FORBSBC

Authentication

- Chapter 2

Learning Objectives

- Create strong passwords and store them securely
- Understand the Kerberos authentication process
- Understand how CHAP works
- Understand what mutual authentication is and why it is necessary
- Understand how digital certificates are created and why they are used

continued…

Learning Objectives

- Understand what tokens are and how they function
- Understand biometric authentication processes and their strengths and weaknesses
- Understand the benefits of multifactor authentication

Security of System Resources

- Three-step process (AAA)
  - Authentication
    - Positive identification of person/system seeking access to secured information/services
  - Authorization
    - Predetermined level of access to resources
  - Accounting
    - Logging use of each asset

Authentication Techniques

- Usernames and passwords
- Kerberos
- Challenge Handshake Authentication Protocol (CHAP)
- Mutual authentication
- Digital certificates
- Tokens
- Biometrics
- Multifactor authentication

Usernames and Passwords

- Username
  - Unique alphanumeric identifier used to identify an individual when logging onto a computer/network
- Password
  - Secret combination of keystrokes that, when combined with a username, authenticates a user to a computer/network

Basic Rules for Password Protection

1. Memorize passwords; do not write them down
2. Use different passwords for different functions
3. Use at least 6 characters
4. Use mixture of uppercase and lowercase letters, numbers, and other characters
5. Change periodically

Strong Password Creation Techniques

- Easy to remember; difficult to recognize
- Examples:
  - First letters of each word of a simple phrase; add a number and punctuation
    - Asb4M?
  - Combine two dissimilar words and place a number between them
    - SleighH9ShoE
  - Substitute numbers for letters (not obviously)

Techniques to Use Multiple Passwords

- Group Web sites or applications by appropriate level of security
  - Use a different password for each group
  - Cycle more complex passwords down the groups, from most sensitive to least

Storing Passwords

- Written
  - Keep in a place you are not likely to lose it
  - Use small type
  - Develop a personal code to apply to the list
- Electronic
  - Use a specifically designed application (encrypts data)

Kerberos

- Provides secure and convenient way to access data and services through:
  - Session keys
  - Tickets
  - Authenticators
  - Authentication servers
  - Ticket-granting tickets
  - Ticket-granting servers
  - Cross-realm authentication

Kerberos in a Simple Environment

- Session key
  - Secret key used during logon session between client and a service
- Ticket
  - Set of electronic information used to authenticate identity of a principal to a service
- Authenticator
  - Device (eg, PPP network server) that requires authentication from a peer and specifies authentication protocol used in the configure request during link establishment phase

continued…

Kerberos in a Simple Environment

- Checksum
  - Small, fixed-length numerical value
  - Computed as a function of an arbitrary number of bits in a message
  - Used to verify authenticity of sender

