Email Cryptography

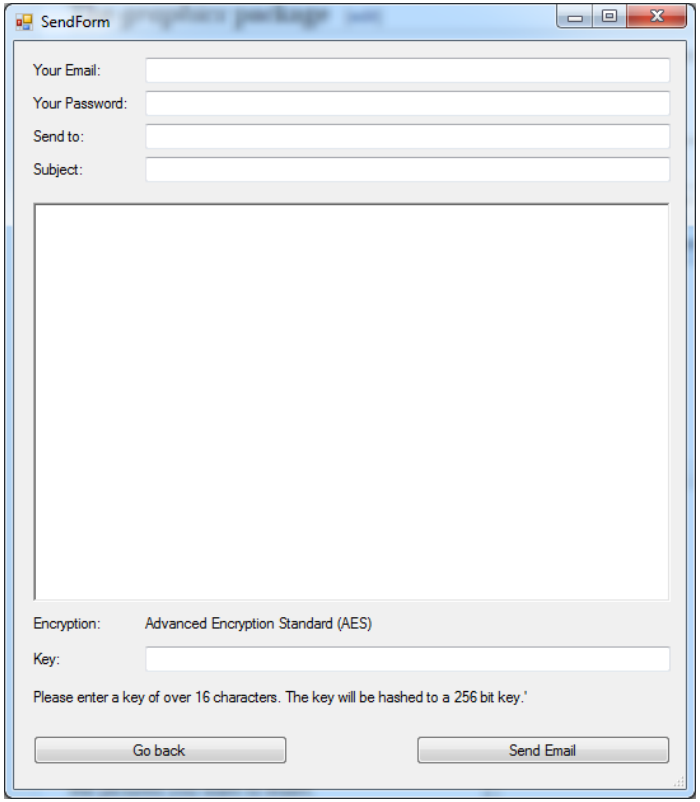
Kong Huang, Kevin Lin

Features

- Securely send encrypted email messages
- Protect messages from various cryptographic and network attacks
- Easy to use user interface

Design

- Form for sending
- Requests user info
- Requires an encryption key of over 16 character length



Design

- Symmetric-key encryption is used for message encryption
- User provided key is hashed and salted using SHA-256
- The resulting 256 bit key is then used in AES-256 encryption algorithm to encrypt the message

