Computer Systems Security

Lesson 03 - Authentication mechanisms

Authentication Mechanisms

- Token Based authentication
- Certificate based authentication
- Biometrics
- Authentication in DS
  - Single sign on
  - Trusted intermediaries

Token Based Authentication

- Object user possesses to authenticate, e.g.
  - memory card (magnetic stripe)
  - smartcard

Token Based Authentication- Memory card

- Store but do not process data
- Magnetic stripe card, e.g. bank card
- Electronic memory card
- Used alone for physical access (e.g., hotel rooms)
- Some with password/PIN (e.g., ATMs)
- Drawbacks of memory cards include:
  - Need special reader
  - Loss of token issues
  - User dissatisfaction (OK for ATM, not OK for computer access)

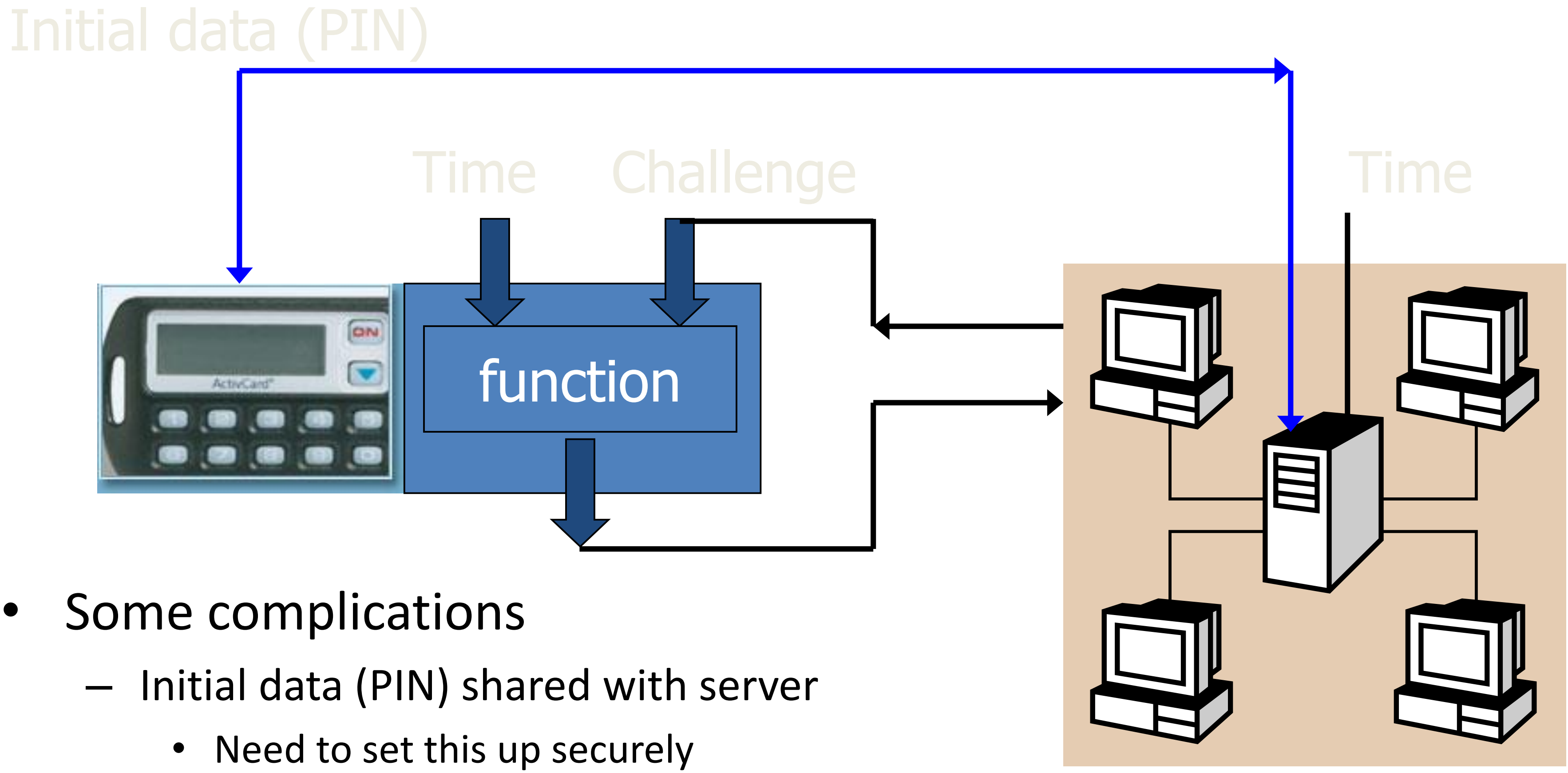
Token Based Authentication - Smartcard

- Credit-card like
- Has own processor, memory, I/O ports
  - ROM, EEPROM, RAM memory
- Executes protocol to authenticate with reader/computer
  - Static: similar to memory cards
  - Dynamic: passwords created every minute; entered manually by user or electronically
  - Challenge-response: computer creates a random number; smart card provides its hash (similar to PK)
- Also have USB dongles

Token-based Authentication - Smart Card

- With embedded CPU and memory
  - Carries conversation with a small card reader
- Various forms
  - PIN protected memory card
    - Enter PIN to get the password
  - Cryptographic challenge/response cards
    - Computer create a random challenge
    - Enter PIN to encrypt/decrypt the challenge

Smart Card Example



- Some complications
  - Initial data (PIN) shared with server
    - Need to set this up securely
    - Shared database for many sites
  - Clock skew

Certificate-Based Authentication

- A Certificate:
  - A collection of information that binds an *identity* of a principal (user, computer, service or device) to the public key of a public/private key pair.
  - Specifies:
    - Information about the identity
    - Purpose for which the certificate may be used
    - A serial number
    - Location where more information about the authority that issued the certificate may be found
  - Digitally signed by a Certificate Authority (CA)

Certificate-Based Authentication

- Public Key Infrastructure (PKI)
  - Infrastructure used to support certificate based authentication in an organization.
  - More on PKI later on.