Kerberos in a Simple Environment

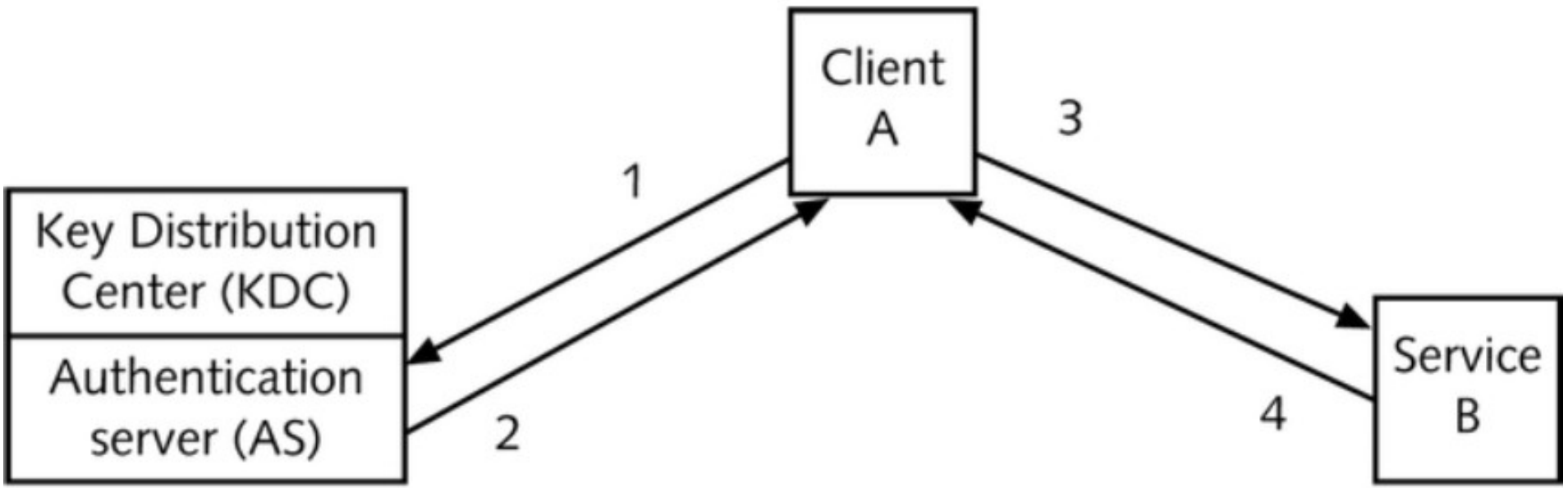

Figure 2-1 Kerberos authentication

Kerberos in a More Complex Environment

- Ticket-granting ticket (TGT)
  - Data structure that acts as an authenticating proxy to principal's master key for set period of time
- Ticket-granting server (TGS)
  - Server that grants ticket-granting tickets to a principal

