iOS Interprocess Communication Security and the Universal Authentication Framework Protocol

Nok Nok LABS

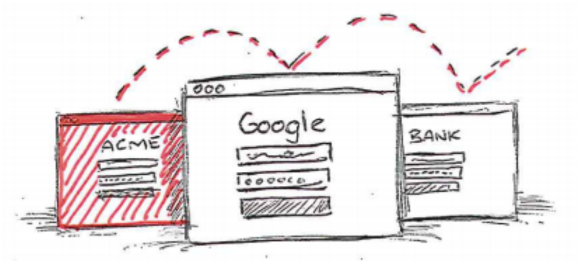
Dr. William Blanke
Mobile Lead Architect
Nok Nok Labs

Agenda

- Introduction to the Universal Authentication Protocol (UAF)
- Android Demo
- Creating a UAF Client for iOS
- Security Threat Analysis and Resolutions
- Q & A

UAF: Why Do I Care?

Passwords are a barrier to delivering secure online services



REUSED

PHISHED

KEYLOGGED

UAF: Why Do I Care?

Options to strengthen password security are problematic

SMS USABILITY

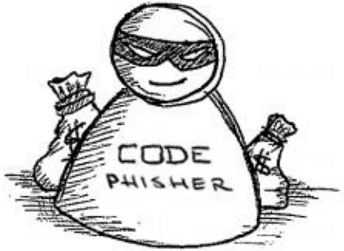
Coverage | Delay | Cost

DEVICE USABILITY

One per site | $$ | Fragile

USER EXPERIENCE

User find it hard



STILL PHISHABLE

Known attacks today

We need a new approach for strong, simple authentication fido™ alliance

Microsoft

PayPal™

Google

infineon

MasterCard

SAMSUNG

lenovo. FOR THOSE WHO DO.

Nok Nok LABS

DISCOVER®

VISA

Ping Identity®

Bank of America

BlackBerry

ARM®

LG Electronics

RSA SECURITY™

SafeNet. THE DATA PROTECTION COMPANY

Synaptics®

GO-Trust Trust in a Mobile World

oberthur TECHNOLOGIES THE M COMPANY

AGNITiO Voice ID

NXP

MedImpact Healthcare Systems

AUTHENTIFY®

SECURE KEY

IdentityX®

Entersekt

FINGERPRINTS

yubico Trust the Net.

QUALCOMM®

CrucialTec

Goldman Sachs

ARXAN Protecting the App Economy™

E*TRADE

ca technologies

FORGEROCK

natural security

IT'S ME!

Giesecke & Devrient Creating Confidence.

