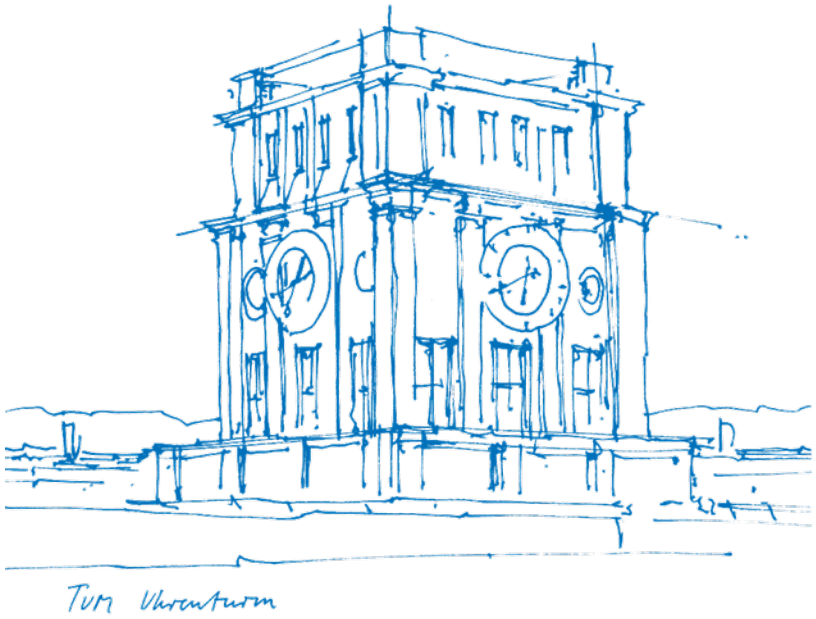
Chair of Network Architectures and Services
TUM Department of Informatics
Technical University of Munich (TUM)

Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication

Matthias Wachs, Quirin Scheitle, and Georg Carle

ANRW'18, Montreal, July 16, 2018
Originally published at TMA'17, Dublin, June 2017



TLS 1.2 handshake does not encrypt certificates

Known for a long time, and thankfully fixed in TLS1.3

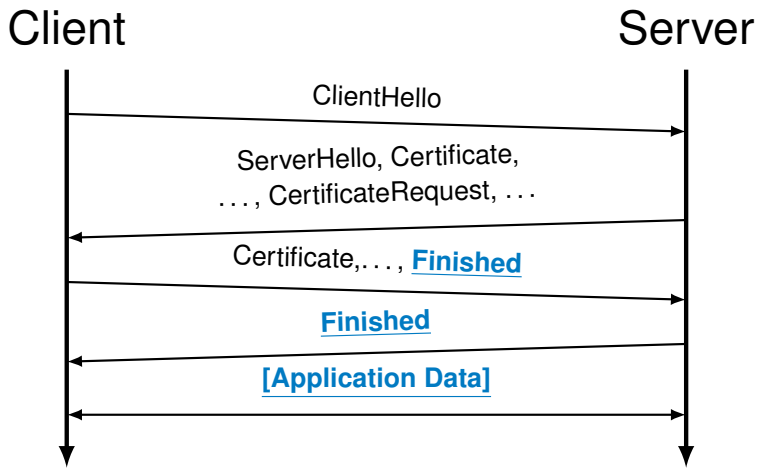


Figure: TLS 1.2 handshake, Unencrypted Data, **[Encrypted Data]**

Server Certificates

- Eavesdroppers can learn the specific websites that a user visits (not just the server's IP address)

Client Certificates

- Used by VPNs, governments, . . .
- Person names, company names, . . . $\rightarrow$ private data!

TLS 1.2 Client Certificate Authentication (CCA)

Where is CCA being used?

- **Network authentication**: 802.1x EAP
- **VPN**: OpenVPN, F5 EdgeConnect, . . .
- **Web**: HTTPS
- **IoT**: MQTT
- **Remote device management,** for example MobileIron
- **Apple Push Notification Service (APNs)**

Apple Statistics:

- 1 billion active devices (2016)
- 800 million iTunes accounts (2014)