Kerberos in a More Complex Environment

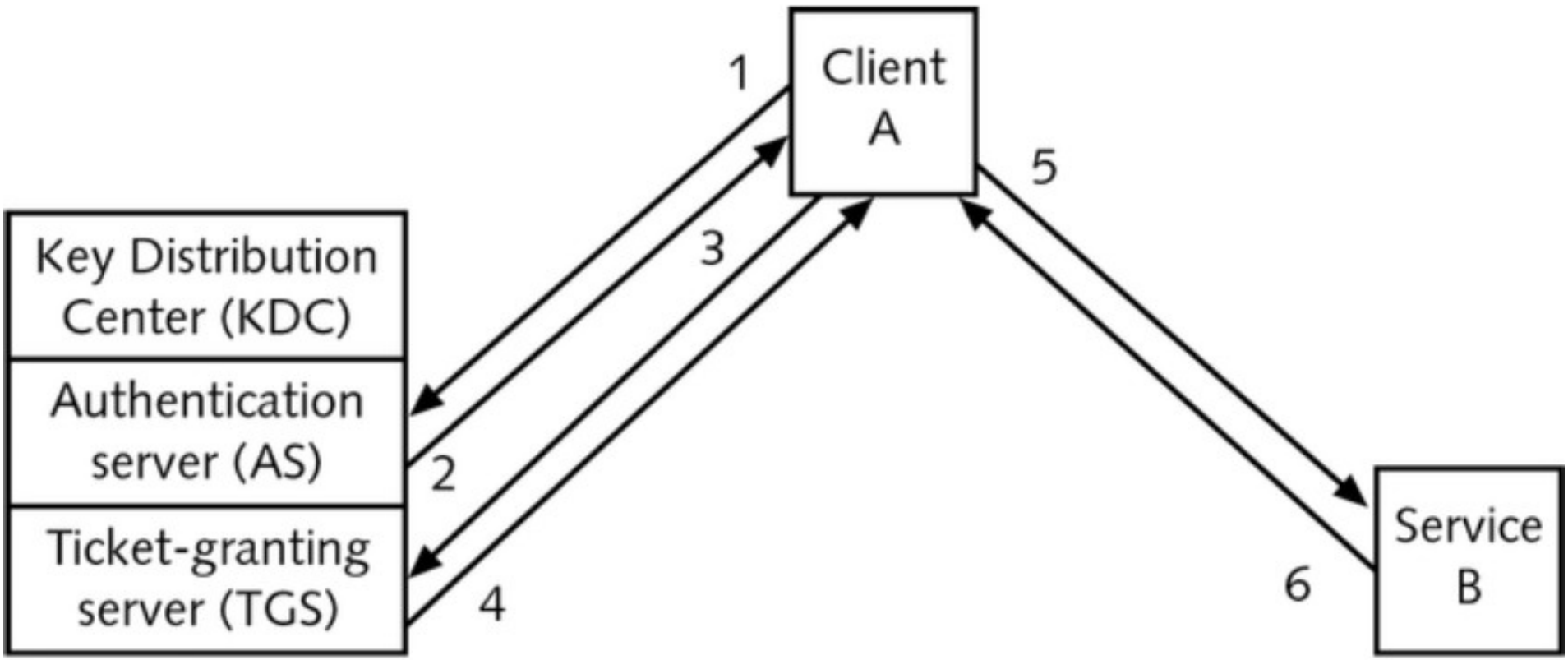

Figure 2-2 Ticket-granting server

Kerberos in Very Large Network Systems

- Cross-realm authentication
  - Allows principal to authenticate itself to gain access to services in a distant part of a Kerberos system

