say you are**
 - **Authentication is performed prior to authorization**
- **Auditing/accounting**
 - **What are you allowed to see**
- **Authorization**
 - **Process determines who is trusted for a given purpose**
- **Security Checklist**
 - **Proof of identity (authentication)**
 - **Access permissions (authorization)**
 - **Eavesdropping prevention/Encryption (confidentiality)**
 - **Protection of information from modification (integrity)**
 - **Proof of involvement (non-repudiation)**
 - **Connectivity between parties (availability)**

❖ Access control

- **The process by which you restrict access to computing resources.**
- **Allows you to enforce the security principle of least privilege**
- **Enforcement of access control is handled by the operating system**
- **MAC/**
 - **Based approach using labels**
 - **Bell-LaPadula**
 - **Introduction**
 - ♦ The bell-Lapadula model deal only with Confidentiality
 - ♦ Military-strength access control.
 - ♦ Every object gets a classification label
 - ♦ Subjects, are assigned a privilege level, called a clearance.
 - ♦ Labels may be used to define projects as well.
 - ♦ Prevent information flow from HIGH level to low level
 - ♦ Based on Government Classification
 - Unclassified
 - Sensitive But Unclassified (SBU)
 - Confidential
 - Secret
 - Top Secret
 - ♦ Bell Lapadula model use lattice
 - ♦ Lattice Based uses less than or equal to relation
 - ♦ A Lattice provides an upper Bound and a lower bound of authorized access

- 3 multilevel
 - ♦ . Simple Security Property (SS)
 - No reading from lower subject to higher object (No Read Up)
 - User can read data only if its security level \leq their clearance level
 - ♦ . * Security Property (Star)
 - A subject cannot write to an object at a lower level (No write Down)
 - User can only write to objects whose security level is \Rightarrow to their own
 - Strong * property - no reading or writing to another level
 - Trusted Subject can violate the star property but not its intent
 - ♦ . Discretionary Security Property (DS)
 - Uses an access matrix to specify discretionary access controls.
 - Discretionary access can be
 - Content Dependent - access decisions based on data content
 - Context Dependent - access based in subject or object attributes
 - ♦ Tranquility property,
 - Security level of an object cannot be changed while it is in use by the computer system
- Limitations of BLP
 - ♦ BLP is intended for systems with static security levels
 - ♦ Restricted to confidentiality
 - ♦ No policies for changing access rights
 - ♦ Does not address covert channels
 - ♦ Does not address modern systems that use file sharing and server
 - ♦ Covert channels are not detected by BLP modeling
- **DAC involves an (ACL)**
 - ACLs offer no protection against malicious programs like Trojan
 - ACL is assigned to an object,
 - Capability list is assigned to a user
 - An alternative to ACLs is to use capability lists for each system user
- **Mandatory (MAC)**
 - **Cannot be made restrictive by the subject**
 - **Owner controls access to resources they own.**
 - **Dependent on Labels and data classification**
 - **Must have Need to know**
 - **DAC models include**
 - Owner-based
 - Access matrix
 - Centralized
 - Decentralized or distributed
 - **DAC is often implemented via ACLs.**
 - **Subjects Clearance must match Classification of Object**
 - **Mandatory controls are prohibitive**
 - **Military Labels**
 - Unclassified
 - Confidential
 - Secret
 - Top secret
 - **ACLs are not a defense against Trojan horse**
- **Non-Discretionary (Role Based) RBAC**
 - **Permissions are based on user job roles**

- **A central authority determines what subjects can have access to certain objects**
- **Defined in terms of organization structure and roles.**
- **Used to Enforce minimum privileges for general system users**
- **Often useful in organizations where there are frequent personnel changes**
- **These controls may be based on**
 - **Role-Based**
 - ♦ Role based access control (RBAC)
 - ♦ Based on the roles that individual users have as part of an organization
 - ♦ Access rights are grouped by role name
 - ♦ Reducing the complexity and cost of security administration in large networks
 - ♦ Role based access control (RBAC) is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies
 - ♦ Access is determined by the role the user has within the company
 - **Rule-Based**
 - ♦ A security policy based on global rules imposed for all users.
 - ♦ A good example could be a firewall
 - ♦ Rule based access control is based on a specific profile for each user
 - ♦ Access is determined by the task assigned to this user
 - ♦ Policy Based Access Control is also known as Rule Set Based Access Control (RSBAC).
 - **Lattice is non-discretionary control**
 - ♦ Was developed to deal mainly with information flow in computer systems.
 - ♦ The basic work in this area was done around 1970
 - ♦ Information flow in computer systems is concerned with flow from one security class (also called security label)
 - ♦ A lattice is a mathematical object that characterises a relationships between things
 - ♦ A set and a relationship(\leq) between members
 - ♦ There are pairs of elements
 - Subject
 - Object
 - ♦ There are pairs of elements that have
 - LEAST upper bound of values
 - Greatest lower bound of values
 - ♦ Access is determined by the sensitivity level assigned to tje role
- **Lattice based**
 - Provides least access privileges of the access pair
 - Greatest lower bound
 - Lowest upper bound

❖ **Authentication**

- **Proving who you claim to be**
- **Verification that the users claimed identity is valid**
- **Proving in some way that you are, who you say you are**
- **The entity could be individual user, machine, or software component**
- **3 means of authenticating a user's**
 - **Something a user knows (TYPE I)**
 - User ID
 - Passwords
 - PINs
 - Cryptographic keys
 - **Something a user has (TYPE II)**

- Memory tokens
- Smart tokens
- **Something a user is (TYPE III)**
 - Biometric
 - Fingerprint

