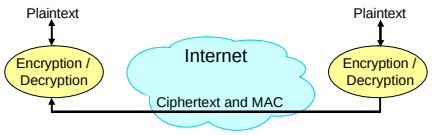
Secure Channels

CS 161/194-1
Anthony D. Joseph
September 26, 2005

Main Points

- Applying last week's lectures in practice
- Creating Secure Channels
- Example Applications
  - PGP: Pretty Good Privacy
  - TLS: Transport Layer Security
  - VPN: Virtual Private Network

What is a Secure Channel?



- A stream with these security requirements:
  - Authentication
    - Ensures sender and receiver are who they claim to be
  - Confidentiality
    - Ensures that data is read only by authorized users
  - Data integrity
    - Ensures that data is not changed from source to destination
  - Non-repudiation (not discussed today)
    - Ensures that sender can't deny message and rcvr can't deny msg

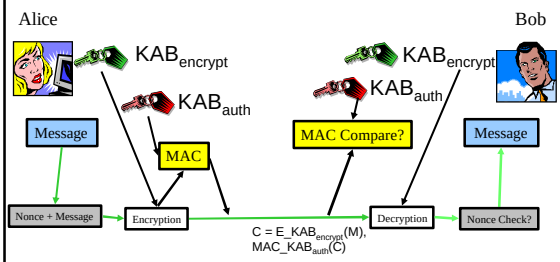
Creating Secure Channels

- Authentication and Data Integrity
  - Use Public Key Infrastructure or third-party server to authenticate each end to the other
  - Add Message Authentication Code for integrity
- Confidentiality
  - Exchange session key for encrypt/decrypt ops
    - Bulk data transfer
- Key Distribution and Segmentation

Symmetric Key-based Secure Channel

- Sender (A) and receiver (B) share secret keys
  - One key for A ➔ B confidentiality
  - One for A ➔ B authentication/integrity
  - Each message sent from A ➔ B contains:
    - Ciphertext = $E\_KAB_{encrypt}$(nonce + msg)
    - Authenticity/Integrity check = MAC_KAB_{auth}(Ciphertext)
- Different keys for each direction = 4 keys
  - $KAB_{encrypt}$, KAB_{auth}, $KBA_{encrypt}$, KBA_{auth}

Symmetric Key-based Secure Channel



How to exchange secret keys?

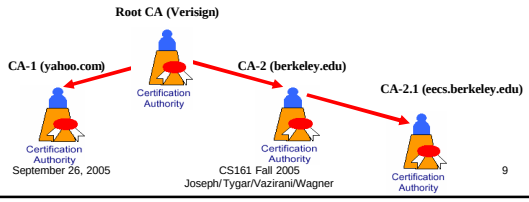
Secure Channel: Choice #1

- Use public key certificates
- Requires Public Key Infrastructure (PKI)
  - Manages wide-scale public key distribution
  - Provides a trust distribution mechanism
- PKI Properties
  - Authentication ➔ via Public Key Certificates
  - Confidentiality ➔ via Encryption
  - Integrity ➔ via Digital Signatures

PKI Components

Certification Authority

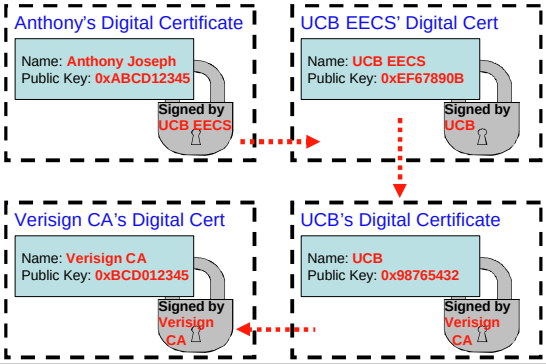
- People, processes responsible for creation, delivery and management of digital certificates
- Organized in a hierarchy
  - Enables delegation of authority (sign on behalf of X)



Digital Certificate

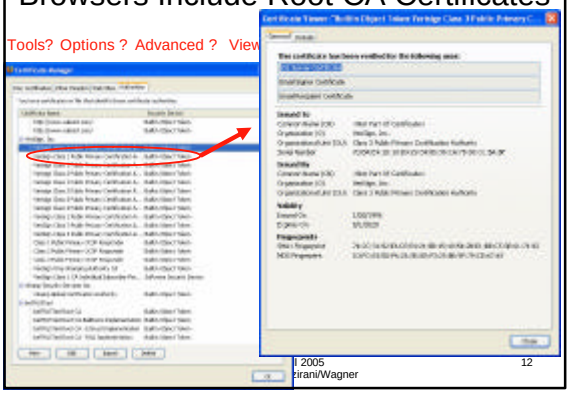
- Signed data structure that binds an entity with its corresponding public key
  - Signed by a recognized and trusted authority = Certification Authority (CA)
  - Provide assurance that a particular public key belongs to a specific entity

Digital Certificate Chain



Browsers Include Root CA Certificates

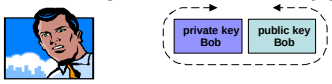
Tools? Options ? Advanced ? View



PKI Example: Creating Certs

1. Alice generates her own key pair

2. Bob generates his own key pair

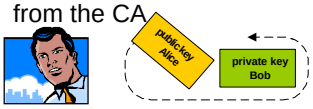


3. Both send their public key to a CA and receive a public key certificate signed by CA

PKI Example: Getting Keys

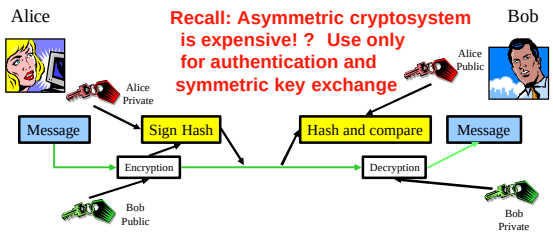
4. Alice gets Bob's public key from the CA

