Security

Learning Objectives

- Clarify need for security (what are we trying to protect?)
- Identify fundamental security objectives
- Review basic network attacks
- Classify typical attackers
- Examine technical safeguards
- Explore firewall options

Internet Security Needs

- “While non-technical publications are obsessed with the Internet, technical publications are obsessed with security”

  Chapman & Zwick, 1995

- Information view: marvelous technological advance in information dissemination with a major danger to pollute and destroy
- Transaction view: major deterrent to E-Commerce growth

What do we Need to Protect?

- Data
  - Information we keep on computers (product design, financial records, personnel data)
  - Lost time, lost sales, lost confidence
- Resources
  - Unauthorized use of computer time & space
- Reputation
  - Misrepresentation, forgery, negative publicity

Fundamental Security Objectives

- Four fundamental objectives of Info Security
  - **Confidentiality** - Protection from unauthorized persons
  - **Integrity** - consistency of data; no unauthorized creation, alteration or destruction
  - **Availability** - ensuring access to legitimate users
  - **Legitimate use** - ensuring appropriate use by authorized users

Basic Security Attacks

- **Intrusion** - unauthorized access and use of systems
- **Denial of service** - an attack aimed at preventing use of company computers
  - email bomb or flooding/Internet worm
  - disabled, rerouted or replaced services
- **Information theft** - network taps, database access, hacking into sites to give out more info or to wrong parties

Technical Safeguards

- Security Services
  - **Authentication** (entity, data origin)
  - **Access control** (prevent unauthorized access)
  - **Confidentiality** (disclosure, encryption)
  - **Data integrity** (value of data item)
  - **Non-repudiation** (falsely denying a transaction)

UNIX Password Security

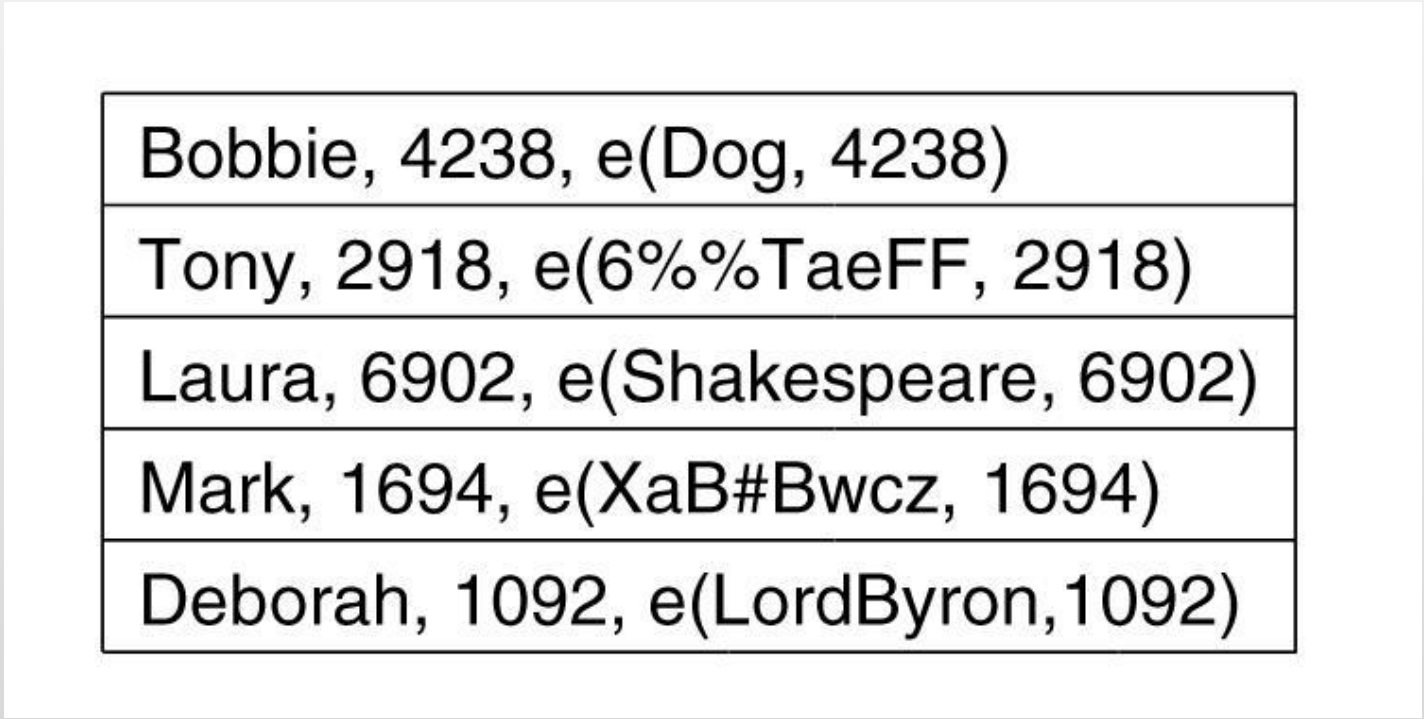


Figure 9-19. The use of salt to defeat precomputation of encrypted passwords.