- Public and private Keys
  - Each certificate’s public key has its associated private key.
  - Public key: Shared
  - Private key: kept secret and stored locally by the principal

Certificate-Based Authentication

- Public/private key algorithms use two keys:
  - One key used to encrypt the other to decrypt
  - Compare with symmetric key algorithms?
  - Usually private key is used to encrypt or digitally sign a request or challenge
  - Related public key is used to decrypt the request or challenge
  - If the result matches what is expected then proof of identity is obtained

- Clients (Many)
  - Access to public key of server
- Server (one)
  - Access to private key

Certificate-Based Authentication

- Authentication steps:
  - 1. Client issues an authentication request
  - 2. A challenge is issued by the server
  - 3. The client workstation uses its private key to encrypt the challenge
  - 4. The response is returned to the server
  - 5. The server has a copy of the certificate hence it can use the pubic key to decrypt the response.
  - 6. The result is compared to the challenge
  - 7. If there is a match, the client is authenticated

Certificate-Based Authentication

- NOTE:
  - Original set of keys is generated by the client
  - Only the public key is sent to the CA
  - CA generates the certificate and signs it using its own private key then returns a copy to the client and retains a copy in its database.
- Examples:
  - SSL/TLS
  - Smart cards

SSL/TLS

- Secure Sockets Layer (SSL)
  - Developed by Netscape for securing network connections
  - Provides authentication, encryption and data integrity using PKI.
  - Uses a public key/private key pair that must be generated before the process begins
  - Communicating elements acquire verification certificates from a Certificate Authority (CA)

SSL/TLS

- Secure Sockets Layer (SSL)
  - Developed by Netscape
  - Authentication of secure web servers and clients
  - Share encryption keys between servers and clients
  - Used mostly in e-commerce (https ???)
- Transport Layer Security (TLS)
  - Defined in RFC 2246
  - Internet Standard version of proprietary SSL
  - SSL and TLS are not compatible

SSL/TLS

- Implementation:
  - Organization obtains a server SSL from CA e.g. VeriSign.
  - The certificate is installed on the web server
  - Certificates can be privately generated but using CAs is recommended.

