# Cryptography and Network Security

Third Edition

by William Stallings

Lecture slides by Lawrie Brown

# Chapter 13 –Digital Signatures & Authentication Protocols

*To guard against the baneful influence exerted by strangers is therefore an elementary dictate of savage prudence. Hence before strangers are allowed to enter a district, or at least before they are permitted to mingle freely with the inhabitants, certain ceremonies are often performed by the natives of the country for the purpose of disarming the strangers of their magical powers, or of disinfecting, so to speak, the tainted atmosphere by which they are supposed to be surrounded.*

**—*The Golden Bough*, Sir James George Frazer**

# Digital Signatures

- have looked at message authentication
  - but does not address issues of lack of trust
  - Mary may forge a message and claim it came from John
  - John can deny sending a meesage
- digital signatures provide the ability to:
  - verify author, date & time of signature
  - authenticate message contents
  - be verified by third parties to resolve disputes
- hence include authentication function with additional capabilities

# Digital Signature Properties

- must depend on the message being signed
- must use information unique to sender
  - to prevent both forgery and denial
- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
  - with new message for existing digital signature
  - with fraudulent digital signature for given message
- be practical save a copy of the digital signature in storage

# Direct Digital Signatures

- involve only sender & receiver
- assumed receiver has sender's public-key
- digital signature made by sender signing entire message or hash with private-key
- can further encrypt using receivers public-key
- important that sign first then encrypt message & signature
- security depends on sender's private-key
  - Have problems if lost/stolen

# Arbitrated Digital Signatures

- involves use of arbiter A
  - validates any signed message
  - then dated and sent to recipient
- requires a great deal of trust in arbiter
- can be implemented with either private or public-key algorithms
- arbiter may or may not see message

## Table 13.1 Arbitrated Digital Signature Techniques

| (a) Conventional Encryption, Arbiter Sees Message |
|---|
| (1) X → A: $M \| \mathrm{E}_{K_{xa}}[ID_X \| \mathrm{H}(M)]$ |
| (2) A → Y: $\mathrm{E}_{K_{ay}}[ID_X \| M \| \mathrm{E}_{K_{xa}}[ID_X \| \mathrm{H}(M)] \| T]$ |
| **(b) Conventional Encryption, Arbiter Does Not See Message** |
| (1) X → A: $ID_X \| \mathrm{E}_{K_{xy}}[M] \| \mathrm{E}_{K_{xa}}[ID_X \| \mathrm{H}(\mathrm{E}_{K_{xy}}[M])]$ |
| (2) A → Y: $\mathrm{E}_{K_{ay}}[ID_X \| \mathrm{E}_{K_{xy}}[M] \| \mathrm{E}_{K_{xa}}[ID_X \| \mathrm{H}(\mathrm{E}_{K_{xy}}[M])] \| T]$ |
| **(c) Public-Key Encryption, Arbiter Does Not See Message** |
| (1) X → A: $ID_X \| \mathrm{E}_{KR_x}[ID_X \| \mathrm{E}_{KU_y}(\mathrm{E}_{KR_x}[M])]$ |
| (2) A → Y: $\mathrm{E}_{KR_a}[ID_X \| \mathrm{E}_{KU_y}[\mathrm{E}_{KR_x}[M]] \| T]$ |

Notation:

X = sender
Y = recipient
A = Arbiter
$M$ = message
$T$ = timestamp

# Authentication Protocols

- used to convince parties of each others identity and to exchange session keys
- may be one-way or mutual
- key issues are
  - confidentiality – to protect session keys
  - timeliness – to prevent replay attacks

# Replay Attacks

- where a valid signed message is copied and later resent
  - simple replay
  - repetition that can be logged
  - repetition that cannot be detected
  - backward replay without modification
- countermeasures include
  - use of sequence numbers (generally impractical)
  - timestamps (needs synchronized clocks)
  - challenge/response (using unique nonce)

# Using Symmetric Encryption

- as discussed previously can use a two-level hierarchy of keys
- usually with a trusted Key Distribution Center (KDC)
  - each party shares own master key with KDC
  - KDC generates session keys used for connections between parties
  - master keys used to distribute these to them

# Needham-Schroeder Protocol

- original third-party key distribution protocol
- for session between A B mediated by KDC
- protocol overview is: Fig 7.9

**1.** A→KDC: $ID_A \| ID_B \| N_1$

**2**. KDC→A: $E_{Ka}[Ks \| ID_B \| N_1 \| E_{Kb}[Ks \| ID_A]]$

**3.** A→B: $E_{Kb}[Ks \| ID_A]$

**4.** B→A: $E_{Ks}[N_2]$

**5.** A→B: $E_{Ks}[f(N_2)]$

# Improvements to the Needham-Schroeder Protocol

- used to securely distribute a new session key for communications between A & B
- Secure even if Step 3 is replayed
- but is vulnerable to a replay attack if an old session key has been compromised
  - then message 3 can be resent convincing B that is communicating with A
- modifications to address this require:
  - timestamps (Denning 81) (clock sync. Issue)
  - using an extra nonce (Neuman 93) (solves sync Issue)

# One-Way Authentication

- required when sender & receiver are not in communications at same time (eg. email)
- have header in clear so can be delivered by email system
- may want contents of body protected & sender authenticated
  - The receiver wants some assurance of the identity of the alleged sender

# Using Symmetric Encryption

- can refine use of KDC but can't have final exchange of nonces:
  **1.** A→KDC: $ID_A \| ID_B \| N_1$
  **2**. KDC→A: $E_{Ka}[Ks \| ID_B \| N_1 \| E_{Kb}[Ks \| ID_A]]$
  **3.** A→B: $E_{Kb}[Ks \| ID_A] \| E_{Ks}[M]$
- Only the intended recipient can read it
- Certain level of authentication of A
- does not protect against replays
  - could rely on timestamp in message, though email delays make this problematic

# Public-Key Approaches

- have seen some public-key approaches
- if confidentiality is major concern, can use:

  $A \rightarrow B: E_{KUb}[Ks] \,||\, E_{Ks}[M]$

  – has encrypted session key, encrypted message
  – More efficient than simply $E_{KUb}[M]$
- if authentication is the primary concern

  use a digital signature with a digital certificate:
  – $A \rightarrow B: M \,||\, E_{KRa}[H(M)]$, problematic
  – Encrypt everything using receiver's public key
  – $A \rightarrow B: M \,||\, E_{KRa}[H(M)] \,||\, E_{KRas}[T||ID_A||KU_a]$
  – with message, signature, certificate

# Digital Signature Standard (DSS)

- A public-key scheme for digital signature use only, combines hash and encryption
- designed by NIST & NSA in early 90's
- DSS is the standard, DSA is the algorithm
  - Based on number theory
  - security depends on difficulty of computing discrete logarithms
  - creates a 320 bit signature, but with 512-1024 bit security
  - Computationally efficient

# Summary

- have considered:
  - authentication protocols (mutual & one-way)
  - digital signature standard