Internet Security

Stephen T. Whitlock
stephen.whitlock@boeing.com
Applied Research & Technology
Boeing Shared Services Group

General Threats

- ✦Disclosure of information
- ✦Modification of information
- ✦Impersonation of identity
- ✦Repudiation of identity
- ✦Repudiation of transaction
- ✦Denial of service
- ✦Traffic analysis

Prevention or Detection

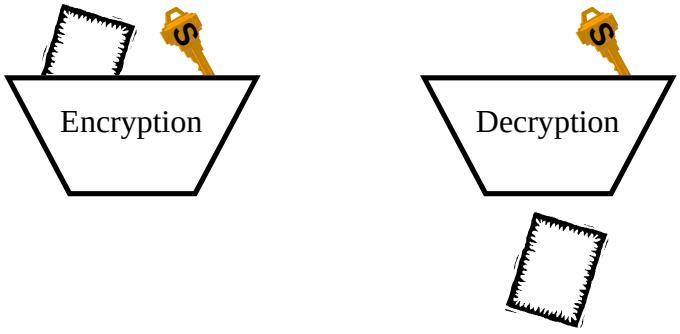
- Cryptography
  - Encryption
  - Digital Signatures
- DNS Security
- Firewalls
- Intrusion Detection

Cryptographic Terms

- ***Plaintext*** - the original information
- ***Ciphertext*** - the information after encryption
- ***Encryption*** - the process of transforming the plaintext into the ciphertext
- ***Decryption*** - the process of recovering the plaintext from the ciphertext
- ***Cryptography*** - the science of securing information by using encryption and decryption
- ***Cryptanalysis*** - of the plaintext by breaking the encryption using the ciphertext
- ***Cryptology*** - the science that includes cryptography and cryptanalysis

Secret Key Encryption

- Same key used for encryption and decryption



Secret Key Characteristics

- Requires a secure method of key distribution
  - More suitable for government agencies or a few individuals than large organizations
- Scales poorly, N users need nearly N^2 keys
  - 100,000 users would need almost 5 billion keys
- Block and stream ciphers
- Algorithms are fast
- Attacked by exhaustive search of key space
  - As computers get faster key length must go up
- Examples: DES, Blowfish, IDEA, RC4, CAST

Public Key Encryption

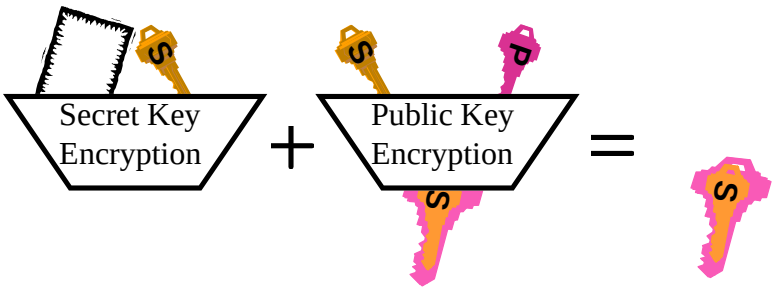
- ✦2 keys are generated as a pair
- ✦One is kept by the user (private key)
- ✦One is distributed (public key)
- ✦The private key decrypts what the public key encrypts
- ✦The public key decrypts what the private key encrypts

Public Key Characteristics

- ✦ Needs an authenticated source for public key
  - From trusted common source, (Hierarchical)
  - From your friends (Peer to peer, web of trust)
- ✦ Algorithms are much slower than secret key
- ✦ Scales well, N users need N pairs of keys
- ✦ Usually attacked by attacking the algorithm
  - Public key algorithms depend on hard mathematical problems
  - They are weakened by increases in computer speeds and mathematical advances
- ✦ Examples: RSA, Diffie-Hellman, El Gamal

Secret Key and Public Key

- The secret key is used to encrypt the data
- The public / private key pair is used to encrypt the secret key



Cryptographic Hash Functions

- One way algorithm that processes a file and produces a unique number that depends on the contents of the file
  - Usually 128 to 512 bits
  - Similar to a checksum; but cryptographically difficult to reverse engineer
- The output can be used as a substitute for the actual file
- Used for digital signatures and other authentication mechanisms
- Examples: MD5, SHA-1

Encryption Example (Sender)

- Sender
  - Generates a hash of the message
  - Encrypts the hash with the sender's private key
  - Generates a random secret key
  - Encrypts a message with the secret key
  - Encrypts the secret key with the receiver's public key
  - Sends the encrypted hash, encrypted secret key and the encrypted message to the receiver

Encryption Example (Receipt)

- Receiver
  - Decrypts the secret key with the receiver's private key
  - Decrypts the message with the secret key
  - Decrypts the hash with the sender's public key
    - ***This authenticates the sender***
  - Generates a new hash of the message and compares it to the decrypted hash
    - ***An agreement between the two hashes validates the message's integrity***

Digital Signature Creation

- Publisher
  - Generates a hash of a document
  - Encrypts the hash with the publisher's private key
  - Publishes the encrypted hash with the document

