

Security of Apple iMessage

Daniel Belcher, Matt Gautreau, Chris LaRose,
Taylor Siebenberg

University of Arizona

May 5, 2014

Introduction

Cryptographic
Hardware

ECDSA

TLS/SSL

MITM

Introduction

Apple iMessage
Encryption

Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg

- ▶ Start: Your iPhone
- ▶ Apple Push Notification Service
- ▶ Transport Layer Security
- ▶ AES Session Key and Message Encryption
- ▶ RSA and ECDSA
- ▶ End: Push and Decrypt

Introduction

Cryptographic
Hardware

ECDSA

TLS/SSL

MITM

AES Co-processor

Apple iMessage
Encryption

Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg



Introduction

Cryptographic
Hardware

ECDSA

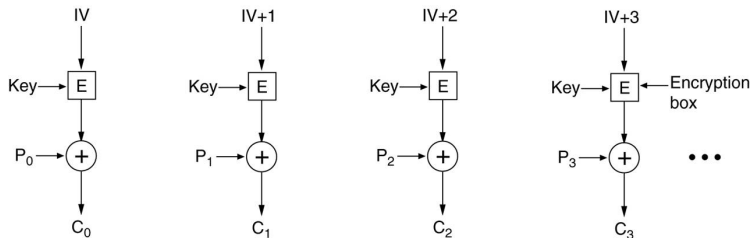
TLS/SSL

MITM

Random Number Generator

Apple iMessage
Encryption

Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg



Introduction

Cryptographic
Hardware

ECDSA

TLS/SSL

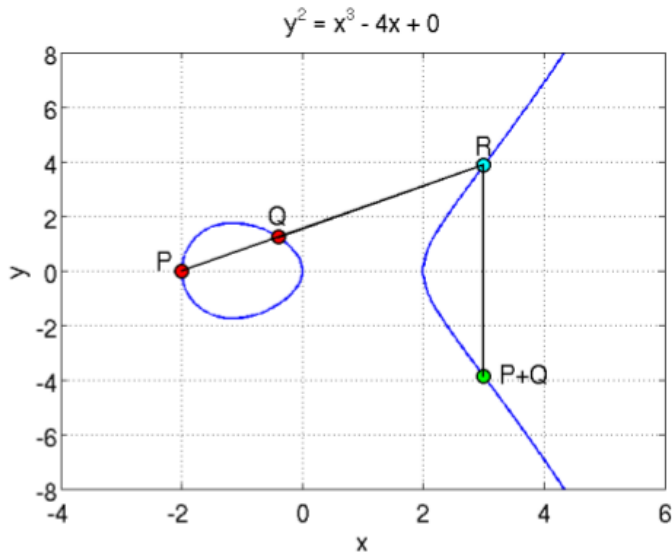
MITM

- ▶ Counter Mode Deterministic Random Byte Generator (CTR_DRBG)
- ▶ National Institute of Standards and Technology Special Publication (NIST SP 800-90A)

Elliptic Curves

Apple iMessage
Encryption

Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg



Introduction

Cryptographic
Hardware

ECDSA

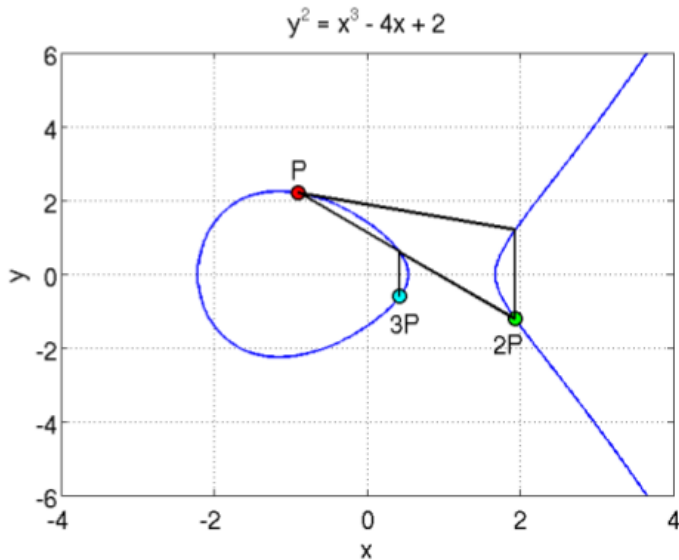
TLS/SSL

MITM

Elliptic Curves

Apple iMessage
Encryption

Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg



Introduction

Cryptographic
Hardware

ECDSA

TLS/SSL

MITM

Transport Layer Security / Secure Socket Layer

Apple iMessage
Encryption

Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg

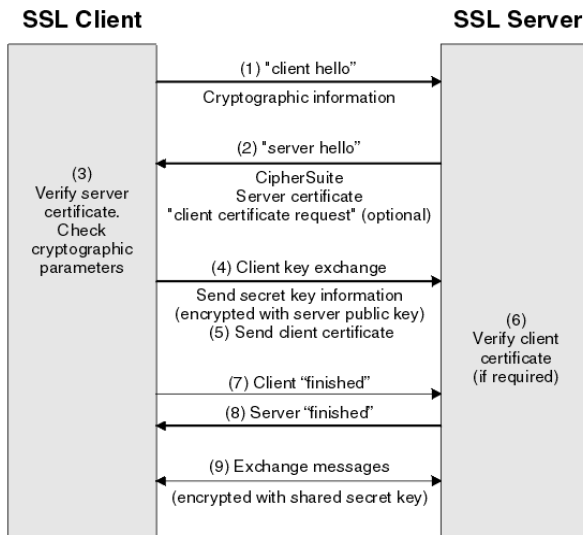
Introduction

Cryptographic
Hardware

ECDSA

TLS/SSL

MITM

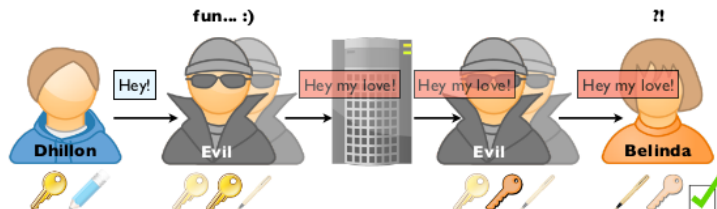


► $\text{MD5}(s_{pm} || \text{SHA-1}(A || s_{pm} || r_C || r_S))$

Two-sided Man-in-the-Middle Attack

Apple iMessage
Encryption


Daniel Belcher,
Matt Gautreau,
Chris LaRose,
Taylor Siebenberg




Evil presented his key to Dhillon instead of Belinda's.

Evil presented his key to Belinda instead of Dhillon's.


He can read and forge Dhillon's messages without any of his private keys.

 Dhillon's ECDSA (priv)

 Dhillon's ECDSA (pub)

 Evil's RSA (priv)

 Evil's RSA (pub)

 Evil's ECDSA (priv)

 Evil's ECDSA (pub)

 Belinda's RSA (priv)

 Belinda's RSA (pub)

Introduction

Cryptographic
Hardware

ECDSA

TLS/SSL

MITM