Security Models

- **No Security** - not an option
- **Security thru Obscurity** - don't tell anyone where your site is
- **Host Security** - enforced security on each host; progressively difficult to manage as number of hosts increase
- **Network Security** - control network access to hosts and services; firewalls, strong authentication, and encryption

Firewall Solutions

- **Definition** - hardware &/or software components that restrict access between a restricted network & the Internet or between networks
- Logically - a separator, restricter, analyzer
- Rarely a single object
  - Restricts people to entering at a controlled point
  - Prevents attackers from getting close to other defenses (host controls)
  - Restricts people to leaving at a controlled point

Firewall Capabilities

- **Focus security decisions** - single point to leverage control
- **Enforce security policy** - minimize exceptions
- **Log Internet activity** - analysis
- **Limit exposure** - separate sensitive areas of one network from another or outside world

Firewall Limitations

- Can’t protect against
  - malicious insiders
  - connections that don’t go through it
  - new threats
  - viruses
    - scans for source & destination addresses & port numbers, not details of data

Types of Firewalls

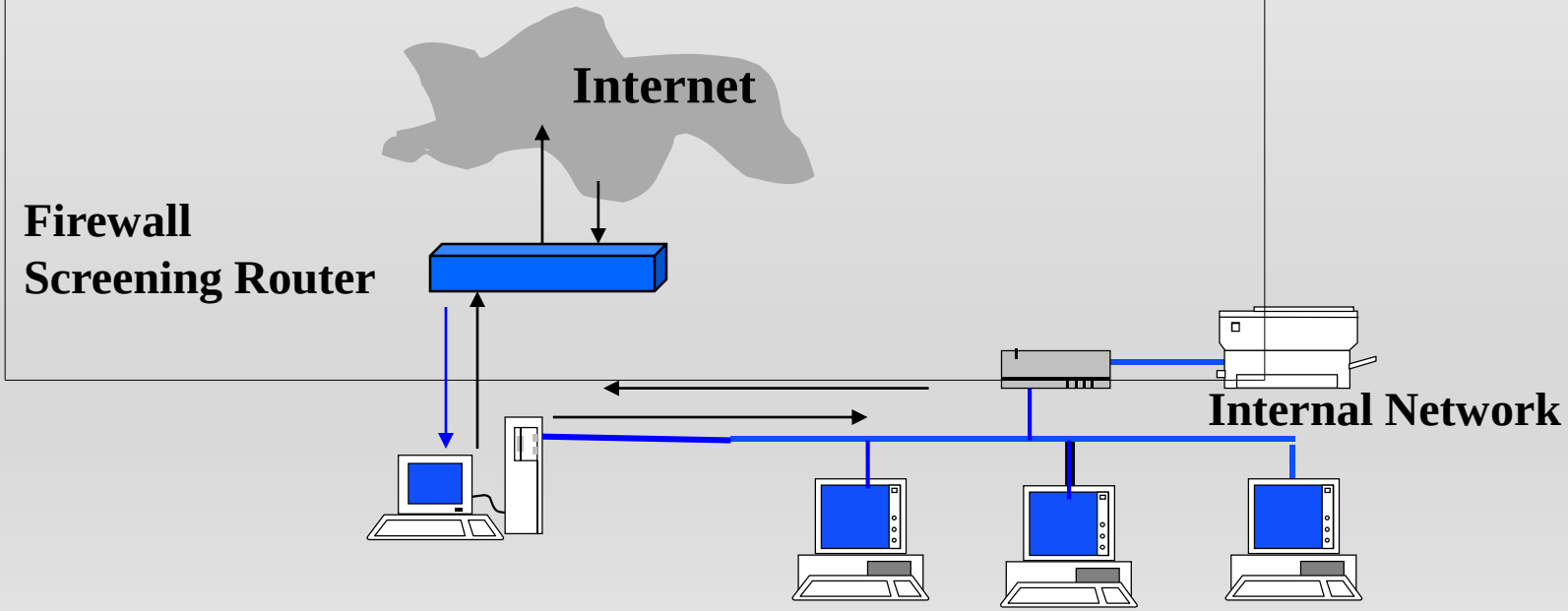
- **Simple traffic logging systems**
  - audit log file of files accessed (HTTPD)
  - site usage/demand hours/links/browsers used
- **IP Packet Screening Routers** (packet filtering gateway)
  - not only looks at ‘can’ it route, but ‘should’ it
  - selectively routes or blocks packets based on rules
  - based on protocols, destination (port 80), known source IP addresses

Types of Firewalls (cont.)