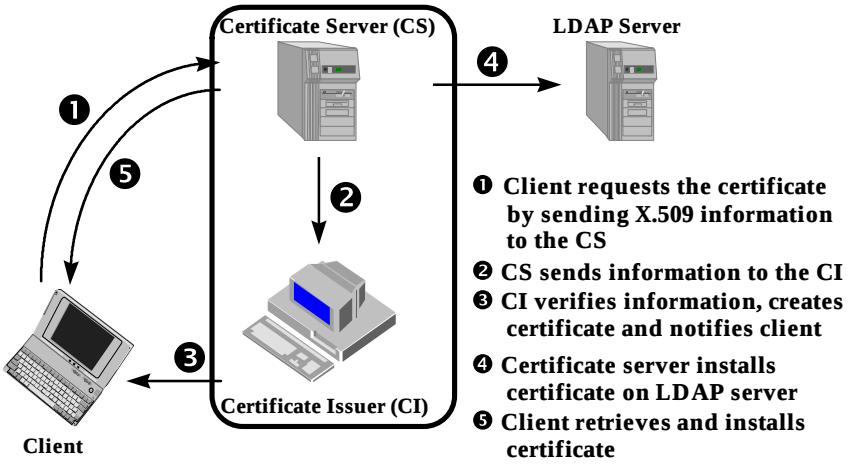
Digital Signature Verification

- Receiver
  - Obtains the document and encrypted hash from the publisher
  - Decrypts the hash with the publisher's public key
    - ***This authenticates the publisher***
  - Generates a new hash of the document and compares it to the decrypted hash
    - ***An agreement between the two hashes validates the document's integrity***

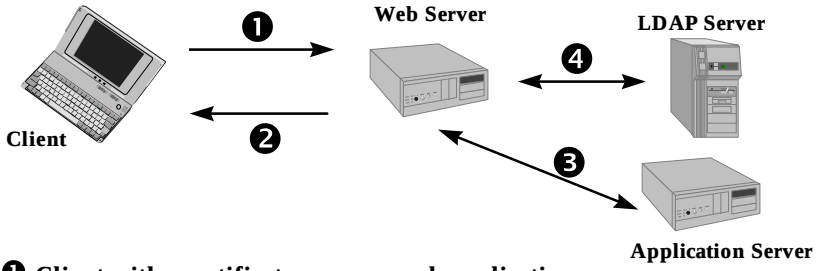
Public Key Infrastructure (PKI)

- Used to distribute and certify a public key
  - X.509 Certificates bind a name to a public key using a digital signature from a trusted Certification Authority (CA)
  - CAs also publish Certificate Revocation Lists (CRL)s
  - SPKI and PGP certificates are usually self signed
- Certificates may be distributed by a public server using LDAP (Lightweight Directory Access Protocol)
- Certificates may be used as a key to look up additional information in the LDAP directory

Getting an X.509 Certificate

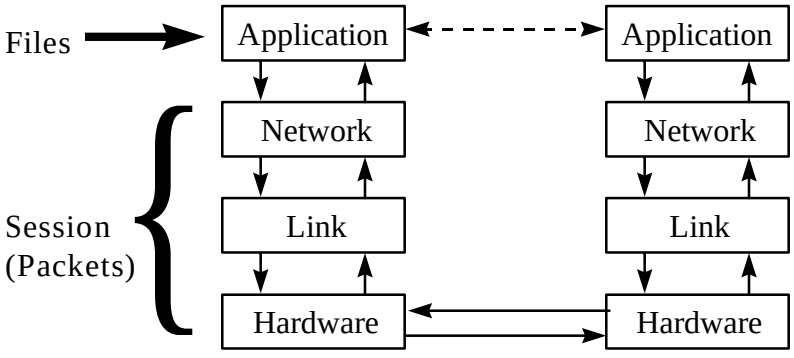


Authentication with Certificates



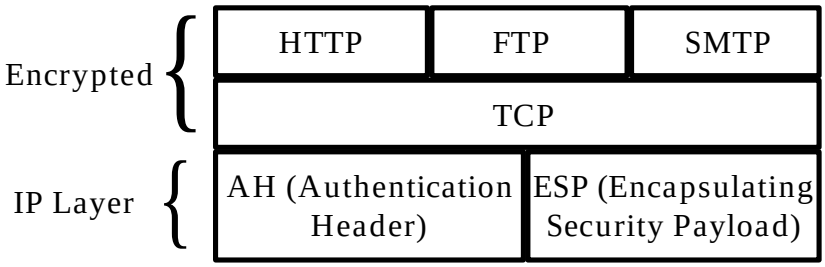
❶ **Client with a certificate accesses web application**
❷ **Web server reads certificate and allows access based on client's identity**
❸ **Web application may be a front end for another application, database or legacy system**
❹ **Application may obtain additional information from an LDAP server**

Encryption Placement



IPSec (IP Security)