➤ **Kerberos**

- **Is an authentication authorization mechanism used on larger networks**
- **Was developed at MIT**
- **Use Symmetric key encryption**
- **Does not send the user's password across the network**
- **AS - Authentication Server creates two session keys, which are temporary**
- **The KDC - Key Distribution Center knows secret keys of Client and Server**
- **It authenticates clients to other entities on a network**
- **A secret key is shared between the KDC and the principal**
- **The session key is shared between two principals**
- **Ticket granting Service TGS grants temporary Ticket (symmetric key)**
- **Kerberos uses TCP port 88 and UDP port 88.**
- **Kerberos Assumptions**
 - Assumes the use of a strong password
 - Kerberos authentication uses session keys that are valid only for one session
- **Initial Exchange**
 - Client sends Hash Password to the TGS Server
 - TGS verifies with the Auth. Server
 - TGS Server responds with
 - ◆ 1) Key for Client and TGS server encrypted with Client Key $[K(c, tgs)]K_c$
 - ◆ 2) Ticket Granting Ticket (TGT) = $[K(c, tgs), c, a, v]K(tgs)$
- **Request for Service**
 - Client sends request for service to TGS with
 - ◆ 1) TGT = $[K(c, tgs), c, a, v]K(tgs)$
 - ◆ 2) Authenticator $K(c, tgs)$
- **TGS sends Client back ticket for server and authenticator for server**
 - 1) Ticket $T(c, s) = [s, c, a, v, K(c, s)]K_s$
 - 2) $[K(c, s)]K(c, tgs)$
- **Client sends Server**
 - 1) Ticket $T(c, s) = [s, c, a, v, K(c, s)]K_s$
 - 2) authenticator = $[c, t, key]K(c, s)$
- **Kerberos design assumes that**
 - Mutual authentication is optional
 - Passwords are encrypted
- **Kerberos features**
 - Scalability for large environments
 - Authentication over untrustworthy networks
- **Kerberos weaknesses**
 - Vulnerable to Replay and brute-force password guessing
 - TGS and Auth server are vulnerable as they know everything
 - Initial exchange passed on password authentication
 - Keys are vulnerable

➤ CHAP

- **CHAP uses a 3-way handshake**
- **CHAP protects against session hijacking**
- **Supports encryption, protects password**
- **CHAP features**
 - A three-way handshake
 - Repeats the challenge at random intervals

➤ Certificates

- **Goal of certificates is to establish trust among clients**
- **Issued by a Certificate Server.**
- **Allow a user to**
 - Encrypt a message (Privacy)
 - Confirm a message was not modified (Integrity)
 - Confirm the sender identity (non-repudiation)

➤ Username/Password

- **Good passwords can provide you with a good first line of defense**
- **The username is unique to each individual user.**
- **The password is supposed to be kept secret**
- **Password should not be a name found in a native language**
- **It should also not be something easily guessable**
- **Password Types**
 - 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
 - ♦ What is your favorite actor, What is your favorite vegetable
- **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)

➤ Tokens

- **Assumed to be an RSA SecureID token-type**
- **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**
- **All SmartCards utilize Certificates**
- **2 types of token devices**
 - Synchronous is based on TIME or EVENT driven mechanisms
 - Asynchronous is based on challenge response
- **Not vulnerable to**
 - Electronic eavesdropping

- Guessing
- Wiretapping
- Sniffing
- Mismanagement
- They provide two-factor authentication
- **Multi-Factor**
 - Involves the use of any two or more of these concepts together
 - Requiring the user to furnish more than one type of proof of identity
- **Mutual Authentication**
 - Involves both parties authenticating themselves to each other.
 - It's a two-way transaction.
- **Biometrics**
 - **Identification**
 - One-To-Many Relation
 - **Authentication**
 - One-To-One Relation
 - **Something you are (physiological)**
 - **Something you do (behavioral)**
 - **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
 - 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
 - ♦ Over 90 measurements of the length, width, thickness, and surface of a hand
 - ♦ Small reference templates file, generally under ten bytes
 - ♦ Scanning devices usually fall into one of two categories
 - Mechanical
 - Image-edge detection
 - ♦ 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

- ◆ 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
- ◆ The scan excludes the lower portion of the iris because of inherent moisture
- ◆ The entire enrollment process is less than 20 seconds
- ◆ Eyeglasses/contact lenses present no problems to the quality of the image
- ◆ Disadvantage must be a certain level of light
- Retina Scan
 - ◆ Retinal Scan technology maps the capillary pattern of the retina
 - ◆ To enroll, a minimum of five scans is required, which takes 45 seconds
 - ◆ 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
- 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
 - ◆ Incorporate pitch, dynamics, and waveform
 - ◆ 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
 - ◆ Considered to be one of the most natural biometric technologies
 - ◆ The process incorporates two significant methods: detection and recognition.
 - ◆ Identification involves either eigenfeatures (facial metrics) or eigenfaces
 - ◆ Eigenfeature determine the distances between such facial features
 - ◆ Thermal imaging systems employ an infrared camera
 - ◆ Advantages to this system are that it can be used in complete darkness
 - Handwritten Dynamic signatures
 - ◆ Signature identification, also known as Dynamic Signature Verification (DSV)
 - ◆ The specific features of the signature
 - ◆ Specific features of the process of signing one's signature
 - ◆ Speed, pen pressure, directions, stroke length
 - ◆ The points in time when the pen is lifted from the paper
 - Keystroke Pattern
 - ◆ Requires 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
 - ◆ "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
 - ◆ Can measure one's keyboard input up to 1000 times per second
 - The Zephyr
 - ◆ User Criteria
 - ◆ System Criteria
 - ◆ Order of effectiveness
 - ◆ Order of acceptance
- **The program that offers security over telnet is SSH**