VASCO®

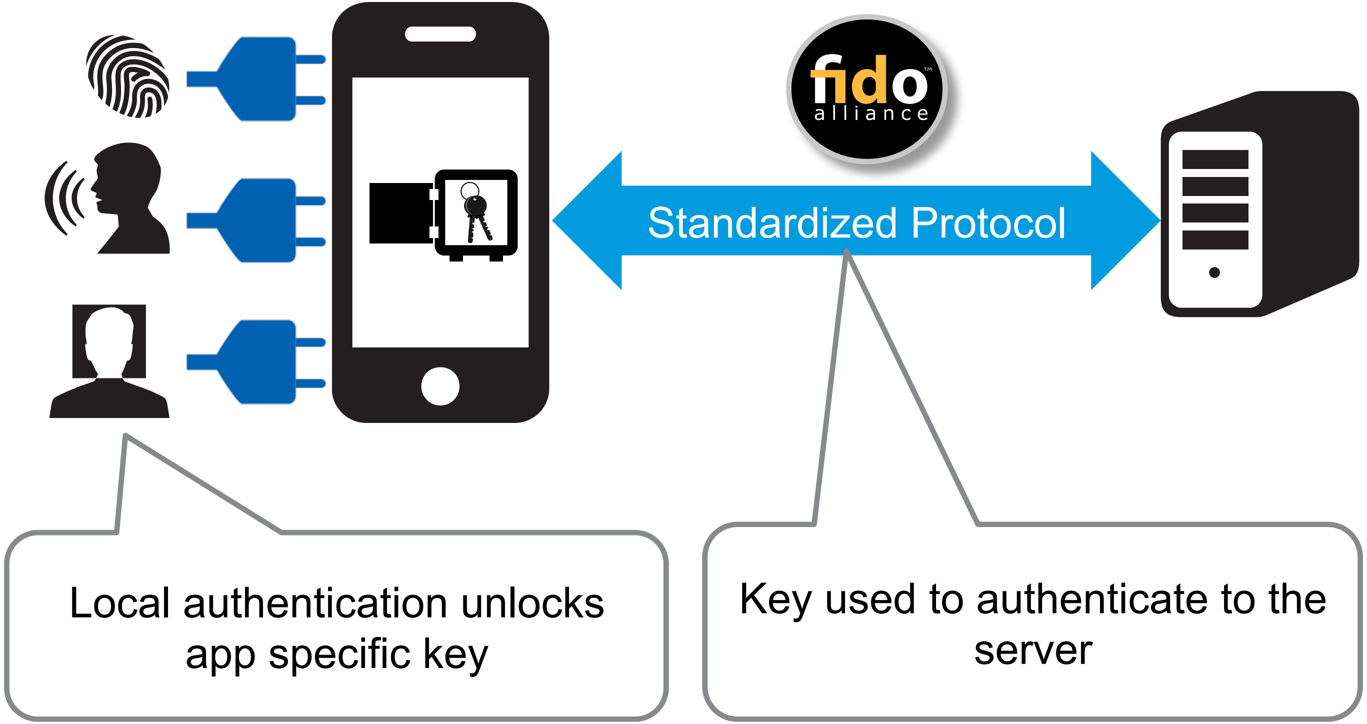
Alibaba Group

gemalto security to be free

YAHOO! JAPAN

About the FIDO UAF Protocol

Insulating your app from device authentication capabilities



Local authentication unlocks app specific key

Key used to authenticate to the server

Benefits of FIDO UAF Approach

Simpler Usability

- Simpler, quicker authentication methods
- Users' existing devices

Stronger Security

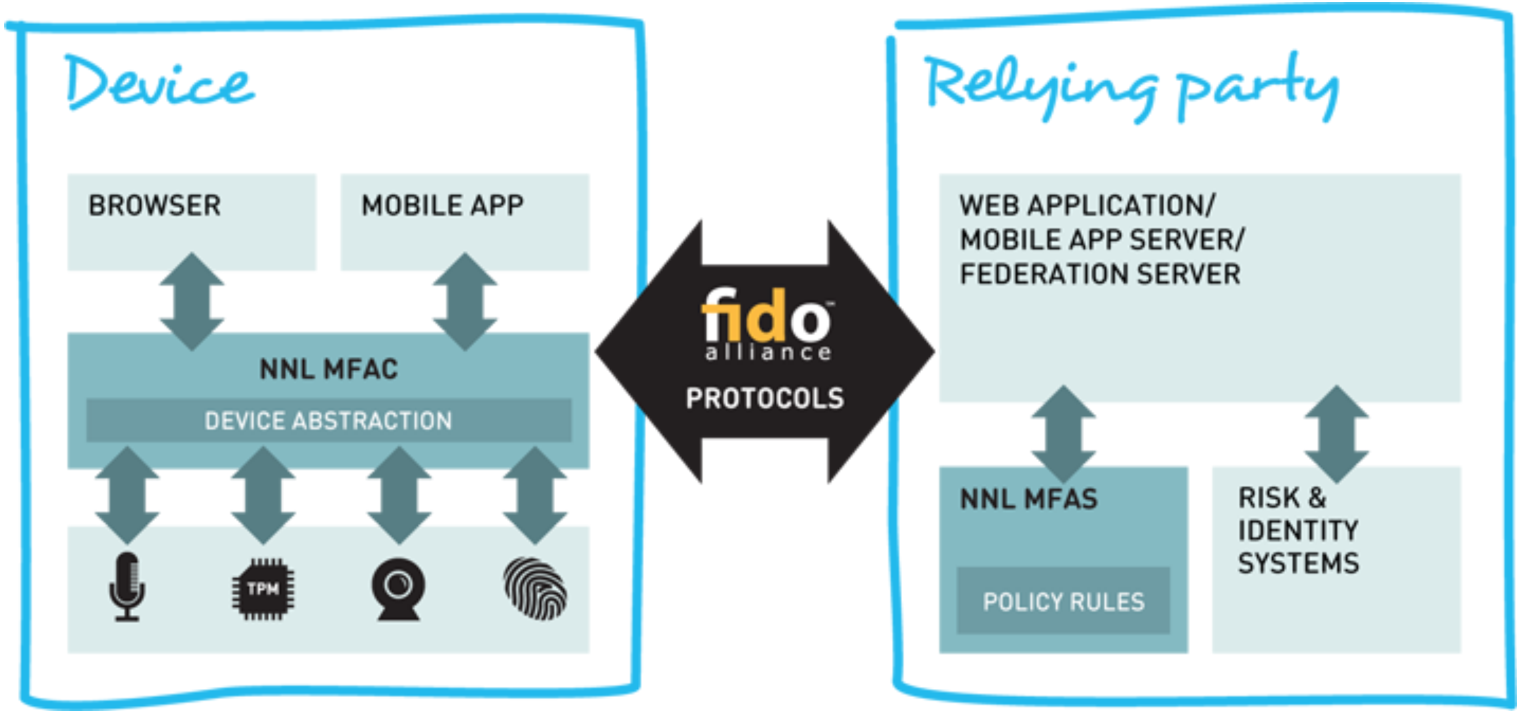
- Public Key Cryptography
- Risk appropriate
- Leverage secure hardware, if available