- **Hardened Firewall Host** (hardware)
  - Halts unauthorized users
  - Concentrates security, hides internal system names, centralizes & simplifies net management
- **Proxy Server** (software)
  - Deals with external server requests on behalf of internal clients
  - May limit certain HTTP methods (CGI or Java applets)

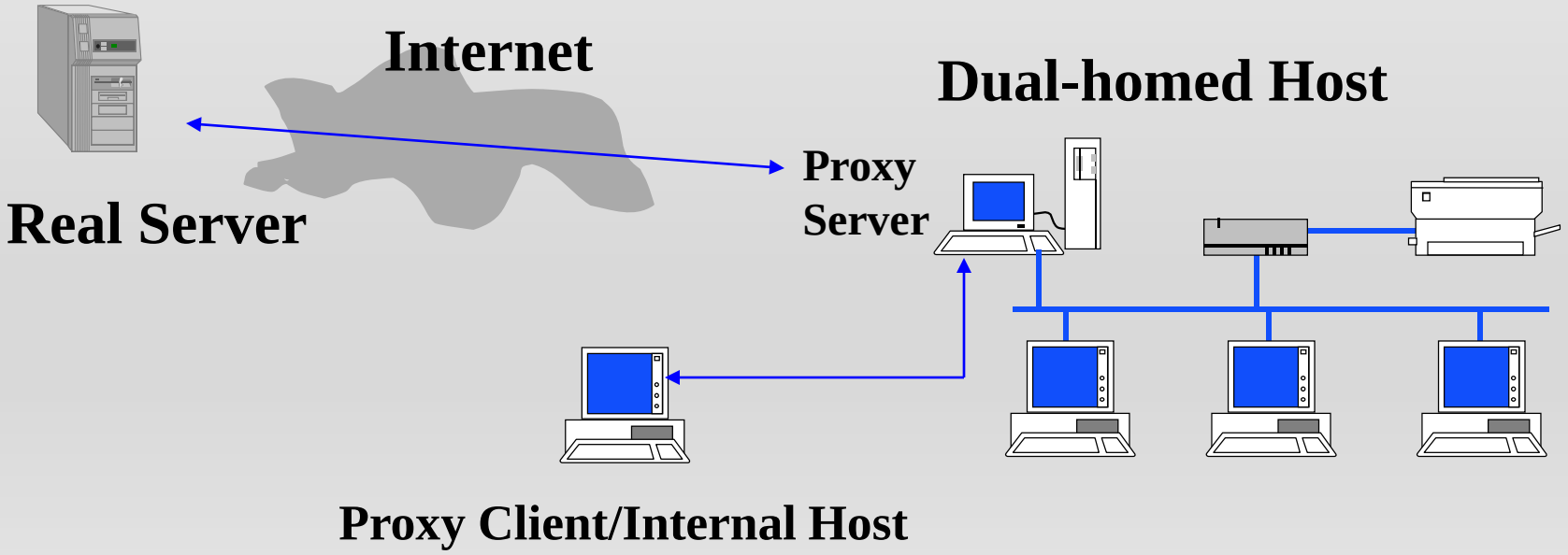
Common Solutions

- **Screened Host**
  - Host attached to internal network using separate router
  - Internal host is only internal system that net hosts can connect to
  - Packet filtering configuration determines if internal hosts may connect to other external hosts



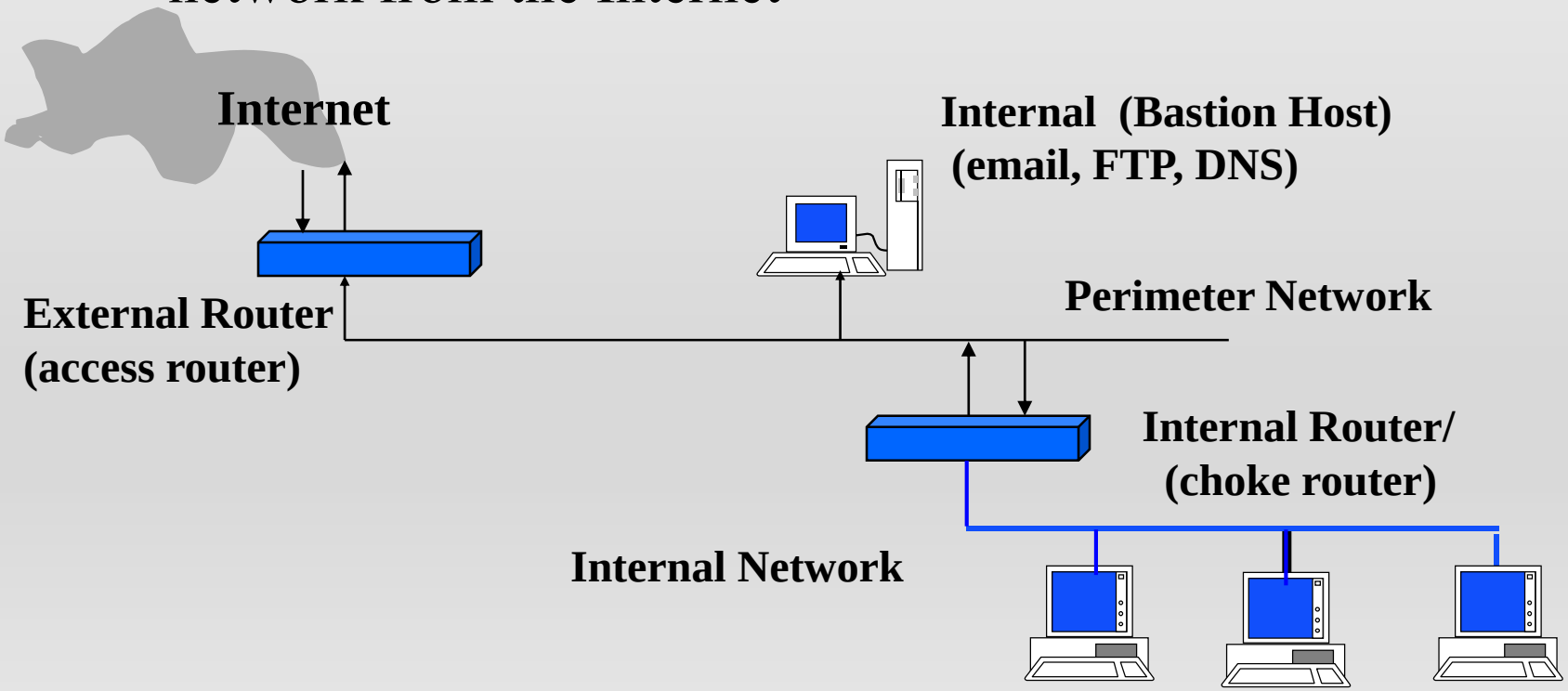
Common Solutions (cont.)