Cross-Realm Authentication

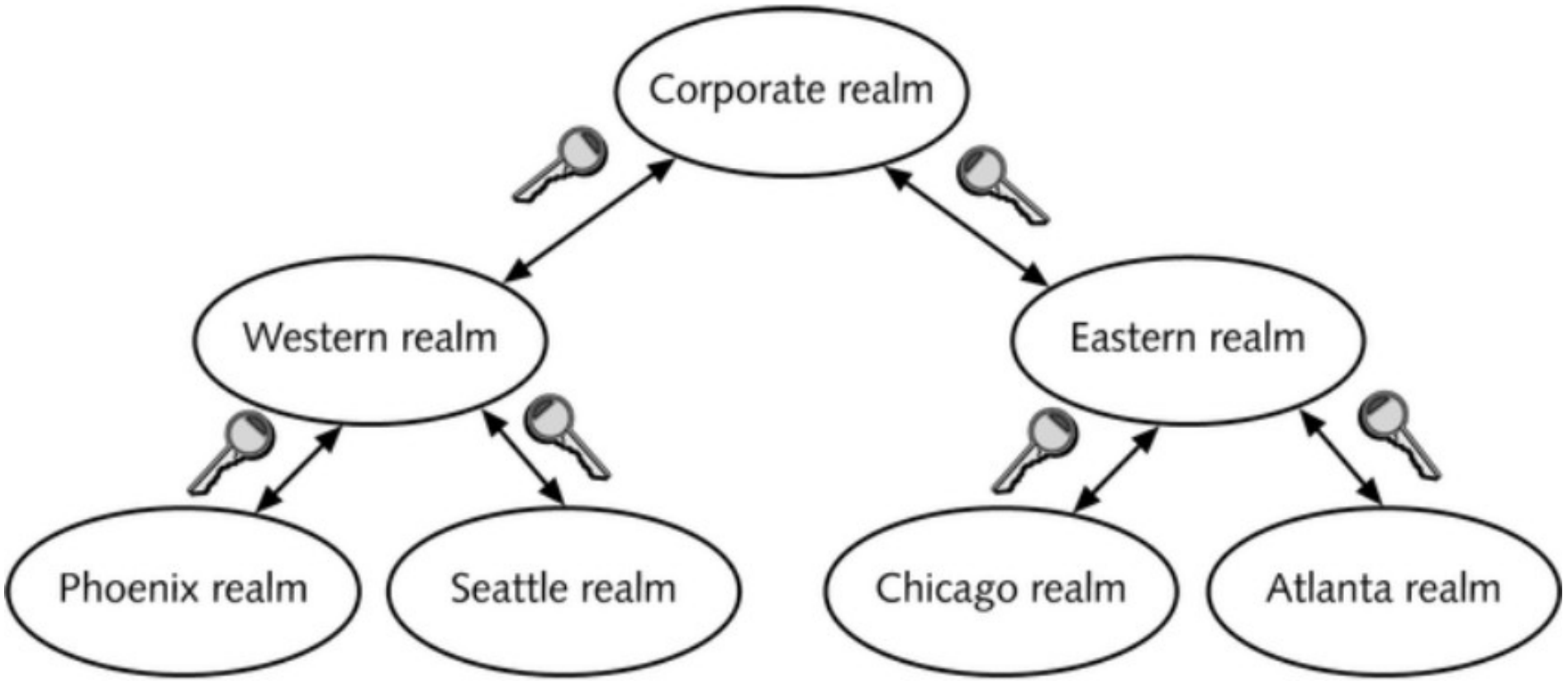

Figure 2-3 Cross-realm authentication

Security Weaknesses of Kerberos

- Does not solve password-guessing attacks
- Must keep password secret
- Does not prevent denial-of-service attacks
- Internal clocks of authenticating devices must be loosely synchronized
- Authenticating device identifiers must not be recycled on a short-term basis

Challenge Handshake Authentication Protocol (CHAP)

- PPP mechanism used by an authenticator to authenticate a peer
- Uses an encrypted challenge-and-response sequence