Reduced Complexity

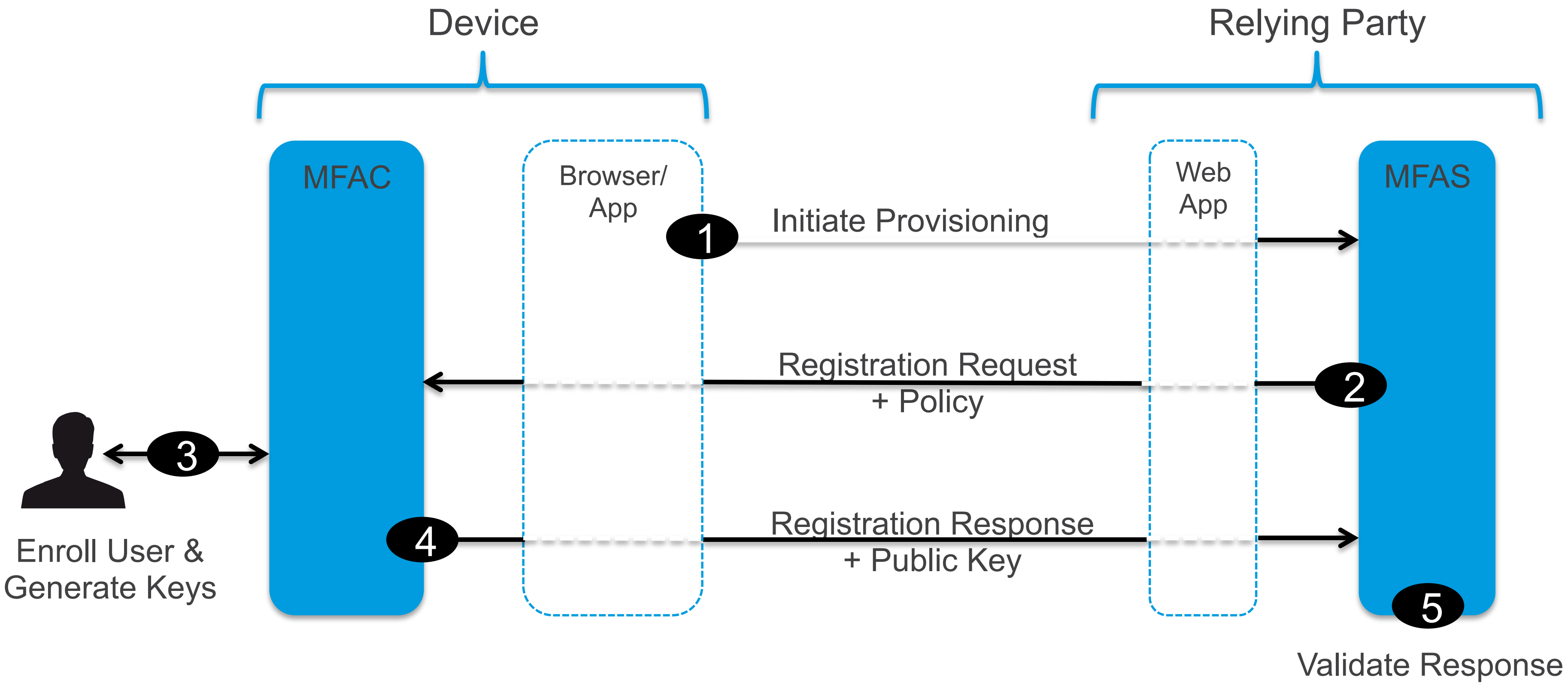
- Unified & flexible infrastructure
- Reduced support
- Future-proof