- Operates in the IP layer, below the TCP layer
- Described in RFCs 1825 - 1829

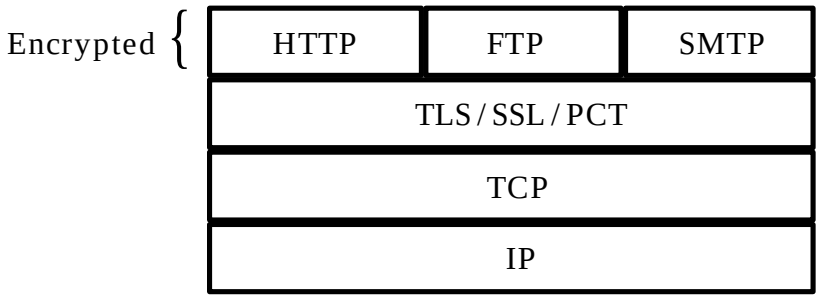


IPSec Characteristics

- Preliminary IETF standard
- Vendor Neutral
- Implemented in the operating system's protocol stack
- Needs a key management system
  - ISAKMP, SKIP
- Add-on to IPv4, part of IPv6
- Firewalls can't follow the conversation
- Successful interoperability tests between about 30 vendors

TLS, SSL, and PCT

- Operates between the TCP and the Application layers



TLS, SSL, and PCT

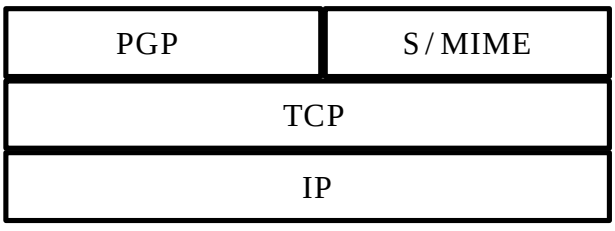
- SSL (Secure Sockets Layer)
  - Written by Netscape
  - Dominant technology (SSL 3.0)
- PCT (Private Communications Technology)
  - Developed by Microsoft from SSL 2.0
  - No longer relevant, some legacy usage
- TLS (Transport Layer Protocol)
  - Built on SSL 3.0 and PCT 2.0
  - Backward compatible with SSL 3.0
  - TLS 1.0 is currently a preliminary IETF standard
  - Will be supported by IE 5.X and Communicator 5.X

SSL / TLS Characteristics

- Server or client authentication
- Message integrity
- Can encrypt any URL transaction
  - Currently only used by HTTP
  - At least 19 more protocols anticipate using TLS
- Supports non-repudiation
- Simple key management
  - public keys managed with certificates
  - secret keys changed every 30 seconds
- Also transparent to firewalls

PGP and S-MIME

- Operate at the Application layer
- E-mail and file encryption



PGP / S-MIME Characteristics

- ✦Protection at the document level
- ✦Provide
  - Confidentiality of message
  - Authentication of sender
  - Integrity of message
  - Non-repudiation of origin
- ✦OpenPGP and S-MIME are preliminary IETF Standards

DNSSec (DNS Security)

- ✦The Domain Name System (DNS) translates between domain names like ***www.w3.org*** and IP addresses like ***18.23.0.22***
- ✦Currently there is no way to distinguish between correct domain information and impersonators
- ✦DNSSec adds certificates and digital signatures to each domain

Firewalls

- Use packet filtering of IP addresses and ports to block undesired traffic
- Use application level gateways to provide acceptable services such as ftp, e-mail or web access
- Audit and log traffic
- A tunnel may allow access to normally blocked protocols by wrapping them in an allowed protocol

Intrusion Detection

- Gathers network packet information from a firewall or gateway
- Analyzes this information for certain patterns
- Triggers alarms or shuts down the gateway when malicious patterns are detected
- A Common Intrusion Detection Framework (CIDF) standard is being developed

Emerging Technologies

- Smart Cards
  - Credit card sized, contain certificates and other information
  - Widely used in Europe, slow to catch on here
- Biometric Devices
  - Measure physical characteristics of a person such as fingerprint, cornea, retina
  - Gradual acceptance due to invasiveness and CPU power needed for pattern recognition
- Advanced Encryption Standard (AES)
  - Replacement for DES
  - Larger block and key size

Issues

- Encryption
  - Export from the US is restricted
  - The US would like to control domestic use
  - Import and use are also restricted in other countries
  - Much PKI technology immature
- IPSec and TLS significantly slow computers and network devices
- Denial of service attacks are still hard to stop

Countermeasures Summary

Threat	Countered by
✦ Disclosure	IPSec, TLS, PGP, S-MIME
✦ Modification	IPSec, TLS, PGP, S-MIME
✦ Impersonation	TLS, PGP, S-MIME
✦ Repudiation	TLS, PGP, S-MIME
✦ Denial of service	DNSSec, Firewall
✦ Traffic analysis	IPSec, TLS, Firewall

References

- ✦ Simson Garfinkel, ***PGP: Pretty Good Privacy***, O'Reilly, 1995
- ✦ Rohit Khare, Editor, ***Web Security: A Matter of Trust***, The World Wide Web Journal 2:3, 1997
- ✦ Bruce Schneier, ***Applied Cryptography***, 2nd Edition, Wiley, 1996
- ✦ Richard E. Smith, ***Internet Cryptography***, Addison-Wesley, 1997
- ✦ William Stallings, ***Network and Internetwork Security***, Prentice Hall, 1995