Push Notification Services

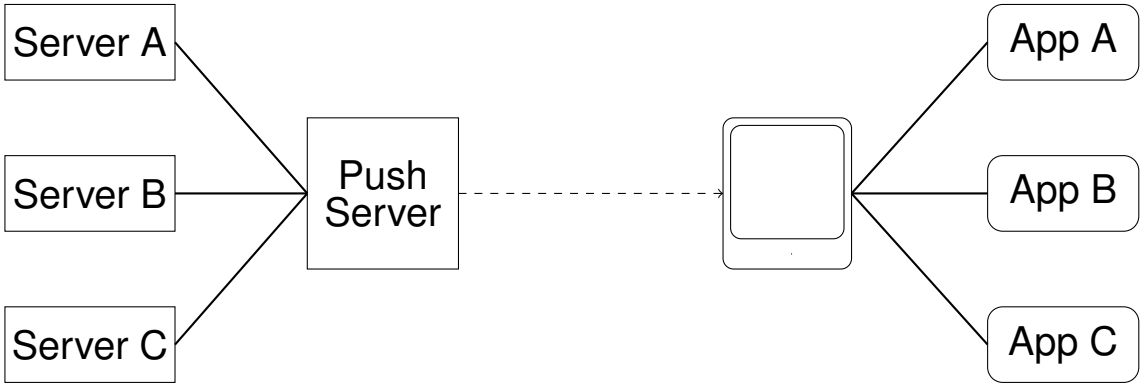


Figure: Push Service Architecture: Messages brokered to Apps through the Push Notification Service.

Resource efficient notification of (mobile) applications:

- **Apple's APNs:** iOS, MacOs, iTunes, watchOS, tvOS, ...
- **Google's FCM:** Android, Chrome
- **Microsoft's WNS:** Windows, Windows Phone

Paradigms:

- *Tightly integrated with operating system*
- *Always connected to backend*

Apple Push Notification Service (APNs)

APNs integral part of iOS and macOS – “always on”
APNs uses Client Certificates for login:

- Generated at device setup
- Unique cryptographic material (CN, public key, fingerprint)

```
Serial Number: ab:12:34:56:78:9a:bc:de:f0:12
Issuer: C=US, O=Apple Inc., OU=Apple iPhone, CN=Apple iPhone Device CA
Validity Not Before: Apr  8 12:34:56 2015 GMT
Validity Not After : Apr  8 12:34:56 2016 GMT
Subject: CN=12345678-1234-1234-1234-123456789ABC
Key ...
(all data redacted)
```

Precise User[1] Tracking in APNs

Several appearances of same device easily linkable

2 of 4 Attacker Types Considered in this Work

- ~~Apple or someone infiltrating Apple: better means available~~
- ~~Local adversary: Can use MAC addresses and more~~
- Regional adversary: Access to one or several large networks
- Global adversary: Access to several core networks

Regional Adversary – Validation at Internet Uplink

- Can a regional adversary track users?

Global Adversary – Validation through Global Path Measurements

- How well can a global adversary leverage APNs to track users?

1: APNs CCA certificates are bound to devices. However, these devices are typically private and carried by a user at most times, which allows inferences into user tracking.

Passive Capturing

Methodology

Analysis of $>$ 2 weeks of TLS CCA traffic at Internet uplink

Regulations by IRB:

- Documented measurement process
- Isolated measurement infrastructure
- Access only for permitted staff
- Raw data must not leave infrastructure

Our self-restrictions:

- No attempt to identify users
- No publication of identifiable data

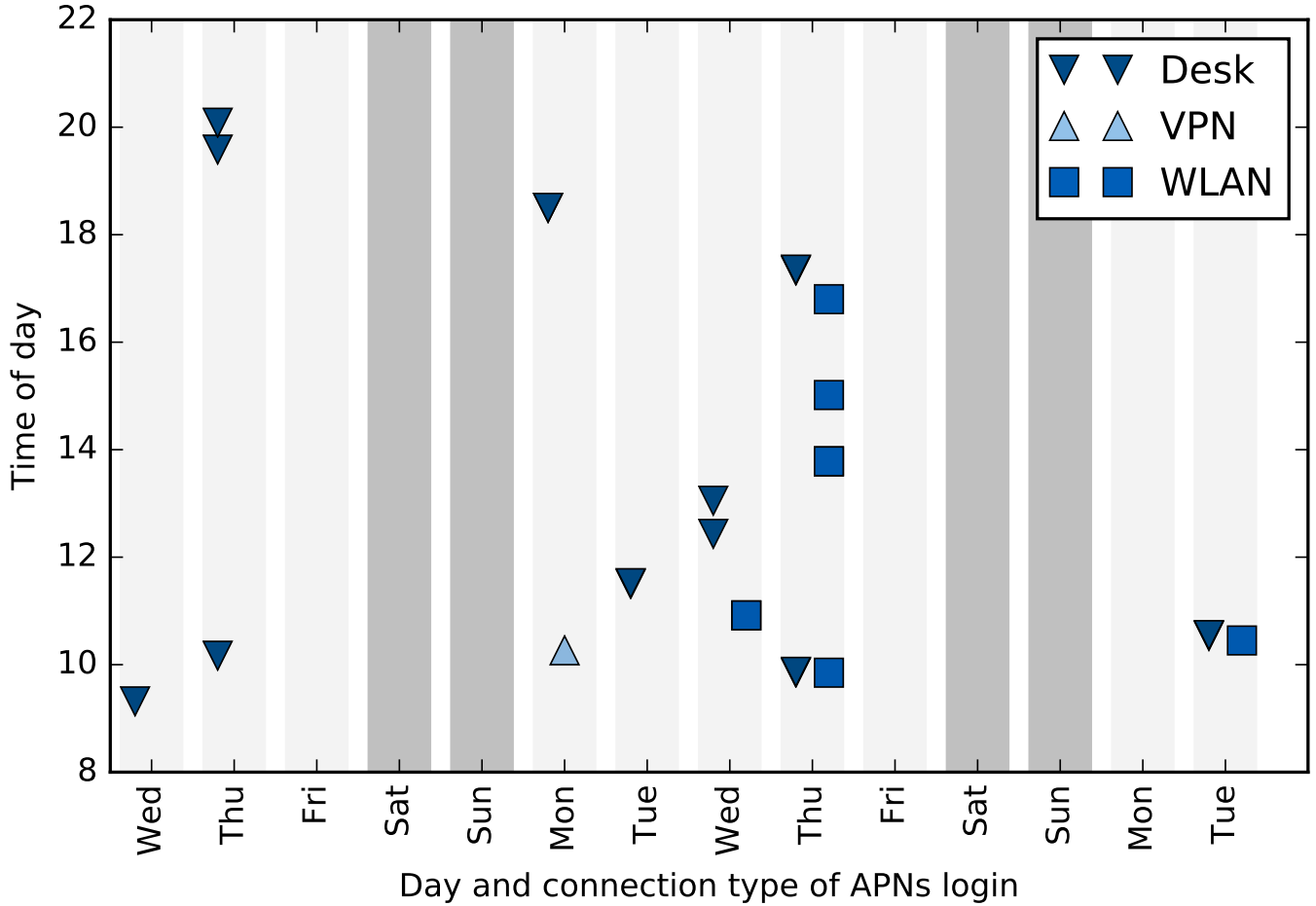
APNs by far the biggest user of CCA

#Certs	Issuer Distinguished Name
56128	/C=US/O=Apple Inc./OU=Apple iPhone/CN=Apple iPhone Device CA
334	/CN=Layer Client CA/C=US/L=San Francisco/O=Layer, Inc/ST=CA
221	/CN=AnyDesk Client
76	/C=KR/ST=Kyunggido/L=Suwon/O=Samsung Electronics (*redacted*)
52	/CN=Ricoh Remote Service (*redacted*)

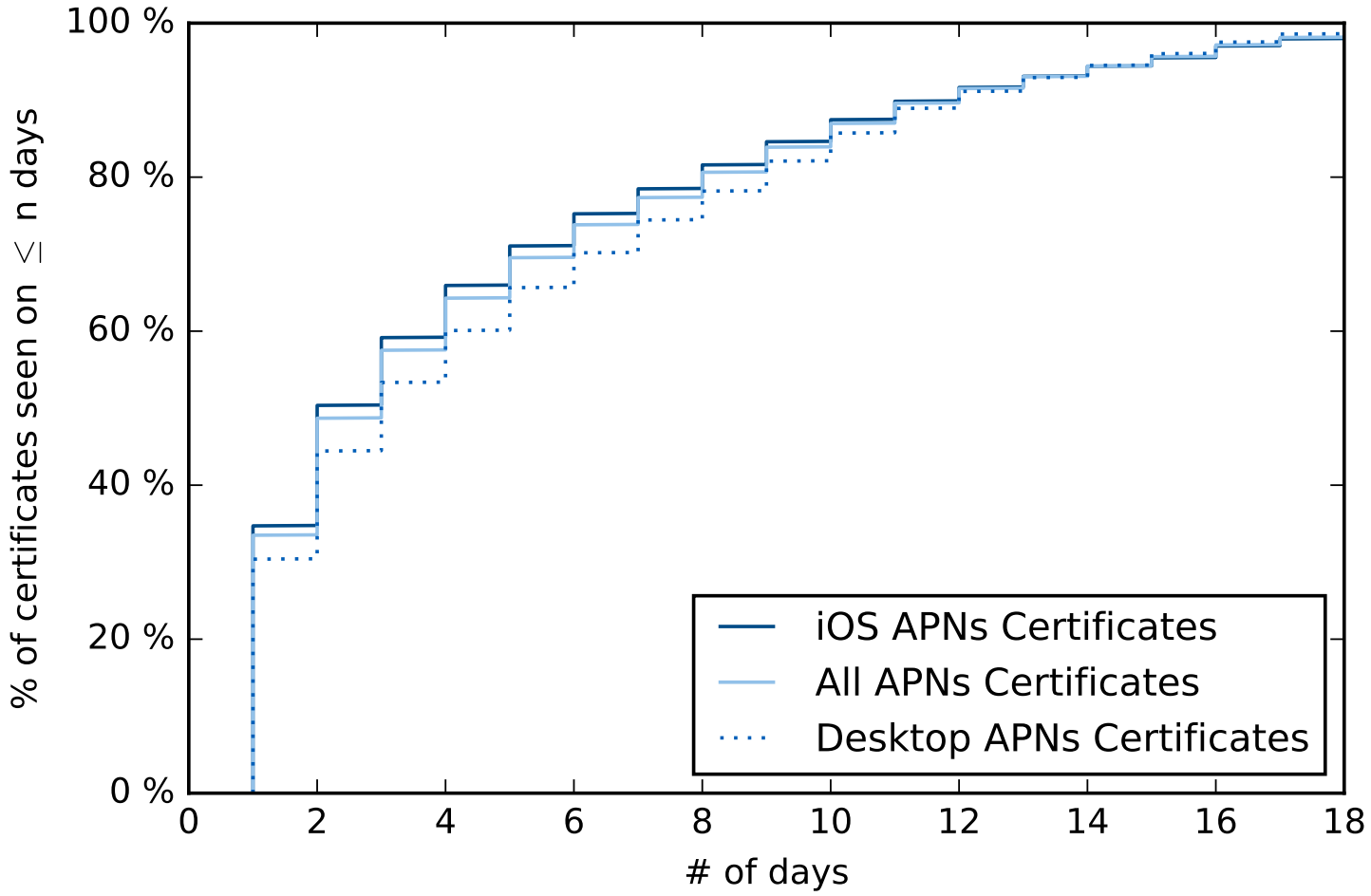
Case Study - how well can we track a single user?