FIDO Ready™ Architecture

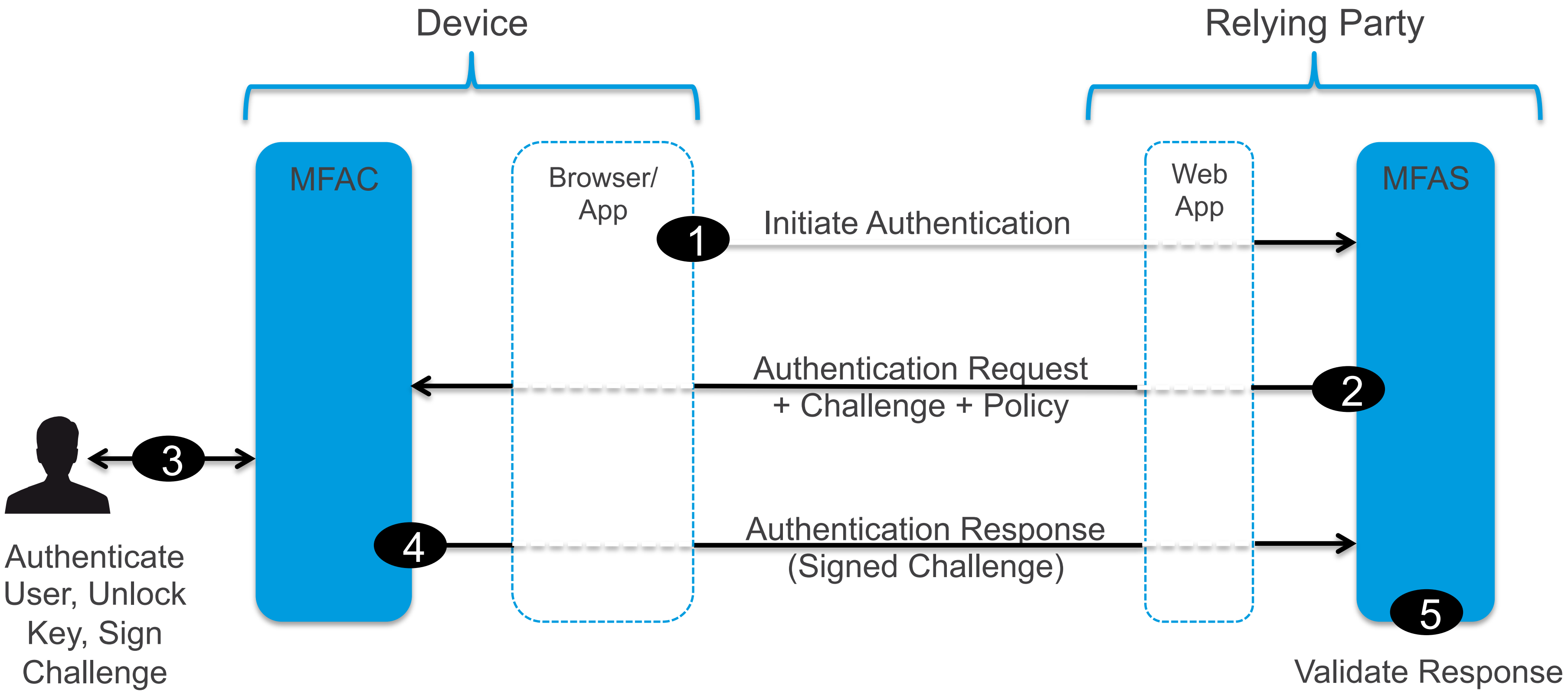
On Samsung Android devices



FIDO Ready™ Registration Flow



FIDO Ready™ Authentication Flow


Device
Relying Party
MFAC
Browser/ App
Web App
MFAS
1
Initiate Authentication
Authentication Request + Challenge + Policy
2
3
Authenticate User, Unlock Key, Sign Challenge
4
Authentication Response (Signed Challenge)