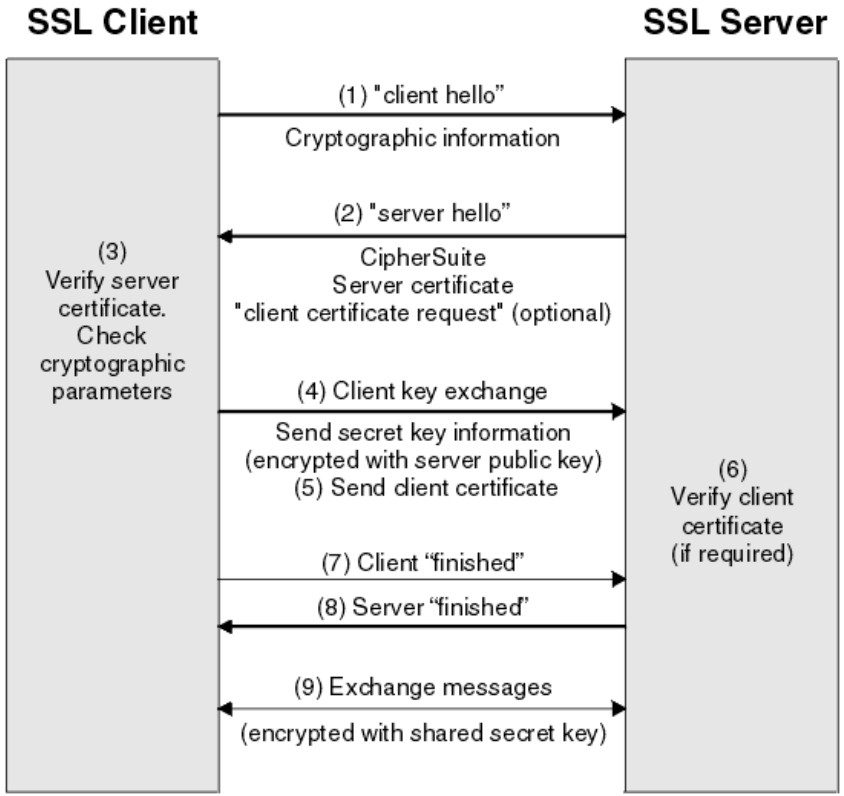
Design

- Email is formatted after encryption to let the other user know they are receiving an encrypted message
- Transmission is handled through TLS

How SSL/TLS works

- Encrypted session uses TLS 1.2, following normal TLS handshake protocol

How SSL/TLS works



Attacks and their defenses

- Data Eavesdropping
  - *How it works:* An attacker intercepts communications between two points mid transit
  - *Our Defense:* TLS encrypts the transmissions so the contained data cannot be eavesdropped
  - However, it does not protect against attacks against the endpoints
    - Ex. bugs in the used TLS stacks, buffer overflows, or bugs in application logic (cross site scripting)

Attacks and their defenses

- Data Modification
  - *How it works:* An attacker modifies data in the packet without the knowledge of the sender or receiver
  - *Our Defense:* Since transmission is encrypted, data cannot be modified without the message becoming invalid
    - Standard TLS protocol uses HMACS (keyed-hash message authentication codes)
    - Attacker needs to know the secret and the message (amongst others) to modify the email (which is impossible given the public key infrastructure in TLS)
    - As such, attacker can only modify the message arbitrarily, causing the server to deem the email invalid

Attacks and their defenses

- Data Replay
  - *How it works:* An attacker maliciously or fraudulently repeats or delays a valid data transmission.
  - *Our Defense:* TLS channel itself is protected against replay attacks using the HMAC in the same fashion as stated in the previous section.
  - In addition, TLS requires the client and server to exchange a nonce in the hello message.
  - The nonce is never repeated in order to prevent the replay attacks.

Attacks and their defenses

- Masquerade Attacks/Identity Spoofing
  - *How it works:* An attacker masquerades as another by falsifying data and gaining an illegitimate advantage.
  - *Our Defense:* TLS authenticates all parties and encrypts all traffic.
  - TLS prevents an attack from performing IP address spoofing on a specific connection (for example, mutual TLS connections)
    - However, an attacker can still spoof the address of the DNS server

Attacks and their defenses

- Man-in-the-Middle Attack
  - *How it works:* An attacker places himself in between a client and server, impersonating both. All traffic passes through this man-in-the-middle, who is able to read and modify any of the data.
  - *Our Defense:* The certificate authority (CA) system is designed to stop this kind of attack.
  - The server uses the private key associated with their certificate to establish a connection (and keeps this key secret)
  - Attacker has to convince a CA to sign their own certificate, and a certificate that is not validated by a known trusted CA will be caught immediately
    - A corrupted CA can still compromise the message. However, our message is encrypted with AES-256 before being sent out, so it is still reasonably secure.

Attacks and their defenses

- Compromised-Key Attack
  - *How it works:* An attacker determines the key, and uses the key to decrypt encrypted data without the knowledge of the sender of the data
  - *Our Defense:* Depending on the key, the message is still secure based on several factors.
  - AES encryption scheme key gets compromised
    - Security relies on the recipient's email service as the attacker requires access to the encrypted message
  - Shared secret key used in the TLS is compromised
    - Nothing can be determined in reasonable time as message will be encrypted with solely an AES scheme or with an AES scheme and the scheme chosen through the TLS protocol
  - If both keys are compromised, the attacker could intercept the encrypted message as it is being sent and decrypt it twice

Questions?