- Firewall Architectures
  - **Dual-homed host** (two network interfaces)
    - One communicates externally, one internally
    - No direct communication internal to external hosts



Common Solutions (cont.)

- **Screened Sub-Net** Architecture
  - Extra layer of security over screened host
  - Perimeter network further isolates the internal network from the Internet



Other Variations

- **Multiple Bastion Hosts**
  - Performance, redundancy, need to separate data & servers
  - Usenet, SMNP/DNS, FTP/WWW
- **Merge Interior & Exterior Routers**
  - Sufficient capability to specify inbound & outbound filters
  - Usually on the perimeter network
- **Merge Bastion Host & Exterior Router**
- **Use Multiple Exterior Routers**
  - Multiple connections to Internet or Internet + other sites
- **Multiple Perimeter Nets**
  - Redundancy, privacy

Not Recommended

- **Merging Bastion Host & Interior Router**
  - Breach of host leaves access to internal net
- **Using Multiple Interior Routers**
  - Routing software could decide fastest way to another internal system is via the perimeter net
  - Difficult to keep multiple interior routers configured correctly
  - Most important & complex set of packet filters
  - May need to use multiples to resolve performance bottlenecks or separate internal networks

Futures

- Third-generation Firewalls
  - combined features of packet filtering & proxy systems
- Client & server applications with native support for proxied environments
- Dynamic packet filtering
  - Packet rules modified “on the fly” in response to triggers
- Underlying Internet protocol undergoing revisions - IPv6

Cryptography Basics

Learning Objectives

- Identify requirements for secure communication
- Discuss cryptographic techniques
- Define cryptosystems & evaluate current encryption methods
- Review digital signature standards
- Discuss challenges of key management
- Review other security options & trust

Secure EC requirements

- For any network transaction:
  - 1. **Privacy** 2. **Confidentiality** 3. **Integrity**
- For reliable, secure communication:
  1. **Authentication**- we are who we say we are
  2. **Certification** - guarantee by 3rd party that 'wawwswa'
  3. **Confirmation** - digital receipt of transaction
  4. **Nonrepudiation** - binding agreement, digital proof of transaction
  5. **Encryption** - for all of the above, encoded passage of information over open networks

Cryptographic Techniques

- Secret writing or cryptic symbolization
- Technique - encryption algorithm or cryptosystem
  - defines a pair of data transformations
    - encryption and decryption
    - encryption = plaintext to ciphertext
    - both use ‘keys’ - seemingly random string
    - key length (number of bits) dependent upon cryptosystem

