Mobile Subscriber WiFi Privacy

Piers O'Hanlon

Ravishankar Borgaonkar

Lucca Hirschi (LSV, University Paris-Saclay)

MoST IEEE S & P Workshop 2017

5G-Ensure

Overview

- Mobile identifiers
- IMSI Catchers/Trackers
  - Conventional
  - WiFi-based
- WiFi authentication flaws
- EAP-SIM/AKA Formal Analysis
- Mitigations
  - User/MobileOS/Operator

Mobile identifiers

- Subscriber identifiers
    - Mobile subscriber identity
        - International Mobile Subscriber Identity (IMSI)
        - Temporary IMSI (TIMSI)
    - Mobile number
        - Mobile Station International Subscriber Directory Number (MSISDN)
- Device identifiers
    - International Mobile Equipment Identity (IMEI)
    - WiFi MAC address
    - Bluetooth MAC address
    - NFC Address
- Network/OS level identifiers
    - IP addresses, Hostnames, DHCP options, Multicast DNS names, etc
- Application level identifiers
    - Usernames, identifiers, handles, etc

What is an IMSI?

- **I**nternational **M**obile **S**ubscriber **I**dentity
  - 15 digit number (**M**Country**C**ode+**MN**et**C**ode+**MSI**d**N**um)
    - e.g. **234123456789012**
  - Identity for mutual authentication of a device to the network
  - Using SIM's secret 128-bit authentication Key (K_i) and for 3/4G the **S**e**q**uence **N**umber (SQN)
- Stored in two places:
  - In the 'SIM Card' (USIM/UICC)
    - IMSI is accessible in read only section of SIM
    - Secret key (K_i) and SQN are not directly readable

  - At the Operator
    - IMSI indexes K_i and SQN from HSS/AuC Database
- An identifier that can be used for tracking

Conventional IMSI Catchers

- Typical features
    - Tracking: IMSI/IMEI, Location
    - Interception: Call/SMS/Data
- Operates on licensed Mobile Bands: 2G(GSM)/3G/4G
- Acts as a fake base station to lure nearby mobile devices
    - ‘Passive’ - mainly for tracking (interception when no/weak ciphering)
    - Active – interception and tracking
- Cost
    - Commercial solutions expensive
    - Now cheaper options using Laptop+SDR board
- Been around since the early 1990s
    - Patented in Europe in 1993

Conventional IMSI Catchers: 2-4G

2G

- Exploits protocol flaws (no mutual authentication..)
- Tracking & Interception
- Easily available to buy online
- Use of fake base station

http://www.epicos.com/EPCompanyProfileWeb/Content/Ability/EM_GSM.JPG

3G/4G

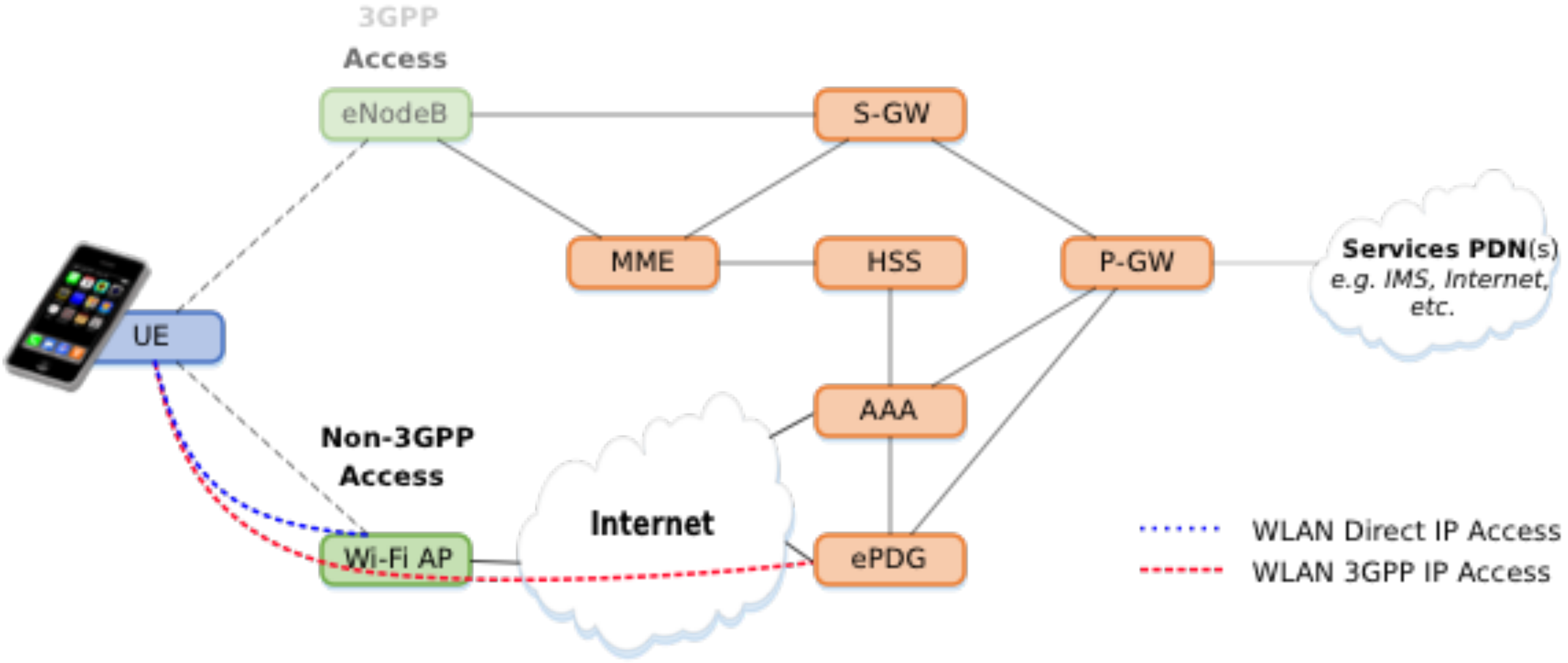
- Exploits architecture issues (Base station > UE..)
- Tracking & difficult to intercept traffic w.r.t 2G
- Commercial products usually downgrades
- Use of legitimate base station also possible