5
Validate Response

Android UAF Demo

Using Samsung Note 4 with PayPal

iOS UAF Client

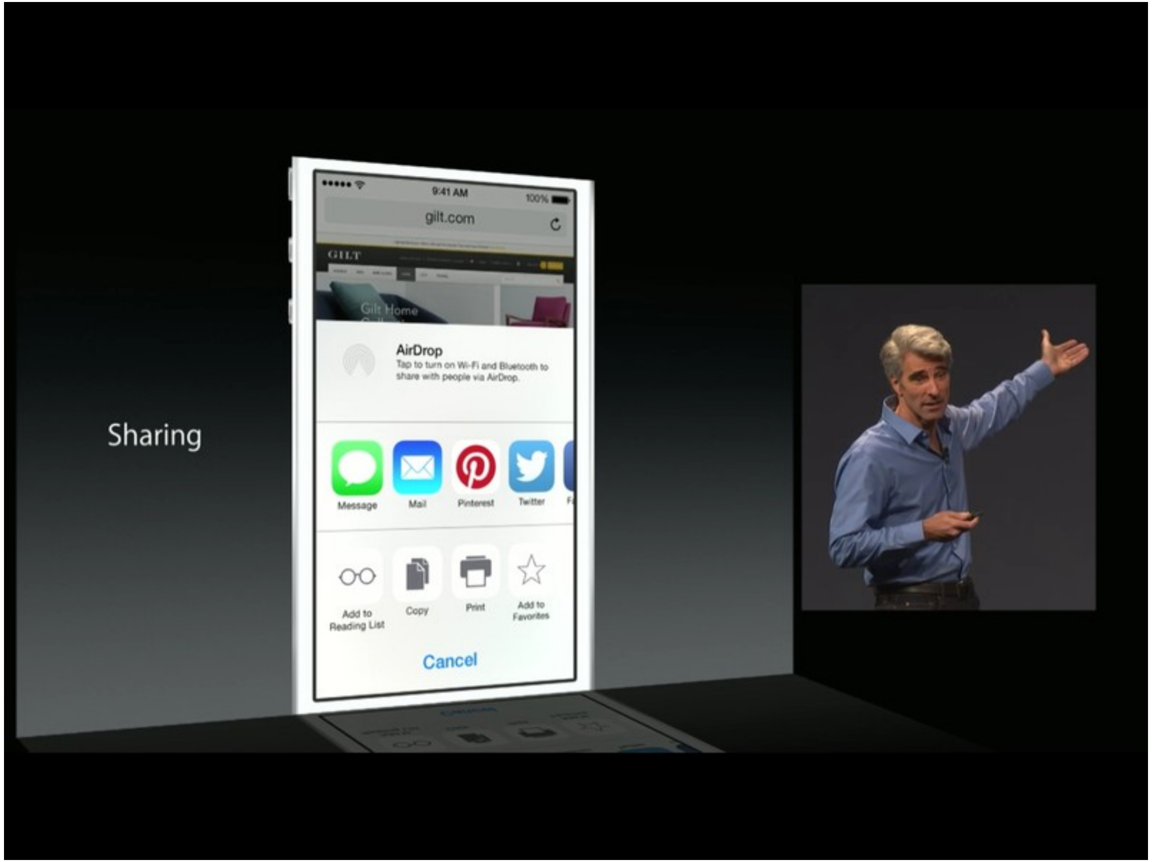
Standalone would be nice, but iOS is a singletasking OS…

iOS IPC Requirements

- Identify the calling replying party app to the UAF client via the iOS operating system.
- Allow transition to another app without user intervention.

