PROTECTING CONVERSATIONS

Basics of Encrypted Network Communications

Naïve Conversations

* Captured messages could be read by anyone
* Cannot be sure who sent the message you are reading

Basic Definitions

* Authentication — Act of confirming the integrity of a message and the identity of the person who sent it
* Encryption — Process of encoding messages so that eavesdroppers cannot read it, but authorized parties can

Early Attempts at Protection

- Wax seals authenticated a message
- Caesar ciphers encrypted the contents of the message
  - “the quick fox” becomes “WKH TXLFN IRA”

More Advanced Protection

- WWII German Enigma machine produced “uncrackable” ciphers
- Signatures or watermarks, combined with shared secrets, give confidence in the identity of the sender

A Step Backwards

* Early networked computers seemed to forget the lessons of the past
  * Underpowered
  * Mainly for research purposes

Cryptography to the Rescue

* Symmetric Ciphers
* Asymmetric Ciphers
* Cryptographic Hashes

Symmetric Ciphers

* Single key is used for both encryption and decryption
* Key is a shared secret between the two parties
* Generally speedy
  * Popular algorithms are moved into hardware for more speed
* 3DES and AES are common (AES is preferable)

Asymmetric Ciphers

* Two separate, mathematically-linked, keys for encryption and decryption
    * One is secret, the other is public
* Anyone can encrypt using the public key; only secret (private) key can decrypt
* Typically slower than symmetric ciphers
* RSA and ECC are common

Cryptographic Hashes

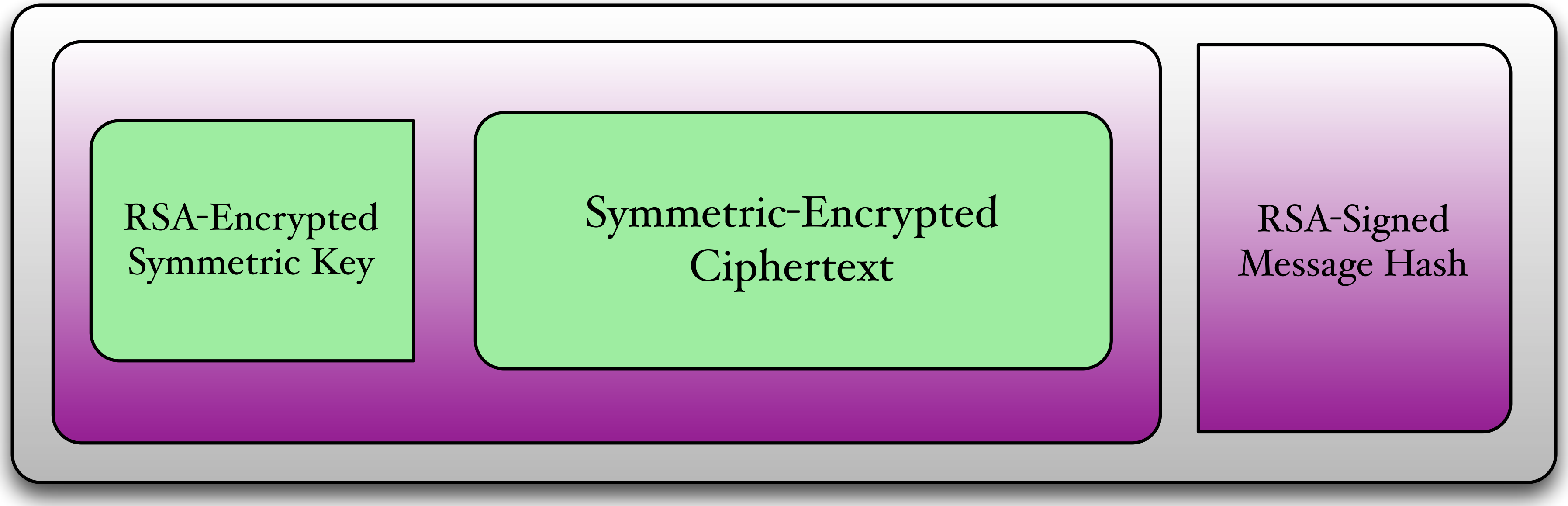
* Algorithm that takes an arbitrarily-long block of data and returns a fixed-sized bit string
* Designed such that changes in the data will very likely change the hash
* Used with symmetric and asymmetric ciphers to produce HMAC (Hash-based Message Authentication Code)
    * HMAC protect message integrity and authenticity
* MD5, SHA-1, and SHA-256 are common

