Computers and Society
Applications of Encryption

Chris Brooks

Department of Computer Science

University of San Francisco

3-0: Public Key Infrastructure

- For real-world applications, a complex web of software systems is required to ensure security.
- This is referred to as a Public Key Infrastructure (PKI).
- Focus shifts from provable protocol properties to system design.
- One of the primary functions of a PKI is the establishment of trust between users with no prior history.
- A certificate authority can provide this, serving as a trusted third party.

3-1: Certificate Authority

- A certificate authority has a number of functions within a PKI
  - Authentication
  - Key generation
  - Key revocation
- Many commercial entities serve as CAs

3-2: *Certificate Authorities*

- A Certificate Authority will wrap a userÂŠs public key in a certificate.
  - X.509 is most common standard.
- Contains the user’Šs identity and public key.
- Signed with the CAŠs private key.
- Risk is shifted:
  - Previously: could unknown user A be compromised?
  - Now: could the CA be compromised?

3-3: Trust Models

- Hierarchical
  - One root CA
  - Considered able to “vouch for” itself.
  - Scalable and fast
- Tradeoff: More levels of hierarchy requires more work to design and maintain, but provides increased reliability/redundancy.

3-4: Trust Models

- Distributed (Web of Trust)
    - No root CA
    - Users are able to authenticate each other
    - Same approach as P2P software
- Highly redundant, but not very efficient.
- Awkward fit for e-commerce.

3-5: Applications of Encryption

- How can we apply encryption to different sorts of protocols?
  - Message-oriented
  - Transaction-oriented
  - Session-oriented
- Steganography
- Digital Watermarking

3-6: Message-oriented protocols

- Each message is independent
- Forwarded and stored in intermediate connections
  - Email is an example
- Requirements
  - Origin authentication, data integrity, data confidentiality, non-repudiation of origin
  - Might also want confirmation

3-7: MIME

- MIME (Multipurpose Internet Mail Extensions) is a set of specs for encoding heterogeneous data types within a single message.
- Text, images, applications, etc.
- Allows heterogeneous applications, platforms, networks to encode, decode and transmit rich data types.
- Defines header format, data types, encoding.
- Messages are encoded using base64 - encodes non-text with text characters.
- No security, though

3-8: ***S/MIME***

- S/MIME: extensions to add public-key encryption to MIME.
- Defines a MIME content type:
  - Application/x-pkcs7-mime
  - Unprotected data is enveloped
    - This encompasses encryption, signing, and both.
  - Signatures: standard public-key signing.
  - Encryption:
    - Symmetric-key encryption of data
    - Added to a data structure that is encrypted with a private key

3-9: S/MIME Example

- I wish to sign the email “letÂŠs meet on Friday”
- Document is converted to canonical form
  - CR/LF fixed, registered charset used. (for text)
- Document is hashed and signed with my private key.
- Body and signature formatted using ASN.1
  - Standard that specifies representation of arbitrary data types
  - Result is encoded as base64 and given the MIME type application/x-pkcs7-mime

3-10: ***S/MIME Example***

- What if I also want to encrypt my message?
- Canonicalize message
- Encrypt with a random symmetric key
- Encrypt the symmetric key with recipientÂŠs public key
- Encode both encrypted key and message with ASN, then base64
- Result is given the MIME type application/x-pkcs7-mime

3-11: S/MIME

- One problem: A non-S/MIME compatible mailer cannot read a message that is signed but not encrypted.
- Alternate structure:
  - Uses multipart/signed MIME type
  - Both plaintext and signed document are included.

3-12: Transaction-oriented protocols

- In a transaction, multiple messages must be sent
- Request, reply, confirmation, authorization
- Security must ensure that messages are sent in the proper order and that the sequence of messages is secure.

3-13: SET

- SET (Secure Electronic Transaction) is a protocol being developed by Visa and Mastercard
- Uses a public-key system to ensure secure payment.
- Provides confidentiality, data integrity, authentication of cardholder and merchant
- Establishes a hierarchical public-key infrastructure
- Public keys are used to exchange symmetric keys.

3-14: SET overview

- *Cardholder* negotiates an order with the *merchant*.
- Merchant authorizes the transaction with the *acquirer*
  - A financial institution that acts as a clearinghouse for bank card transactions.
- Acquirer may communicate with *issuer*.
  - Institution that issued your credit card.
  - This communication will happen over a private channel.
  - May not take place at the time of transaction.

3-15: Dual Signatures

- SET prevents information leakage through the use of dual signatures.
- I want to buy a car and need the bank to transfer the funds.
- I donÂŠt want the dealer to see my bank balance
- I donÂŠt want the bank to see the terms of the deal.
- I only want the money to be transferred if my offer is accepted by the car dealer.

3-16: Dual Signatures

- I generate a message digest for each message and sign them.
- I then concatenate the digests and sign that.
- I send each party their message, plus the concatenated version.
- If the dealer accepts my offer, she sends the digest of the offer to the bank.
- Bank can concatenate this digest with the digest of the authorization I sent them to verify authenticity.