SSL/TLS

- Design:
  - Runs on top of layer 4
  - Designed to run in user-level processes
  - Running on layer 4 allows SSL deployment in user-level processes rather than requiring OS changes.
  - Runs on top of TCP and not UDP
  - Partitions the TCP octet streams into records with headers and cryptographic protection to provide a reliable, encrypted and integrity protected stream of octets.

SSL/TLS

- Design contd..
  - Four types of records:
    - User data
    - Handshake messages
    - Alerts (error messages or notification of connection closure)
    - Change cipher spec

SSL/TLS

- Authentication process:
  - 1. A user enters server URL in the browser
  - 2. The web page request is sent to the server
  - 3. The server receives the request and sends its server certificate to the client
  - 4. The client’s browser checks its certificate store for a certificate from the CA that issued the server certificate
  - 5. If the certificate is found:
    - The browser validates the certificate by checking the signature on the servers’s certificate using the public key provided on the CA’s certificate

SSL/TLS

- Authentication process: (contd…)
  - 6. If the test in 5 above succeeds, browser accepts the server certificate as valid.
  - 7. A symmetric encryption key is generated and encrypted by the client, using the server’s public key.
  - 8. The encrypted key is returned to the server.
  - 9. The server decrypts the key with the server’s own private key. The two computers now share an encryption key that can be used to secure communications between the two of them.

SSL/TLS

- Negotiating Cipher suites:
  - A named combination of authentication, encryption and message authentication code (MAC) algorithms used to negotiate security settings of a network connection.
  - A complete package of whatever will be defined to completely specify all the crypto SSL/TLS will need.

SSL/TLS

- Negotiation Cipher suites:
  - These include:
    - encryption algorithm,
    - key length,
    - integrity checksum algorithms
  - Cipher suites are pre-defined and each is assigned a numeric value
  - In SSLv2 the value is 3 octets long but in SSLv3 and TLS its 2 octets.

SSL/TLS

- Negotiating Cipher suites:
  - There are about 30 Cipher suites and 256 reserved values for private use.
  - In SSLv2, the server returns the subset of the client’s suggested cipher suites that it is willing to support but lets the client make the final choice.
  - In SSLv3, the server takes charge and makes decision from the list sent.

SSL/TLS

- Negotiating Cipher suites
  - Key exchange/agreement algorithms
    - RSA,
    - Diffie-Hellman,
    - ECDH – Elliptic Curve Diffie-Hellman,
    - SRP – Secure Remote Password Protocol,
    - PSK – Preshared Key
  - Authentication
    - RSA
    - DSA – Digital Signature Algorithm,
    - ECDSA – Elliptic Curve DSA

SSL/TLS

- Negotiating Cipher suites
  - Bulk Ciphers
    - RC4, Tripe DES, AES, IDEA or Camellila
  - Message Authentication
    - For SSL: SHA, MD5, MD4 or even MD2
    - For TLS: MD5 or one of the SHA hash functions

SSL/TLS

- Example:
- In the SSL/TLS RFC, the cipher suites are referred to by names e.g.:
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
  - SSL means SSLv3 (SSLv2 uses SSL2)
  - RSA: RSA algorithm
  - EXPORT: means it is exportable
  - WITH: {Used to imply the names weren’t long enough}
  - DES40: DES with 40 bit keys
  - CBC: CBC-mode encryption
  - SHA: HMAC-SHA is used for the MAC

SSL/TLS

- Attacks fixed in SSLv3
  - Downgrade attack:
    - In SSLv2, there is no integrity protection for the initial handshake.
    - An active attacker can remove the cipher suites with strong encryption from the list of requested cipher suites.
    - Can cause the client and sever to agree on a weaker suite.