Encryption Cryptosystems

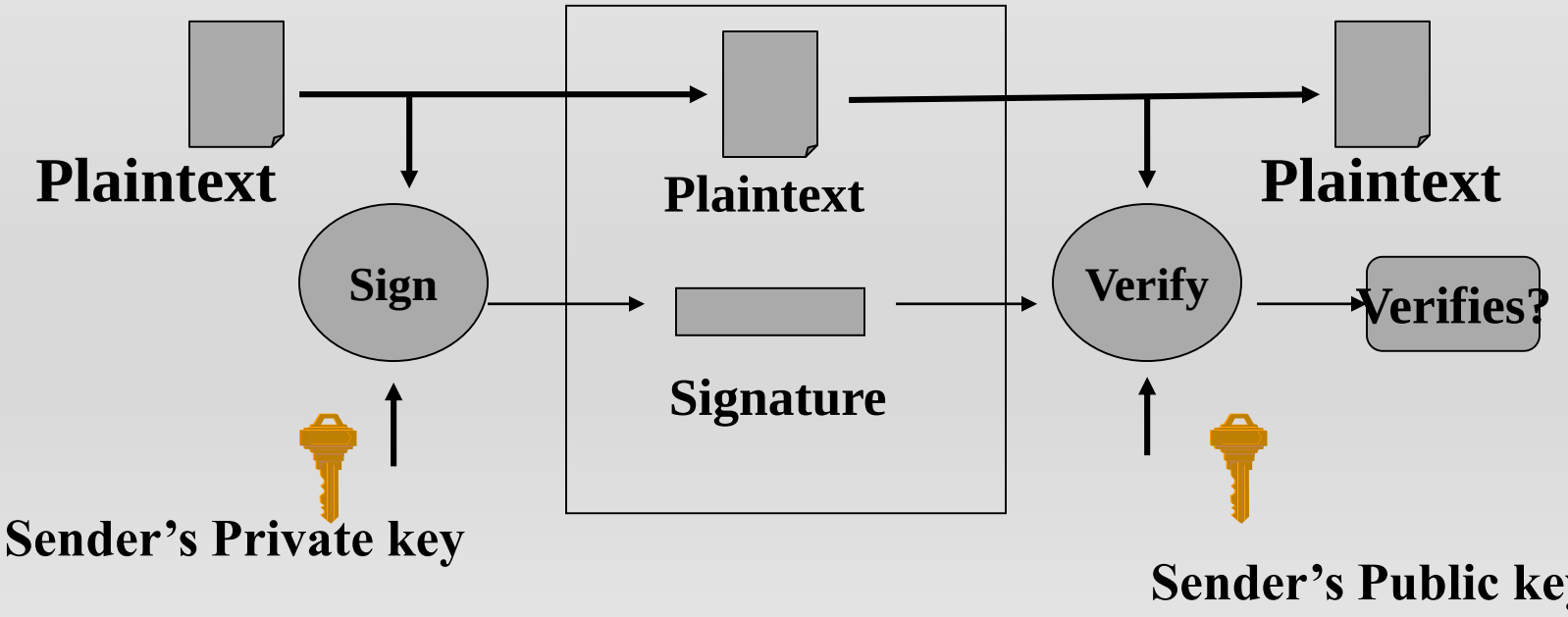
- Symmetric - **private key systems** (same key)
  - DES - Data Encryption Standard / 56-bit key
  - Vulnerable to exhaustive key search (2^{56} possibilities)
  - New standard in process

Encryption Systems (cont.)

- Asymmetric - **public key systems** (key pair)
  - 1976 - Stanford development
    - encryption mode: public key to private key
    - authentication mode: private key to public key
    - cryptosystems operating both ways called reversible
  - 1978 - RSA - reversible cryptosystem
    - based upon multiplication of two prime numbers
    - possible to crack via large computer resource
    - 1994 - 429-bit code cracked by scientific collaboration after 17 years
    - requires continual updating of modulus to protect
      - Jaws Tech, Inc. 4,096-bit (100 years)

Digital Signature Standards

- Accompanies a digitally encoded message
  - verifies originator of message
  - assures message not modified
  - satisfies non-repudiation requirement



Digital Key Management

- Life cycle management (cryptoperiod)
  - Generation & registration (random numbers)
  - Distribution & Availability
  - Key backup/recovery/key escrow
  - Replacement or update
  - Protection against disclosure
  - Termination or archival (confidentially archived information must be accessible after key retirement)

Other Security Methods

- Authentication Protocols built into communications protocol
  - transformed password (one-way function)
  - challenge-response (random value rec'd/sent)
  - time-stamp (synchronized clocks)
  - one-time password (different variant each login)
  - zero-knowledge technique (interactive proof)
- Address-based Authentication (network address)
- Personal Tokens (hardware & pw/ smart cards)
- Biometrics (fingerprint, voiceprint, handwriting)

Kerberos

- Complete authentication system - MIT
  - DES symmetric cryptography
  - Online authentication servers
  - Host server & clients share symmetric keys
  - Client requests a ‘ticket’ / sends to server
  - Ticket interpreted only by correct server
  - Session key is generated by authentication server after successful exchange
    - Authentication service (AS) / Ticket-granting Service (TGS) / Client/Server (CS) authentication exchange

Internet Security

- Three levels (Network, application, system)
  - Network - data packet integrity in-transit (Authentication/confidentiality/access controls)
    - IP layer/ headers + data = IP datagram
    - Not inherently secure (IP Spoofing - attacks w/false source addresses)
    - Authentication headers - integrity check values to indicate source & transit integrity of datagram
      - Security Association / Security Parameter Index