CHAP Challenge-and-Response Sequence

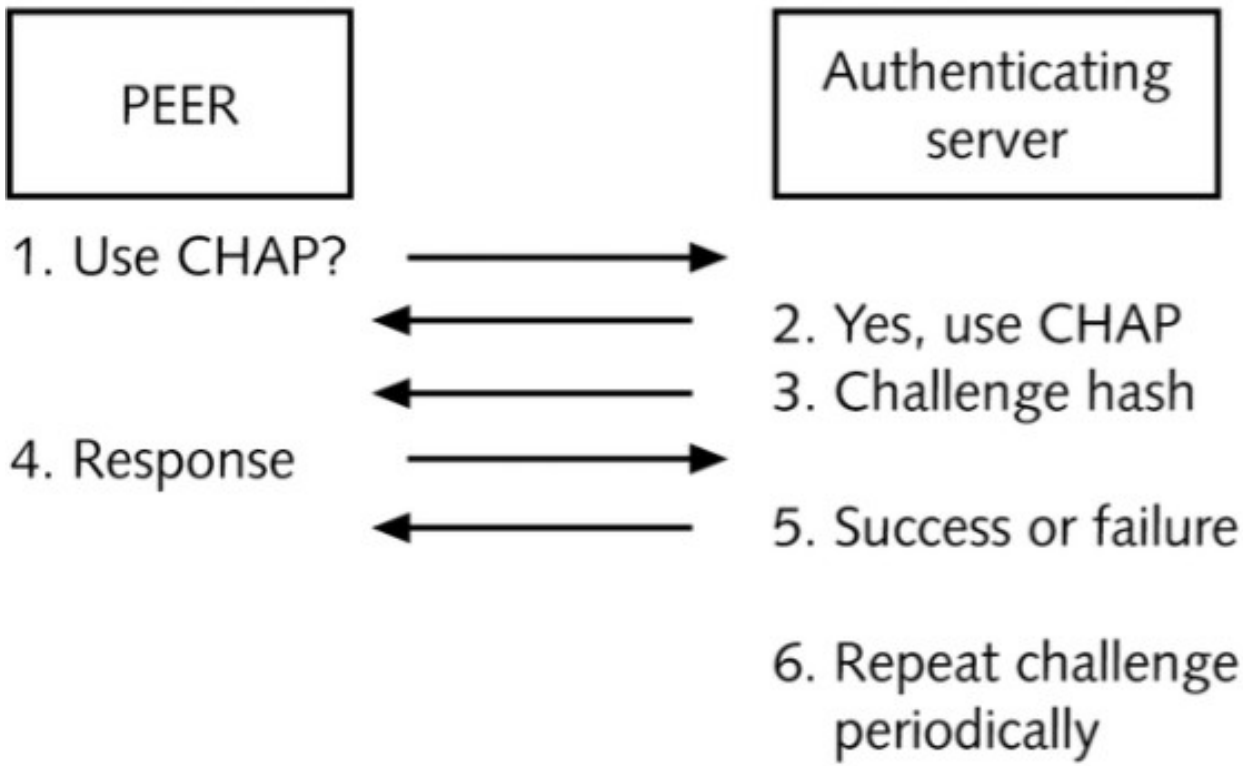

Figure 2-4 CHAP challenge-and-response process

CHAP Security Benefits

- Multiple authentication sequences throughout Network layer protocol session
  - Limit time of exposure to any single attack
- Variable challenge values and changing identifiers
  - Provide protection against playback attacks

CHAP Security Issues

- Passwords should not be the same in both directions
- Not all implementations of CHAP terminate the link when authentication process fails, but instead limit traffic to a subset of Network layer protocols
  - Possible for users to update passwords

Mutual Authentication

- Process by which each party in an electronic communication verifies the identity of the other party

Digital Certificates

- Electronic means of verifying identity of an individual/organization
- Digital signature
  - Piece of data that claims that a specific, named individual wrote or agreed to the contents of an electronic document to which the signature is attached

Electronic Encryption and Decryption Concepts

- Encryption
  - Converts plain text message into secret message
- Decryption
  - Converts secret message into plain text message
- Symmetric cipher
  - Uses only one key
- Asymmetric cipher
  - Uses a key pair (private key and public key)

continued…

Electronic Encryption and Decryption Concepts

- Certificate authority (CA)
  - Trusted, third-party entity that verifies the actual identity of an organization/individual before providing a digital certificate
- Nonrepudiation
  - Practice of using a trusted, third-party entity to verify the authenticity of a party who sends a message