Pre-shared Keys

* Prevents captured traffic from being deciphered
* Anyone who could read message could have sent it
* Time consuming to set up
    * Keys often reused

Public Key Encryption

* Packets are limited to the size of the key pair
  * Due to padding, 1024-bit RSA key yields a maximum message size of about 111 bytes (instead of the expected 128 bytes)
* Arbitrary message lengths would likely require multiple RSA ciphers per message
* Signing messages with the key pairs gives authenticity to the messages



GPG Model of Encryption

Random symmetric keys protected by Public Key Crypto

Diffie-Hellman Key Exchange

* Two parties without knowledge of each other can jointly establish a shared secret key over an insecure channel
* No authentication is provided — key exchange is anonymous
* Discrete logarithm problem provides security
  * Best known algorithms cannot retrieve secret data

Diffie-Hellman Key Exchange

Alice				Bob		
Secret	Public	Calc.	Send	Calc.	Public	Secret
a	p, g		p,g »			b
a	p, g, A	g^a mod p = A	A »		p, g	b
a	p, g, A		« B	g^b mod p = B	p, g, A, B	b
a, **s**	p, g, A, B	B^a mod p = s		A^b mod p = s	p, g, A, B	b, **s**

Diffie-Hellman Key Exchange

* B^a mod p = A^b mod p
* (g^b)^a mod p = (g^a)^b mod p
* Computationally hard to figure out large secret exponent from the public data

Station to Station Protocol

- Adds authentication to Diffie-Hellman Key Exchange
- Basic Protocol:
  - Alice » Bob : g, p, A
  - Alice « Bob : B, Cert_B, E_s(S_B(B, A))
  - Alice » Bob : Cert_A, E_s(S_A(A, B))
- Encrypted signatures can be verified by the certificates

Enhancing Basic Protection

* Protocol like Station to Station generates a symmetric cipher between known hosts
    * Can be used to securely transmit data between hosts
* Still vulnerable to several attacks
    * Replay attacks
    * Data modification
    * Side-channel attacks

Replay Attacks

* Attacker does not know the contents of the message, but can see it effects
* Attacker intercepts messages and replays them in the future to replicate the observed effects
* Example: if a message seen to cause a missile to fire, can replaying cause more missiles to fire?
* Sequence numbered messages allow the receiver to track received messages

Data Modification

* Corrupting messages can cause issues in poorly written software
* Desirable to prevent message modification
* HMAC of encrypted message contents
    * Hash of the contents of the encrypted message
    * Signed by the message sender

Side-Channel Attacks

* Attack based on information gained from the implementation of the crypto-system, rather than brute force of weakness of the algorithms
* Message length analysis could be one form of side-channel attack
* Encrypted messages can be padded to random lengths to hide the real length of the plaintext

Encrypted Protocols Insufficient

- Only protects data in transit
- Example: Email communication
  - Encrypted session to SMTP server
  - Encrypted session to IMAP/POP3 server
  - No guarantees about security between SMTP servers
  - No guarantees about storage of messages on intermediate servers (caching, store-and-forward)
- Solution: Use GPG to protect data end-to-end

Summary

* Authentication and Encryption secure the transmission of messages between two parties
    * Prevents attackers from reading them and ensures the sender identity
* Simply providing encryption is not enough to secure messages
* Need to think about data at rest as well as data in transit

QUESTIONS?