iOS 8 Extensions

- User must initiate action
- No way to identify calling app



iOS Custom URL Schemes

- App can initiate IPC without user intervention
- App can identify caller

```
- (BOOL) application: (UIApplication *) application
    openURL: (NSURL *) url
    sourceApplication: (NSString *) sourceApplication
    annotation: (id) annotation
```

x-callback-url

- Two apps each with custom URL schemes
- Bidirectional IPC!

- De facto standard
- But is it secure?

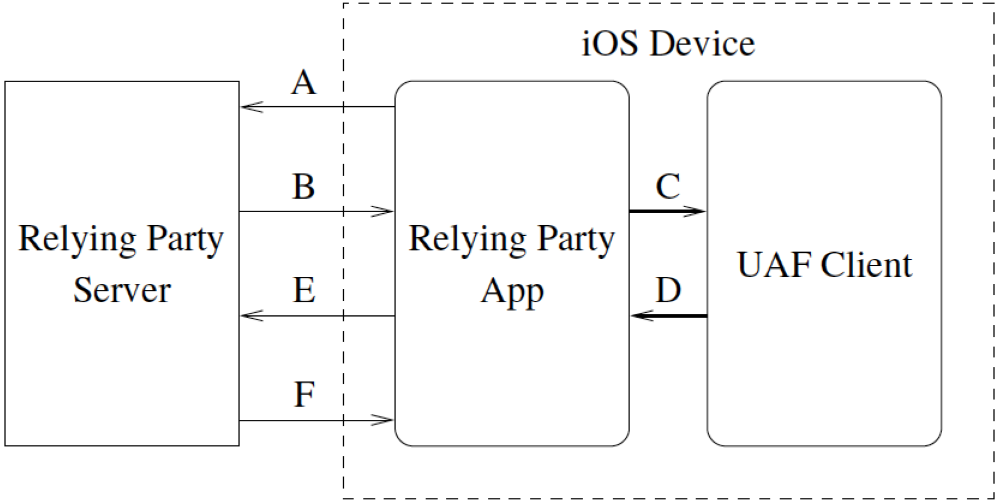
Threats and Resolutions

Note: If more than one third-party app registers to handle the same URL scheme, there is currently no process for determining which app will be given that scheme.

App Programming Guide for iOS

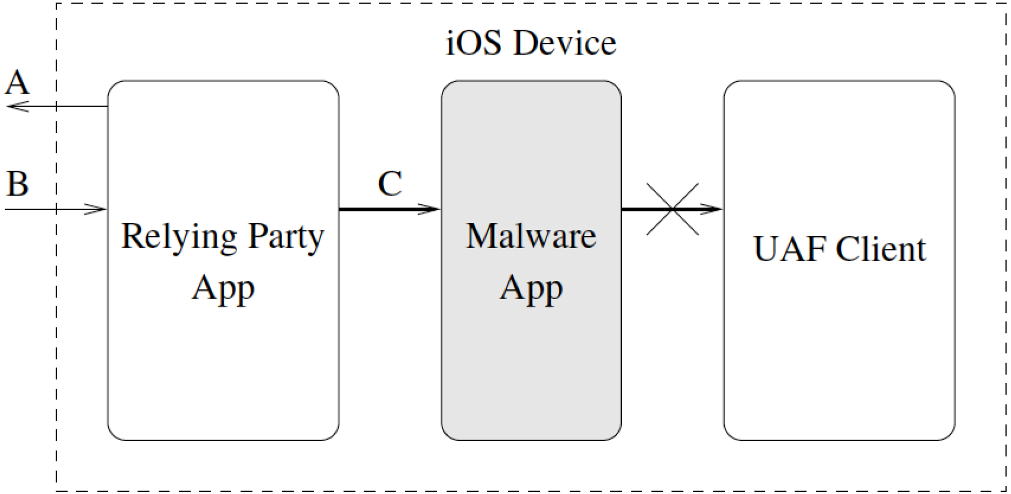
Normal UAF Exchange

- AB
  - Get request from server
- CD
  - Custom URL scheme
- EF
  - Post response to server