Internet Security (Network)

- Packet Encryption - Encapsulating Security Payload (ESP) provides confidentiality + integrity
  - Algorithm (transforms)
  - Tunnel-mode encryption (entire datagram encrypted)
  - Transport-mode encryption (data only encrypted)
- Key Management - no single standard
  - Host-oriented - all users share same association & key
    - Potential for decrypt another's messages
  - User-oriented - user has 1 or more association & keys
    - Lower risk / Superior method
- Firewalls - screening routers/proxy servers, perimeter networks

Internet Security (Network)

- Virtual Private Networks (VPN)
  - Secure groups of network sites using Inet backbone
    - IP tunneling / firewalls
- Messaging - special security needs above network measures
  - E-mail / mail enabled applications
    - Writer to reader protection via user agent
    - Message Transfer Agents (MTAs) = message transfer backbone (originating & delivering)

Internet Security (Messaging)

- Basic Message Protection Services
  - Message origin authentication / content integrity / content confidentiality / non-repudiation of origin
- Enhanced Message Protection Services
  - Confirmation services (proof of delivery & submission, non-repudiation of delivery & submission)
  - Other - I.e. security labeling service

Internet Security (Messaging)

- Secure Messaging Protocols
  - PEM - Privacy Enhanced Mail (basic services)
    - Wraps itself around standard mail message
  - MIME Security Multi-parts
    - Multi-purpose Internet Extensions - supports structuring of message body
    - Different body parts - text, image, audio, etc
    - 1995 specifications:
      - Security Multi-parts for MIME
      - MIME Object Security Services (MOSS)
      - Transforms messages into standard representation for transport

Internet Security (Messaging)

- S/MIME - RSA alternative to MOSS spec
  - built upon Public-Key Cryptography Stds (PKCS)
  - Protects MIME body parts, w/new data structure that becomes MIME content
  - Signed, enveloped or both
  - Mailer must be S/M compliant to read
- PGP (Pretty Good Privacy) free app using digital signatures & encryption
  - Defines own public key pair mgmt system
  - Casual e-mail, not wide-scale e-commerce

Internet Security (Messaging)

- X.400 Security
  - 1984/1988 international stds for mail gateways
  - Security features specific to X.400 protocols
  - X.400 secured mail cannot be conveyed over Inet
- Message Security Protocol (MSP)
  - US/DOS protocol similar to S/MIME, PKCS
  - Encapsulates message for basic & some enhanced services

Message Protocol Comparison

- S/MIME - strongest commercial acceptance
- PGP - free; not compatible w/public-key infrastructure; scalability questionable
- MSP - most comprehensive feature set; not commercially widespread
- MOSS - compatibility issues w/public-key; weak commercial vendor acceptance
- PEM - not compatible with MIME/outdated
- X.400 - most comprehensive features; not compatible with Inet messaging

Web Security

- Web Risks - server content / communications
- Solutions - SSL / S-HTTP / SET (evolving stds)
- SSL (Secure Sockets Layer) - session protection
  - Developed by Netscape to add communication protection
  - New layer protocol operating above TCP protocol
  - Protects any application protocol normally operating over TCP (HTTP, FTP, TELNET)
  - HTTPs represents SSL communication handling
  - Services: server authentication / client authentication / integrity (check values) / confidentiality (encryption)

Web Security (SSL cont.)

- SSL has two sub-protocols
  - SSL Record Protocol - defines basic format
    - Compression/MAC/encryption/data length
    - Assumes pre-existing keys
  - SSL Handshake Protocol - coordination
    - Negotiates protection algorithms between client and server for authentication, transmission of key certificates, establish session keys for use in integrity check and encryption
  - Domestic (128-bit) and intern'l (40-bit)

Web Security - S-HTTP

- Secure HTTP - security extension
  - Protects individual transaction request or response messages, similar to e-mail
  - Services: authentication, integrity, confidentiality + digital signatures (adds non-repudiation)
  - Flexibility in how messages are protected and key management

Web Security Threats

- Executable Programs - no foolproof defense
  - Java Applets - execution occurs on client system
    - Trusted execution environment (sandbox)
    - Should not: inspect or alter client files, run system commands or load system s/w libraries
    - Should: contact only originating server
    - Potential for hostile applets to send forged e-mail, crash browsers, kill running applets, consume resources
  - Active-X - reusable software components
- Source Authentication Programs -read signed code

Digital Certificates

Learning Objectives

- Differentiate digital signatures & certificates
- Define certificate authority & key methods
- Review certificate application process
- Evaluate X.500 certificate formats
- Examine certificate revocation & suspension
- Review certificate infrastructures
- Examine SET and DOD MISSI

Digital Signatures & Certificates

- Two levels of authentication
  - signatures -
  - certificates -
- Each requires a registration process

Certificate Authority (CA)

- Recognized & trusted party
  - Confirms identity of private key holder (subscriber)
  - Digitally signs the collection of information known as a certificate
  - Includes public key of private key holder
- 3rd Party (Open) - fee-based key distribution
- Internal to org or group (Closed) - self-contained key distribution & authentication