Informed Consent

Note: We are tracking a device. As mobile devices are typically closely carried, they allow conclusions about users.



What % of certificates is traceable?



≈ 50% of certificates observed on 3 or more days.

Is global tracking feasible?

Cut short in this presentation, key insights of large RIPE Atlas active measurement campaign:

- Majority of APNs logins are routed through few central IXPs/ISPs
- Listening at these, attackers can globally track >80% of devices

Responsible Disclosure

We informed Apple's product security team before publication:

- Very quick response
- Several phone calls, continuous contact
- Several engineers in calls and working on resolution

Fixed with January 2017 security patches

What now?

TLS 1.3 encrypts certificates

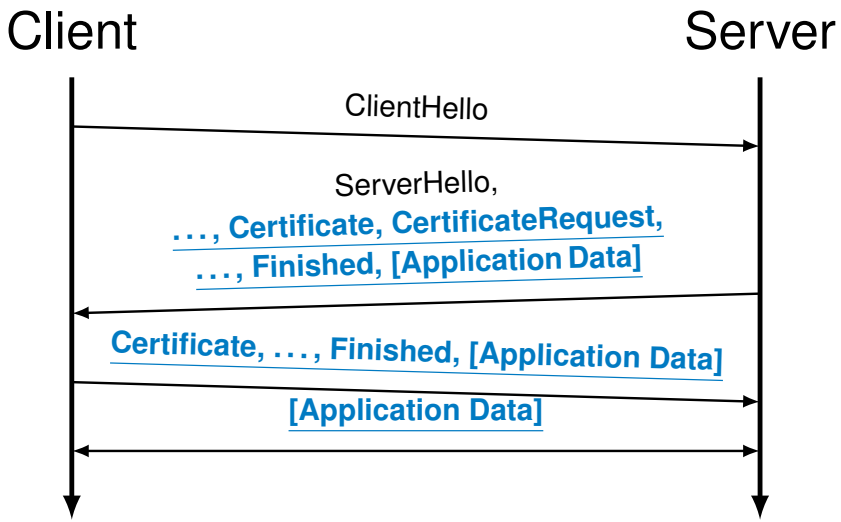


Figure: TLS 1.3 handshake, Unencrypted Data, **[Encrypted Data]**

But: ClientHello Extensions still unencrypted:

- Server Name Indication (SNI)
- Application-specific data

Key Messages, Data, and Code

- TLS-CCA sends certificates unencrypted
- In an “always-on” mobile scenario, this can cause serious privacy issues
- We quantified this issue in the Apple Push Notification Service (APNs), Apple fixed promptly
- Be **very** careful about traceable identifiers in protocol design!
- Reproducibility: Turned replication/reproduction into a lab at TMA PhD school

Data and Code:

`https://github.com/tumi8/cca-privacy`