5. Bob gets Alice's public key from the CA

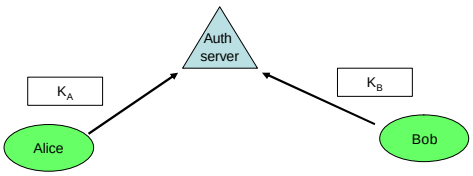


PKI Example: Secure Channel

5. Alice uses private key to encrypt and sign: authentication, confidentiality, integrity

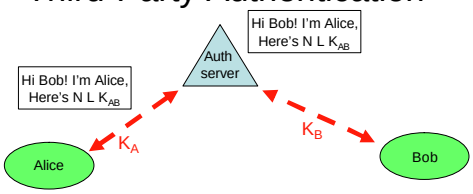


Secure Channel: Choice #2



- Use a trusted third-party authentication server and symmetric key cryptography for authentication, integrity, and confidentiality
- Users share secret key with auth server

Third-Party Authentication



- Alice constructs a secure channel to auth server
- Alice sends secret key message for Bob
  - Also includes nonce and session key lifetime - Why?
- Server constructs secure channel to Bob
- Server forwards message

Authentication Choices

- Both require a trusted third-party server
- Both require wide-spread deployment of server infrastructure
- Still have distribution problem
  - Root certificates versus shared secrets
- Difference is use of public/private key cryptosystem versus private/shared key one
- Another alternative:
  - Pretty Good Privacy (more later on)

Three Concrete Examples

- Pretty Good Privacy (PGP)
- Transport Layer Security (TLS)
- Virtual Private Networks (VPN)

Pretty Good Privacy (PGP)

- Provides
  - Authentication, Confidentiality, Integrity (optional)
- Application examples: file transfers, e-mail
- Weaker authentication than PKI, but
  - Freely available: standalone and plug-ins for many e-mail clients
  - Not controlled by a government or standard organization

PGP Services

- Authentication
  - Digital signature; uses DSS/SHA or RSA/SHA
- Confidentiality
  - Encryption (triple DES or RSA)
- Integrity
  - Optional digital signature on entire message
- Also provides
  - Compression ➔ Zip
  - E-mail compatibility ➔ Radix-64 conversion
  - Large file support ➔ Segmentation

PGP: Public Key Management

- No rigid public key management scheme
- Problem: how to reliably get public key
  - Possible solution: physically (secure but unpractical) or by phone
- PGP solution: build a "web of trust"
  - Let's assume you know several variably trusted users
  - Each of these indvidual can sign certificates for other users
  - Each signature has an associated trust field indicating the level of trust in the certificate

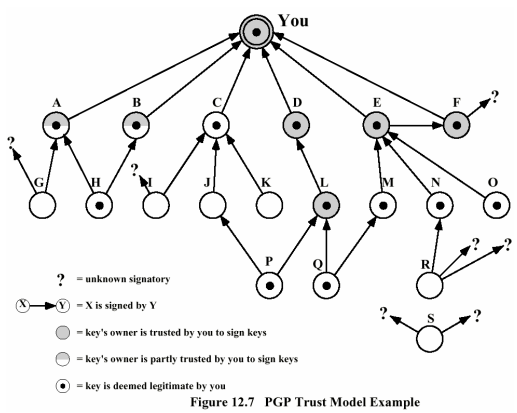
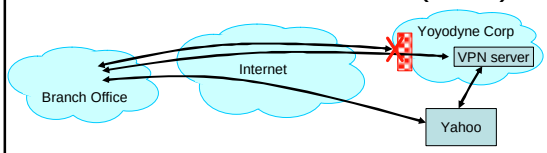


Figure 12.7 PGP Trust Model Example

Transport Layer Security (TLS)

- Follow on to Secure Socket Layer (SSLv3)
- Often used for secure HTTP web browsing
  - HTTPS (HTTP over SSL over TCP), SMTP, and NNTP [https://bearfacts.berkeley.edu/]
  - Stunnel standalone program tunnels any TCP traffic
- Steps:
  1. Negotiate algorithm choices for authentication and bulk data transfer
  2. Use public key encryption-based key exchange or certificate-based authentication
  3. Encrypt stream with symmetric cipher
     - MAC and optional compression

Virtual Private Network (VPN)



- Often need to provide secure remote access to a network protected by a firewall
  - Remote access, telecommuting, branch offices, …
- VPN tunnels all or some traffic from a machine or network to another network
  - Provides Authentication, Confidentiality, Integrity

VPN Implementations

- Typically a virtual network driver that forwards traffic over a secure channel
  - Many commercial clients for PCs
  - Open source client: OpenVPN
  - Commercial hardware available for performance or networks
- Software clients use IPSEC or TLS/SSL
- Try it for yourself!
  - http://www.net.berkeley.edu/vpn/

VPN Perimeter Security Issues

- A VPN enables access to servers
  - That's the goal!
- But, if remote machine or network is compromised, attacker gains access to the servers
  - Same as if they were inside building
    - Defeats physical and network security

VPN Perimeter Security Issues

- Slammer worm penetrates unsecured network of a D-B contractor
- Squirms through a VPN into D-B's internal network
- Disables safety monitoring system for ~5hrs
- Plant was already offline
- Analog systems still online

Ohio's Davis-Besse Nuclear Power Plant (Jan 2003)

SecurityFocus 08/19/03