Recap

• Three types of functions
  – Cryptographic hash, symmetric key crypto, asymmetric key crypto
• Cryptographic hash
  – Easy to compute \( h(m) \)
  – Hard to find an \( m \), given \( h(m) \)
  – Hard to find two values that hash to the same \( h(m) \)
• How to find collisions?
  – Birthday paradox: for 50% prob. & \( m \) bits, \( \sim 2^{m/2} \)
• Symmetric key crypto
  – MAC: Compute \( H = AES_K (SHA1(M)) \) & Send <\( M, H \)>
• Asymmetric key crypto
  – Guarantees rely on computational hardness

Heard of Firesheep?

• Firesheep
  – A Firefox extension
  – A packet sniffer to intercept unencrypted cookies from certain websites (such as Facebook and Twitter)
  – Allows the user to take on the log-in credentials of the victim
• Solution?
  – Encrypt your traffic!
  – This is before Facebook started using https, but now Facebook uses https.

“Securing” HTTP

• Threat model
  – Eavesdropper listening on conversation (confidentiality)
  – Man-in-the-middle modifying content (integrity)
  – Adversary impersonating desired website (authentication, and confidentiality)
• Enter HTTP-S
  – HTTP sits on top of secure channels
  – All (HTTP) bytes written to secure channel are encrypted and authenticated

Encrypted Communication

Hey, I want to be more secure

Sure, use this public key and encrypt your traffic

Key: f-pub

What is wrong with this?

– How do you know you’re actually talking to Facebook and f-pub belongs to Facebook?
Digital Certificates

- A digital certificate is a statement signed by a third party principal, and can be reused
  - e.g., Verisign Certification Authority (CA)
- To be useful, certificates must have:
  - A standard format, for construction and interpretation
  - A protocol for constructing chains of certificates
  - A trusted authority at the end of the chain
- Example
  - When Facebook sends you the public key, it also sends a signature for the public key signed by Verisign.
  - You pre-store Verisign’s public keys & certificates (self-signed by Verisign), i.e., you have already established trust with Verisign.
  - Use Verisign’s public key to verify Facebook’s public key.

X.509 Certificates

- The most widely used standard format for certificates
- Format
  - Subject: Distinguished Name, Public Key
  - Issuer: Distinguished Name, Signature
  - Period of validity: Not Before Date, Not After Date
  - Administrative information: Version, Serial Number
  - Extended information
- Binds a public key to the subject
  - A subject: person, organization, etc.
- The binding is in the signature issued by an issuer.
  - You need to either trust the issuer directly or indirectly (by establishing a root of trust).

Transport Layer Security (TLS)

- SSL (Secure Socket Layer) was developed by Netscape for electronic transaction security.
- SSL was adopted as TLS as an Internet standard.
- A protocol layer is added below the application layer for:
  - Negotiating encryption and authentication methods.
  - Bootstrapping secure communication
- It consists of two layers:
  - The Record Protocol Layer implements a secure channel by encrypting and authenticating messages
  - The Handshake Layer establishes and maintains a secure session between two nodes.
TLS Record Protocol

- The record protocol takes an application message to be transmitted:
  - fragments the data into manageable blocks,
  - optionally compresses the data,
  - computes a message authentication code (MAC),
  - encrypts and
  - adds a header.

CSE 486/586

TLS Handshake Protocol

Phase 1: Establish security capabilities
- Cipher suite: a list of cryptographic algorithm supported by the client
  - Establish protocol version, session ID, cipher suite, compression method, exchange random values

Phase 2: Server authentication and key exchange
- Optionally send server certificate and request client certificate
  - Certificate
  - Certificate Request
  - ServerHelloDone

Phase 3: Client authentication and key exchange
- Send client certificate response if requested
  - Certificate
  - Certificate Verify

Phase 4: Finish
- Change cipher suite and finish handshake
  - Change Cipher Spec
  - Finished

CSE 486/586

CSE 486/586 Administrivia

- PA4 due Friday next week
- Final: 5/15 (Friday), 11:45am – 2:45pm
  - NSC 201

Authentication

- Use of cryptography to have two principals verify each others' identities.
- Direct authentication: the server uses a shared secret key to authenticate the client.
- Indirect authentication: a trusted authentication server (third party) authenticates the client.
- The authentication server knows keys of principals and generates temporary shared key (ticket) to an authenticated client. The ticket is used for messages in this session.
  - E.g., Verisign servers

Direct Authentication

- Authentication with a secret key
  - "Nonce" used as a "challenge" random num.

"Optimized" Direct Authentication

- Authentication with a secret key with three messages

CSE 486/586

CSE 486/586

CSE 486/586

CSE 486/586

CSE 486/586

CSE 486/586
Reflection Attack

Needham-Schroeder Authentication

- An authentication server provides secret keys.
  - Every client shares a secret key with the server to encrypt their channels.
- If a client A wants to communicate with another client B,
  - The server sends a key to the client A in two forms.
    - First, in a plain form, so that the client A can use it to encrypt its channel to the client B.
    - Second, in an encrypted form (with the client B’s secret key), so that the client B can know that the key is valid.
  - The client A sends this encrypted key to the client B as well.
- Basis for Kerberos

Kerberos

- Follows Needham-Schroeder closely
- Time values used for nonces
  - To prevent replay attacks
  - To enforce a lifetime for each ticket
- Very popular
  - An Internet standard
  - Default in MS Windows

Nonce $N_A$ in Message 1

Because we need to relate message 2 to message 1

Chuck has stolen $K_B$ and intercepted message 2.

He can masquerade as the authentication system.

Kerberos
Summary

• Digital certificates
  – Binds a public key to its owner
  – Establishes a chain of trust
• TLS
  – Provides an application-transparent way of secure communication
  – Uses digital certificates to verify the origin identity
• Authentication
  – Needham-Schroeder & Kerberos

Acknowledgements

• These slides contain material developed and copyrighted by Indranil Gupta (UIUC), Jennifer Rexford (Princeton) and Michael Freedman (Princeton).