Public Key Methods

- Public key-private key distribution
  - Public key users have key to a CA
  - Requests copy of certificate & extracts public key (relying party)
- Certificate is self-protecting
  - CA's digital signature is inside the certificate
  - CA's signature would not verify if tampered with
- Certificates distributed over unsecured channels
- Downside is multiple CAs (certification path)

Certificate Issues

- Validity Period - Restricted lifetimes
  - Limit cryptanalysis & vulnerability
  - Scheduled start & expire times
- Legal aspect of closed vs. open CAs
  - Open may provide better evidence
  - Similar role to that of notary
  - Utah Digital Signature Law -
    - Reliability of any digital signature depends upon reliability of a CA association of the key w/a person

Key Management

- Key pair generation & transfer
  - Key-pair holder system
    - Generated in user system where private key stored
    - Supports non-repudiation / private key never leaves
  - Central system
    - Generated in other system or CA
    - Greater resource & controls, higher quality, back-up or archive functions
- Mixed methods for types of key-pairs
    - Digital signature at key holder encryption at CA

Key Management (cont.)

- Private-key Protection / Access Control
  - Storage in tamper-resistant device (smart card)
  - Storage in encrypted file
  - Password or PIN for personal authentication
  - Software control / digital wallet
- Key-pair Update / policy
- Different Types / Different Requirements
  - RSA can perform encryption & signatures
    - Digital sig keys - should be created & remain on system (ANSI X9.57); recreated as needed; no archival required
    - Encryption keys - backup & archival needed

Key Management (cont.)

- Other differing requirements
  - Encryption limits (56-bit) restrict signature strength
  - Two types may have differing cryptoperiods
  - Not all algorithms have RSA dual properties
  - Private encryption keys may have to be provided to government, digital signature keys should never be

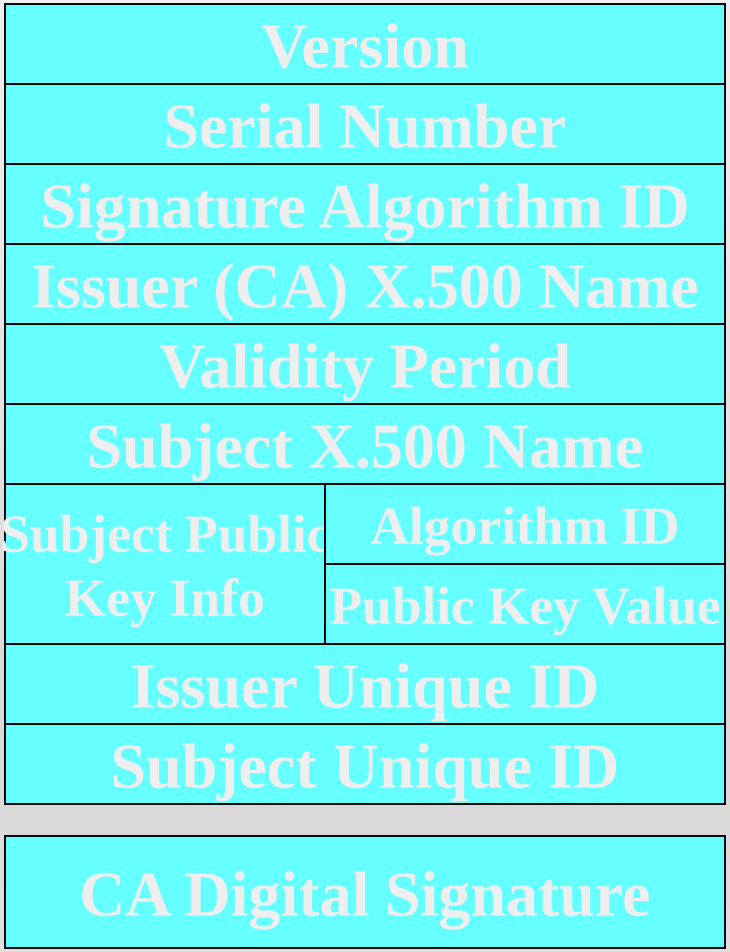
Certificate Application Process

- Registration with Certificate Authority
  - Establish relationship & provide subscriber info
  - Explicitly apply & accept certificate
- Authentication
  - Personal presence, ID documents
  - Use of intermediaries as local registration authorities
- Distribution
  - Accompanying digital signature
  - Directory Service (X.500 standards)

Certificate Distribution Protocols

- International Telecom Union (ITU) & ISO
- 1984-88 - X.509 for public key distribution
- Slow acceptance due to competitive issues
- Proprietary alternatives
  - MS Exchange, Notes directory, Novell NDS, Banyan StreetTalk
- LDAP (Internet Lightweight Directory Access) access protocol rather than db technology
- S/MIME or specialized Web Servers