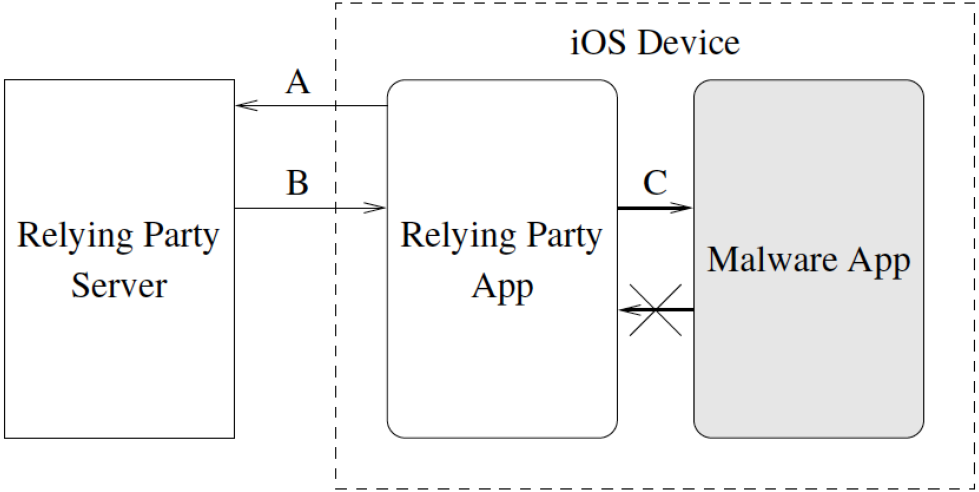
Man in the Middle

- Malware registers UAF Client custom URL scheme
  - Flip/flop required
    - Who knows?
  - UAF client detects Bundle ID
    - Matched with HTTPS whitelist