3-17: Session-oriented protocols

- A session is a protocol for the ongoing exchange of messages between two agents.
  - TCP is a session-oriented protocol
- Messages are considered to be part of a larger communication
  - Reliability, in-order delivery, timeliness important
- Initial handshake used to establish a security context.

3-18: SSL

- Sits on top of TCP
- Provides secure communication over TCP sockets.
    - SSH, scp, https all use SSH.
- Provides authentication of both server and client, data integrity, and confidentiality.

3-19: SSL

- SSL consists of two sub-protocols:
- SSL Handshake Protocol
  - Negotiates encryption scheme
  - Transmit certificates
  - Establish symmetric session keys
- SSL Record Protocol
  - Compresses and encrypts data
  - Numbers packets
  - Generates checksum
  - Provides data length (for padding)

3-20: Steganography

- Steganography is the science of embedding a secret message within another message.
- Secret is carried innocuously within a harmless-looking wrapper.
  - Useful when an encrypted message might draw suspicion.
- One use of steganography is the embedding of *watermarks*

3-21: Watermarks

- Traditionally, a watermark has been used to verify the authenticity of a document.
  - Difficult to reproduce.
  - Tampering will destroy watermark.
- DriverŠs Licenses, diplomas, official letterhead.
- More recently, used to track or prevent redistribution
  - TV logos

3-22: *Digital Watermarks*

- Three purposes:
  - Ensure authenticity of digital goods
    - Should be difficult to copy watermark.
  - Prevent unauthorized use/ensure copyright
  - Prevent copying
    - Should be difficult to remove watermark.

3-23: Digital Watermarks

- Adding the watermark to the image itself prevents removal by changing the format. (e.g. GIF->JPEG)
- Research challenge: How to construct a watermark that is resistant to manipulation of the document
  - Cropping, editing, rotation, scaling, D/A/D conversion, noise addition, etc.

3-24: Authentication

- Proof of authenticity can be embedded into a digital good.
- Author generates a watermark, signs it, and embeds it.
- Commercial services might assign an ID
- Presence of watermark is advertised.
- User can verify, creator, date created, etc.

3-25: Copy Protection

- Watermarking can be used to prevent illicit copies from being made.
- Requires hardware support.
- CD -> DAT: Audio watermark included a flag; allowed one copy (for personal use).
  - Difficulty: manufacturer compliance.
- DVD: Proposed schemes allow manufacturer to specify copy protection
  - No copies, one copy, many copies.
  - Again, the problem is that manufacturers must comply

3-26: *Usage tracking*

- Content Providers can also use a watermark to track usage.
- Help find and track unauthorized usage, ensure copyright.
- Each copy of an image has a unique identifier
  - Referred to as a fingerprint
  - Buyer, timestamp, etc.
- Images also have a watermark embedded
- Provides notification of copyright

3-27: Usage Tracking

- Finding the user who originally posted/gave away the image is called the traitor tracing problem.
- Similar: who allowed their smartcard to be used to build a pirate decoder?
- Web spiders can be used to crawl sites, download images, check for watermarks and extract the corresponding fingerprints.
- Legal issues are unresolved
- Am I responsible for all loss that results from giving away copyrighted material?

3-28: Example: Replacing bits

- Image, sound, and video are resistant to changes in the low-order bits.
  - This is what makes compression possible.
- In a 24-bit AIFF, the lowest bits can be treated as noise.
- We can replace those low-order bits with bits that encode a message.
- This could be a string, another image, or anything else that can be represented digitally.

3-29: Wrinkles

- Simply changing all the lower-order bits is very brittle.
  - Attackers need only flip a few bits to remove a watermark.
  - Depends on keeping the hiding mechanism secret.
- A key can be used to specify which blocks contain the watermark.
- The watermark may be redundantly embedded.

3-30: Wrinkles

- Manipulating low-order bits is easy to understand, but not very secure.
- Easy to detect and defeat.
  - e.g. uncompress and recompress, crop, shear.
- This is called a bit-plane or least-significant-bit watermark.

3-31: Wrinkles

- More secure watermarks can be generated by transforming the image and changing bits in the transformed space.
- Luminance, quantization in images
- Choose random pairs and vary contrast
- Frequency, harmonics in sounds
  - Fourier transform
- This falls into the realm of signal processing ÂŰ beyond our scope!

3-32: Attacks

- Add jitter
  - Moves the location of blocks containing a message.
- Mosaic
  - Single image is chopped into several subimages.
  - Defeats spiders.
- Addition of watermarks
  - It is possible in some schemes for an attacker to embed his own watermark and mark it appear to be the original.
  - Timestamping by a trusted third party can solve this.

3-33: *Larger Issues in Watermarking*

- The assumption underlying watermarking is that information providers can prevent copying and earn profits by selling their work directly.
- ItŠs not clear that this assumption is reasonable.
- History is full of examples of these schemes being circumvented.
- What are alternative ways for information producers to get paid?