X.509 Certificate Format



Version 1, 2, or 3
Unique for this certificate
Used by CA (DSS w/SHA hash *)
Issuing CA name
Start & expiry date
Holder of private key
Value of holder's public key & algorithm (RSA w/MD5 hash *)
Optional unique ID for CA
Optional unique ID for holder

*** Object identifier**

Certificate Extensions

- X.509 V.3 extensions clarify owners & use
  - Key & policy information
    - Authority & Subject key ID, Key use, period, policy
  - Subject & issuer attributes
    - Alternative names (e-mail), Company, address, etc
  - Certification path constraints
    - Links to CA via root & directory infrastructures
  - Certificate revocation lists (CRL)

Revocation & Suspension

- Limited life-time (validity period)
- Suspected compromise of private key
- Name or attribute changes
- Revoked by CA, subscriber, employer
- CRL - certificate revocation list (X.509)
  - Time-stamped, signed, and distributed
  - Posted to Web site or via X.500 directory
  - Real-time revocation checking (resources)

CRL Format

- Standard format for certificate revocation
  - CRL Number
  - Reason Code
    - Key compromise, CA compromise, Affiliation change, superceded, cessation of operation
  - Invalidity Date
  - Distribution Points
    - File size control - entry removal, different CRL by reason, CA control
- CRL hold list for suspension

Validity Periods

- Encryption Key Pairs
  - Public key used only while certificate is valid
  - Private key for decryption part of local policy
- Digital Signature Key Pairs
  - Historic validation (non-repudiation)
    - All certificates, CRLs or status as it existed
  - Real-time (valid certificate exists now)
    - Software pub, CA sign on a public key, time stamp
- CA Signature Key Pairs
  - Both real-time & historic validation / impacts all certificates signed

Certificate of Authorization

- Proper use (i.e. purchasing authority)
  - Commit corporation, authorized official, guaranteeing authenticity (i.e. software)
  - Authorization information
    - Certificate can convey (Basic Constraints field)
    - CA certifying identity may not know / corp. security
    - Authority may change prior to validity period
- Attribute Certificates (bound to certificate subject)
  - ANSI X9 from financial industry / attribute authority
- Privilege Attribute Certificate (passed to application server & attached to session)

Certificate Infrastructures

- SDSI (Simple Distributed Security Infrastructure) -
  - 1996 Subset of X.509 functionality/omits complexity
  - Specifies local linked naming (person-company)
  - Adds simple types of authorization (group definition, delegation certificate)
- SPKI (Simple Public-Key Infrastructure)
  - Under development in IETF
    - Assigns authorizations to a public key w/o binding identity to companion private key
    - Simpler encoding scheme / closed group potential

Public Key Infrastructure

- Wide spread use requires practical methods
  - Scalability
  - Multiple Applications
  - Interoperability among Infrastructures
  - Multiple Policies & Paths
  - Simple Risk Management
  - Limitation of CA Liability
  - Standards / Structuring Conventions (Trust Models)

Infrastructure Evolution

- General Hierarchies
- Top-down Hierarchies (Privacy Enhanced Mail - PEM)
  - Internet Policy Registration Authority (IPRA)
    - Operated by MIT under Internet Society
  - Policy Certification Authorities (PCA)
    - Must register with IPRA / specialized or closed
  - Lower-Level Certificate Authorities
    - Represent organizations or departments

Evolution (cont.)

- Forest of Hierarchies
  - Trust issue of a single authority
  - International considerations
  - DOD proposing w/defense orgs of allied nations
  - Complexity increases as it grows
- PGP's Web of Trust (Each user is own CA)
  - User collects keys on a key ring and designates to what extent the key is trusted

Certificate Policies

- Progressive-Constraint Trust Model
  - Any CA specifies conditions or limitations on subject
- Certificate Policies Extension
  - X.509 V.3 adds field for conveying certificate policy references
  - User systems are preprogrammed to accept an appropriate level of policy references
  - Critical or non-critical flags (must have v. like)

Certificate Management

- Legislation
  - Spotty in US and global
    - Utah, California, Denmark, Germany, Italy
    - UN Model Law / UNCITRAL planned study
  - Technology-neutral or specific
  - Minimalist approach for flexibility
    - Validity & enforceability to electronic messages
  - Quality, Standards, & Liability

SET Infrastructure

- Visa / MasterCard joint venture
- Comprehensive protocol & infrastructure
- Public-key technology
  - Encryption of payment instructions
  - Authentication of card holders & merchants
  - Authentication of acquirers (processor banks)
  - Integrity-protection of transaction info
- Top-down hierarchy infrastructure
  - Root CA, Brand CA, Cardholder CA, Merchant CA

DOD MISSI Infrastructure

- NSA Multilevel Information Systems Security Initiative
- DOD Defense Messaging System (DMS)
  - Top-down hierarchy
    - Policy Approving Authority
    - Policy Creating Authority
    - Administrative CA
    - Organizational Registration Authority