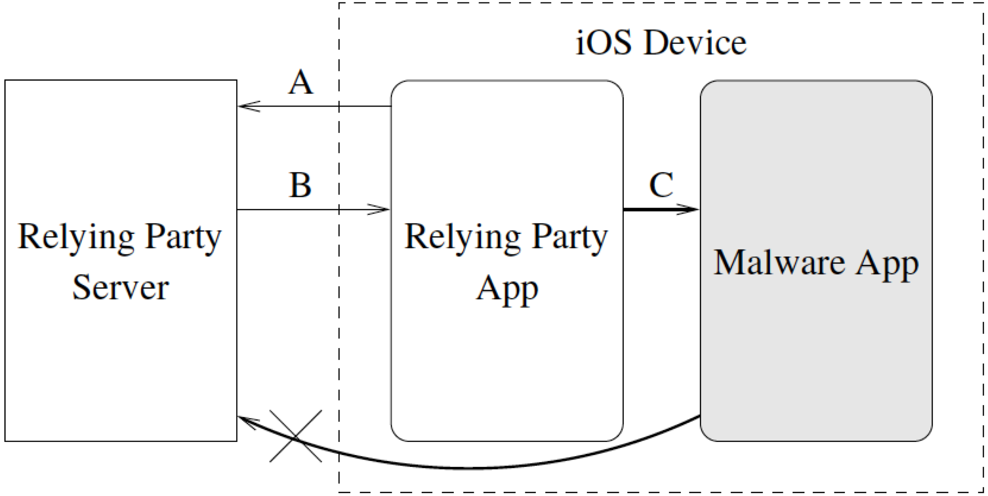
UAF Client URL Spoof

- Malware processes the request itself
  - RP app detects Bundle ID



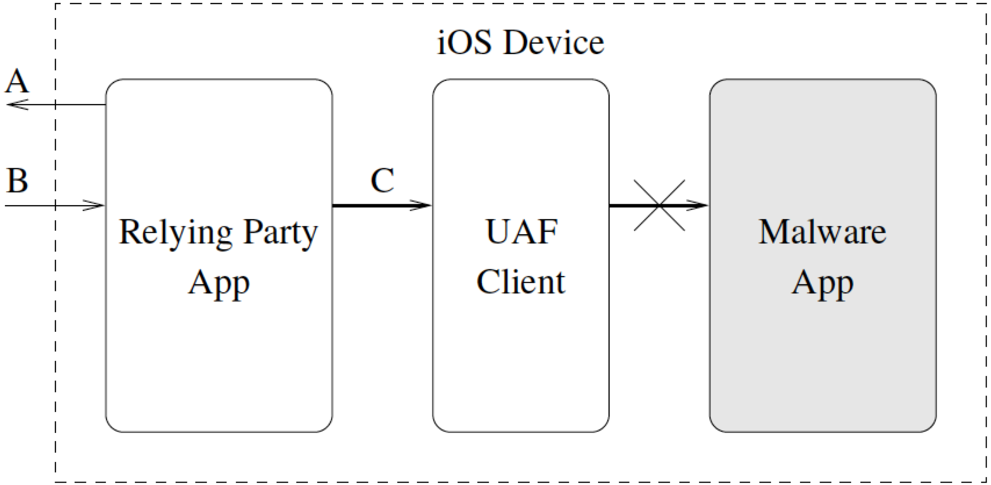
URL Client URL Spoof with Post to Server

- Malware posts response directly to server
  - Can’t register
  - No server session



Relying Party App URL Spoof

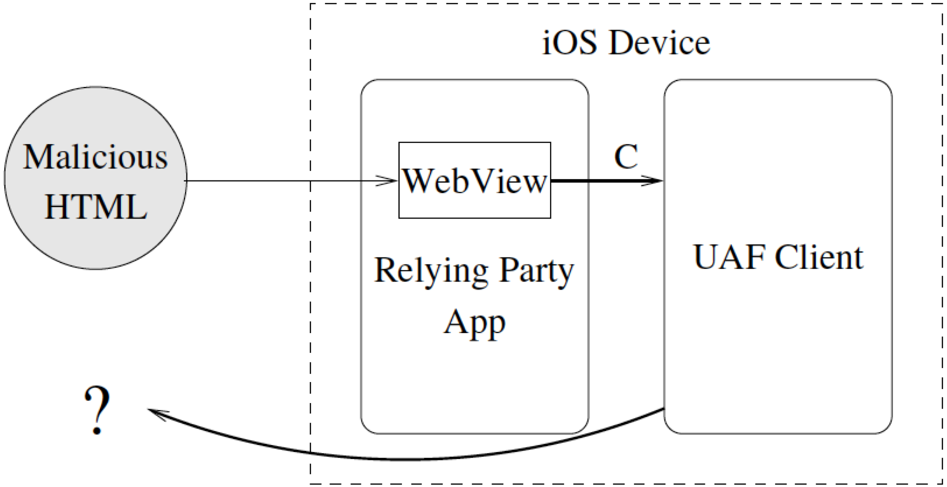
- Malware registers RP App custom URL
  - Symmetric key generated for every request
    - Malware can't obtain this



Embedded WebView

- Malicious outside content
  - eg chat messages

- Always scan external content



Compromised Devices

- Jailbroken devices
  - OS rooted
- Masque Attack
  - Enterprise apps

- Bundle IDs no longer trustworthy

- Hardware protection
  - iOS Secure Enclave based TouchID KeyChain API

For More Information

FIDO (Fast ID Online) Alliance

- FIDO Universal Authentication Framework (UAF) specifications
- http://fidoalliance.org/

Nok Nok Labs

- https://www.noknok.com

Q&A

and **THANK YOU** for your time.

William Blanke
bblanke@noknok.com