Cryptography

Lecture 27
Announcements

• Scholarly Paper EC due today
• “Optional” HW10 due on Wednesday, 5/15
• Final Exam Info:
  – Monday, 5/20 from 1:30-3:30pm in CSI 3117 (our regular classroom)
  – Final review sheet on course webpage, solutions are on Canvas
  – Cheat sheet posted on Canvas
  – TA OH on 5/15 TBA
  – Instructor OH 5/17 TBA
Agenda

• This time:
  – Current Events Presentations
  – Wrapping Up
  – Final Review
Certificates and Public-Key Infrastructure
A single certificate authority

- $pk_{CA}$ must be distributed over an authenticated channel
  - Need only be carried out once
- Usually, $pk_{CA}$ included in browser, browser programmed to automatically verify certificates as they arrive.
- To obtain certificate, must prove that url is legitimate.
- All parties must completely trust CA.
Multiple certificate authorities

• Parties can choose which CA to use to obtain a certificate.
• Parties can choose which CA’s certificates to trust.
• Problem: some CA may become compromised.
• Each user must manually decide which CA to trust.
Delegation and certificate chains

• Example of certificate chain:

\[ pk_A, cert_{B\rightarrow A}, pk_B, cert_{C\rightarrow B} \]

Need only trust Charlie in the above example.

• Certificate asserts that legitimate party holds public key and that the party is trusted to issue other certificates.

  – Delegation of CA’s ability to issue certificates
The “web of trust” model

• Model is used by PGP (“pretty good privacy”) email encryption software for distribution of public keys.
• Anyone can issue certificates to anyone else
• Each user must decide who to trust
• Example:
  – Alice holds $pk_1, pk_2, pk_3$ for users $C_1, C_2, C_3$
  – Bob has certificates $cert_{C_1 \rightarrow B}, cert_{C_3 \rightarrow B}, cert_{C_4 \rightarrow B}$
• Public keys and certificates can be stored in a central database.
Invalidating Certificates

• Expiration: Include expiration date as part of the certificate.
  – Very coarse grained method. E.g. employee leaves company but certificate does not expire for a year.

• Revocation
  – CA includes a serial number in every certificate it issues.
  – At the end of each day, the CA will generate a certificate revocation list (CRL) with the serial numbers of all revoked certificates.
  – CA will sign the CRL and the current date.
  – Signed CRL is then widely distributed.
Putting it all together: SSL/TLS

• TLS: Transport Layer Security Protocol
  – Protocol used by browser when connecting via https
• Standardized protocol based on a precursor called SSL (Secure Socket Layer).
  – Latest SSL version: SSL 3.0
  – TLS version 1.0 released in 1999
  – TLS version 1.1 in 2006
  – TLS version 1.2 (current) in 2008
  – 50% of browsers still use TLS 1.0
• Allows a client (web browser) and a server (website) to agree on a set of shared keys and then use those keys to encrypt and authenticate their subsequent communication.
• Two parts:
  – Handshake protocol performs authenticated key exchange to establish the shared keys
  – Record-layer protocol uses shared keys to encrypt/authenticated the communication.
• Typically used for authentication of servers to clients (usually only servers—websites—have certificates).