

PKI, Encryption, Certificates and You

Patrick Gallagher

- Worn a lot of hats
- Development and IT
- Engineering and consulting
- Apple IT training workbooks
- Security and Mobility



Why Focus on These Technologies?

- Bad actors
 - Governmental
 - Non-Governmental
- Protect our Data
 - At Rest
 - In Transit
 - In Use*

Agenda

- Definitions
- Symmetric Encryption
- Asymmetric Encryption
- PKI
- Assorted other things

Definitions

Cryptography

- Techniques, technologies, and protocols to secure data in the presence of bad actors
- Also cryptology

Encryption

- Encoding data so that adversaries cannot read them
- Also encipherment

Symmetric Encryption

Symmetric Encryption



Symmetric Encryption



Examples

- Advanced Encryption Standard (AES)
- Message Authentication Codes (MAC)
- Wi-Fi



Pros and Cons

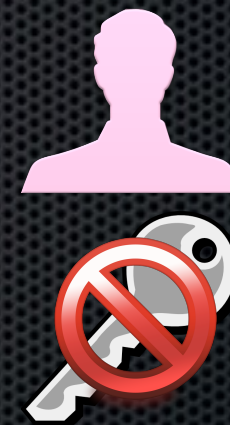
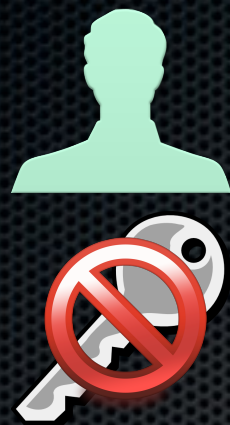
- + Fairly easy math
- + Fast
- - Key distribution



Key Distribution



Key Distribution



Asymmetric Encryption

Asymmetric Encryption



Public Key



Private Key



Private Key



Public Key

Examples



- PGP/GPG
- Some parts of SSL/TLS
- Digital Signatures
- S/MIME

Pros and Cons



- + Flexible usage
- + Solves key distribution problem
- - Complex math
- - Slow
- - Trust problem

Trust Problem



- How do you trust that the public key you have came from who you think it did?
- Is the person/entity who they claim to be?
- Web of Trust (PGP)
- Public Key Infrastructure

PKI

What is PKI?

- Manage trust by delegation
- Technical and human
- X.509 ITU-T standard
- Public and private
- Manage certificates



PKI Parts

- Servers
- Services
- People
- Policies
- Procedures
- Many...



Relevant PKI Parts

- Certificates
- Certificate Signing Requests (CSRs)
- Certificate Authorities (CAs)
- Intermediate CAs
- Trusted roots/X.509 anchors



Certificate

- Public key
- Identity information
- Extensions
- Signed by a CA*



Certificate Signing Request

- Certificate
- No private key
- Sent to CA



Certificate Authority

- Signs certificates
- Indicates their trust in you
- “Are you who you say you are?”
- “Are you trustworthy?”
- Add identity and extensions



Certificate Authority

- Public/private key pair
- Signs certificates with its private key
- Signature verified with its public key
- Keys to the kingdom



Intermediate CA

- Delegate signing authority
- “Chain up” to a Root CA
- Control risk



Trusted Roots

- Well-known CAs and Intermediates
- Distributed with OS or browser
- You will trust any cert that chains up to one of your trusted roots*
- Told who to trust



Ending Trust

- Remove the root
- Revoke a certificate
- Certificate Revocation List (CRL)
- Online Certificate Status Protocol (OCSP)



How Certificates Work



Assorted Other Things

- SSL/TLS & key exchange
- Hashes
- Message Authentication
- Digital Signatures
- Codesigning
- When things go wrong...

SSL/TLS

- Secure Sockets Layer (old)
- Transport Layer Security (new)
- Do you trust the identity of the server?
- Asymmetric cryptography (slow math)
- Secure key exchange
- Symmetric cryptography (fast math)

Hashes

- Confirm the integrity of a message
- (Content didn't change)
- Easy math
- One way
- Modify message, modify hash
- No collisions
- MD5, SHA-0, SHA-1, SHA-2, etc.

Message Authentication Codes

- Symmetric keys
- Confirm integrity
- Confirm authenticity



Digital Signature



- Confirm integrity
- Confirm authenticity
- Non-repudiation (proof of sender to third party)
- Asymmetric keys
- S/MIME

Codesigning



- Similar to digital signature
- Developer seals assets using their private key
- OS can detect changes to sealed assets
- Prevent execution
- Gatekeeper

When Things Go Wrong...

goto fail;



goto fail;

- Simple programming error
- Client-side problem
- Short cut certificate validation
- Enabled Man In The Middle attack
- Always run the latest software
- <http://gotofail.com/>

Heartbleed

- Programming error
- Server-side problem
- OpenSSL 1.0.1 versions



Heartbleed

- Unchecked parameter
- Exposes server memory
- Undetectable exploit



Heartbleed

- Patch OpenSSL on servers
- Revoke and replace certificates
- Change passwords
- <http://heartbleed.com/>
- <http://xkcd.com/1354/>



The Good News

- Both are attacks against *implementations*
- Not attacks against crypto or protocol
- Inconvenient but tractable solutions

Agenda

- Definitions
- Symmetric Encryption
- Asymmetric Encryption
- PKI
- Assorted other things

Questions?



If there is time...

Patrick Gallagher

patrick@digitalpeaks.com