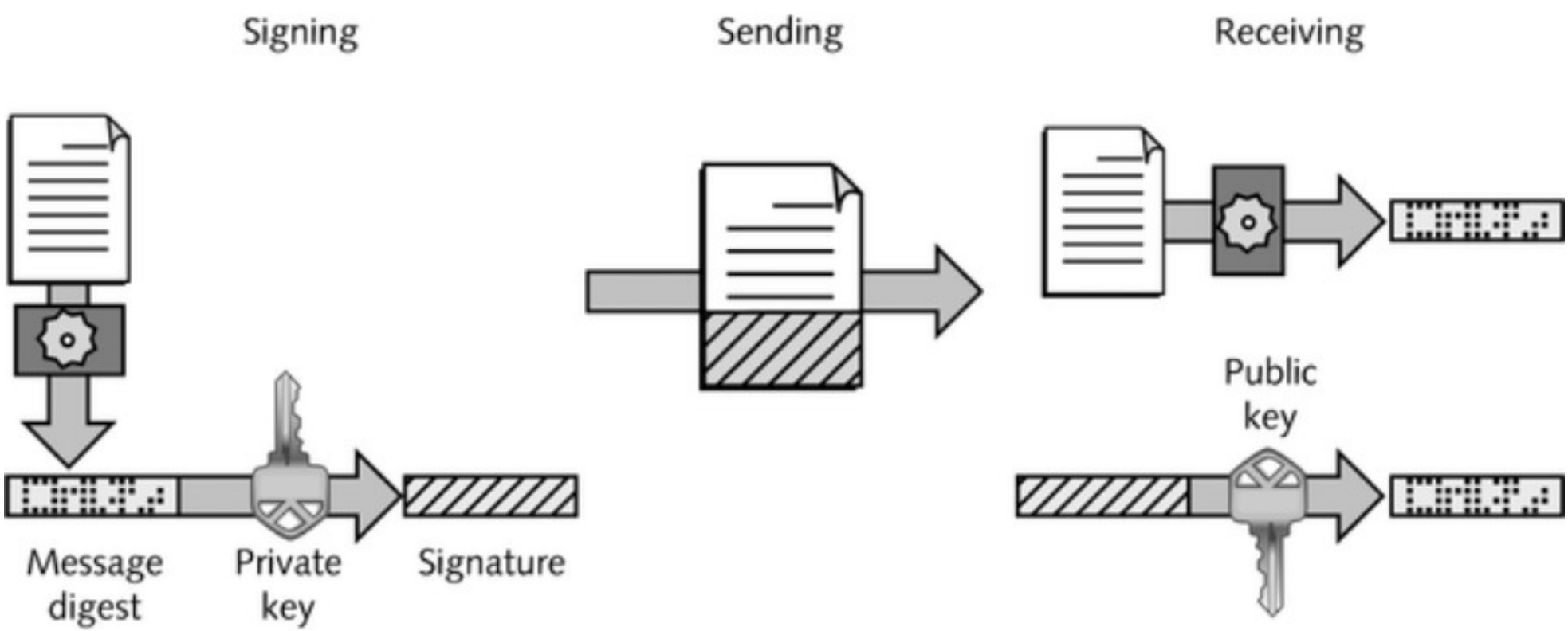

Figure 2-5 Digital signatures

How Much Trust Should One Place in a CA?

- Reputable CAs have several levels of authentication that they issue based on the amount of data collected from applicants
- Example: VeriSign

Security Tokens

- Authentication devices assigned to specific user
- Small, credit card-sized physical devices
- Incorporate two-factor authentication methods
- Utilize base keys that are much stronger than short, simple passwords a person can remember

Types of Security Tokens

- Passive
  - Act as a storage device for the base key
  - Do not emit, or otherwise share, base tokens
- Active
  - Actively create another form of a base key or encrypted form of a base key that is not subject to attack by sniffing and replay
  - Can provide variable outputs in various circumstances

One-Time Passwords

- Used only once for limited period of time; then is no longer valid
- Uses shared keys and challenge-and-response systems, which do not require that the secret be transmitted or revealed
- Strategies for generating one-time passwords
  - Counter-based tokens
  - Clock-based tokens

Biometrics

- Biometric authentication
  - Uses measurements of physical or behavioral characteristics of an individual
  - Generally considered most accurate of all authentication methods
  - Traditionally used in highly secure areas
  - Expensive

How Biometric Authentication Works

1. Biometric is scanned after identity is verified
2. Biometric information is analyzed and put into an electronic template
3. Template is stored in a repository
4. To gain access, biometric is scanned again
5. Computer analyzes biometric data and compares it to data in template
6. If data from scan matches data in template, person is allowed access
7. Keep a record, following AAA model

FORBSBC

False Positives and False Negatives

- False positive
  - Occurrence of an unauthorized person being authenticated by a biometric authentication process
- False negative
  - Occurrence of an authorized person not being authenticated by a biometric authentication process when they are who they claim to be

Different Kinds of Biometrics

- Physical characteristics
  - Fingerprints
  - Hand geometry
  - Retinal scanning
  - Iris scanning
  - Facial scanning
- Behavioral characteristics
  - Handwritten signatures
  - Voice

Fingerprint Biometrics

Figure 2-6 Fingerprint scanner: Digital Persona U.areU. Pro

Hand Geometry Authentication

Figure 2-7 Hand geometry scanner: HandkeyII by Recognition Systems Inc.

Retinal Scanning

Figure 2-8 Retinal scanner by Eyedentify Inc.

Iris Scanning

Figure 2-9 Iris scanner by Panasonic Authenticam

Signature Verification

Figure 2-10 Signature scanner by Interlink ePad VP9105

General Trends in Biometrics

- Authenticating large numbers of people over a short period of time (eg, smart cards)
- Gaining remote access to controlled areas

Multifactor Authentication

- Identity of individual is verified using at least two of the three factors of authentication
  - Something you know (eg, password)
  - Something you have (eg, smart card)
  - Something about you (eg, biometrics)

Chapter Summary

- Authentication techniques
  - Usernames and passwords
  - Kerberos
  - CHAP
  - Mutual authentication
  - Digital certificates
  - Tokens
  - Biometrics
  - Multifactor authentication