SSL/TLS

– Downgrade attack (contd…)
  - SSLv3 fixed this by adding a “finished” message to the end of the initial handshake.
  - Each side sends a digest of the messages in the handshake

SSL/TLS

- Truncation attack:
    - SSLv2 depended on TCP closing a connection to indicate that there is no more data to send.
    - TCP connection is not cryptographically encrypted.
    - An attacker could easily close the connection by sending a TCP close message.
    - SSLv3 added the “finished” message to indicate that there is no more data to send.

MD5 for Authentication

- Beyond encryption, MD5 can be used for authentication
- Each user has a file containing a set of keys:
  - Input into the MD5 hash
- Information being supplied to the authenticating server (e.g. passwords) has its MD5 checksum calculated using these keys then transferred to the authenticating server along with the MD5 hash result.

Remote Authentication

- 1. Secure RPC Authentication
- 2. Dial-in Authentication
- 3. Remote Dial-in User Services (RADIUS) Authentication

Secure RPC Authentication

- The client may not want to identify itself to the server
- The server may not require any identification from the client
- Example:
  - Network File System (NFS)
- They use RPC authentication

Secure RPC Authentication

- Is open ended hence can use different forms and multiple types of authentication including:
  - NULL Authentication
  - UNIX Authentication
  - DES Authentication
  - Diffie-Hellman Encryption

Dial-in Authentication

- Passwords are required in dial-in connections
- Authentication process must precede any successful login
- Point-to-Point (PPP) is the most common protocol in all dial-in connections
- Uses PPP authentication mechanisms

Dial-in Authentication

- PPP Authentication:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Protocol (CHAP)
  - Extensible Authentication Protocol (EAP)

Dial-in Authentication

- PAP Authentication:
  - Allows the peer to establish identity of the authenticator in a two-way handshake
  - Send to the authenticator an initial packet containing the peer name and password
  - Authenticator responds with authenticate-ACK if everything checks out and authentication process is complete.

Dial-in Authentication

- CHAP authentication protocol
  - Employed periodically to identify any user who uses a three way handshake
  - Use a handshake to initialize a link (Like PAP)
  - After establishing a link, the peer seeking authentication and the authenticator share a secret text that is actually never shared across the network
  - Uses challenge-Response

Dial-in Authentication

- CHAP authentication protocol (contd…)
  - Authenticator first sends a challenge:
    - Identifier, a random number, hostname of the peer (user)
  - The peer responds to the challenge by using a one way hash to calculate a value; the secret is the input to the hash

Dial-in Authentication

- CHAP authentication protocol (contd…)
  - The peer then sends to the authenticator an encrypted identification, the output of the hash, the random number, the peer name or user name
  - The authenticator verifies these by performing the same encryption and authenticates the peer if everything checks out

Dial-in Authentication

- Student ToDo:
  - Read on Extensible Authentication Protocol (EAP)

RADIUS

- Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- To be discussed later

Biometrics

- Identification by physical characteristics
- A two factor authentication:
  - Something you have is something that is part of you.

Biometrics

- Includes the use of:
  - Facial recognition and identification
  - Retinal scans
  - Iris scans
  - Fingerprints
  - Voice recognition
  - Lip movement and
  - Keystroke analysis

Biometrics

- NOTE:
  - Biometrics currently in use have been chosen because they represent characteristics that are unique to individuals.
  - Relative accuracy of each system is judged by the number of false negatives and false positives that it generates.

Biometrics

- Vulnerabilities:
  - Gummy finger attack (May 2002)
    - http://cryptome.org/gummy.htm
  - **Theorized**: Malicious attackers cutting body parts from the real person and using them to authenticate (terrorism).

Biometrics

- Advantages
  - Cannot be disclosed, lost, forgotten
- Disadvantages
  - Cost, installation, maintenance
  - Reliability of comparison algorithms
    - False positive: Allow access to unauthorized person
    - False negative: Disallow access to authorized person
  - Privacy?
  - If forged, how do you revoke?

Biometrics

- Common uses
  - Specialized situations, physical security
  - Combine
    - Multiple biometrics
    - Biometric and PIN
    - Biometric and token