http://edge.alluremedia.com.au/m/g/2016/05/nokia_ultra_compact_network.jpg

WiFi-Based IMSI Catcher

- Features
  - Tracking: IMSI, Location
  - No interception
- Operates in unlicensed ISM Bands: WiFi
  - Range - few hundred meters – can be extended…
  - Fake Access Points
  - Redirect/Spoofs mobile packet data gateway
  - Exploits protocol & configuration weaknesses
- Based on two separate access techniques [3GPP TS33.234]
  - **WiFi Network Authentication (‘WLAN direct IP access’)**
  - **WiFi-Calling Authentication (‘WLAN 3GPP IP access’)**
- Cost
  - Low: Virtually any WiFi capable computer

Mobile network Architecture



WiFi Network attachment
(WLAN direct IP access)

- Unencrypted WiFi access points (APs)
  - Captive Portal approaches
    - Wireless Internet Service Provider roaming(WiSPr) etc
- Encrypted WiFi APs
  - Pre-shared password/credentials
- ‘Auto Connect’ Encrypted WiFi APs (802.1X)
  - WiFi key is negotiated without user intervention
  - Based on credentials in the USIM/UICC (‘SIM Card’)
  - Controlled by operator provided configuration
    - Manual
    - Automatic/pre-installed

Manual Configuration

- Some Android devices require initial manual configuration
  - After which it automatically connects
- Instructions on operator websites
  - Follow simple steps to set up
- Android provides various Carrier controlled mechanisms
  - Lollipop (v5.1 MR1): UICC Carrier Privileges
  - Marshmallow (v6.0): Carrier Configuration
    - “Privileged applications to provide carrier-specific configuration to the platform”

Automatic configuration

- Some Android and Windows phones automatically connect based on SIM
- iOS configures phone based on inserted SIM
    - Activates an operator specific .mobileconfig file
    - Configures a range of operator specific options
        - Including a list of 802.1X supported WiFi SSIDs
- Our analysis of iOS9 profiles showed
    - More than 60 profiles (44 countries) for 802.1X WiFi
    - Containing 66 unique SSIDS plus other config
- **=> Phones continuously trying to silently automatically authenticate**

Automatic WiFi Authentication

- Port Based Network Access Control [IEEE 802.1X]
  - Uses **E**xtensible **A**uthentication **P**rotocol (EAP) [RFC3748] **o**ver **L**AN (EAPOL) over WiFi
- Based upon two EAP Methods
  - EAP-SIM [RFC 4186]
    - GSM based security - Currently most widely used
  - EAP-AKA [RFC 4187]
    - 3G based security - Being deployed
- Support in all major Mobile OSes: Android, iOS, Windows Mobile, and Blackberry devices
  - Reported the issue to them all and to operators & GSMA
- Deployed in many countries – adoption growing

EAP-SIM/AKA Identities

- Three basic identity types for authentication
  - Permanent-identity (IMSI)
    - Typically used initially after which temporary ids are used
  - Pseudonym identity
    - A pseudonym for the IMSI has limited lifetime
  - Fast reauthentication-identity
    - Lower overhead re-attachment after initial exchange
- Behaviour affected by peer policy
  - “Liberal” peer - Current default
    - Responds to any requests for permanent identity
  - “Conservative” peer – Future deployment option
    - Only respond to requests for permanent identity when no Pseudonym identity available

EAP-SIM/AKA transport

- Basic EAP protocol is not encrypted
- Currently EAP-SIM/AKA in EAPOL is unencrypted
    - **Thus IMSI is visible (to a passive attacker) when permanent identity used for full authentication** 😱
    - **Also open to active attacks by requesting full auth** 😱
- Problem amplified due to pre-configured profiles
    - Mobile devices are constantly checking for pre-configured SSIDs and attempting authentication
- WiFi Access keys not compromised
    - All content still protected

WiFi-Calling Operation
(WLAN 3GPP IP access)

- Phone connects to Edge Packet Data Gateway (EPDG) over WiFi
  - Voice calls over WiFi
  - Phone connects on low/no signal
    - Also connects in Airplane mode + WiFi …
- Connection to EPDG uses IPsec
  - Authenticates using Internet Key Exchange Protocol (IKEv2)
- Supported on iOS, Android, and Windows devices
  - WiFi-Calling available in a number of countries
  - The issue also been reported to OS makers and Operators

IPsec brief overview

- **I**nternet **P**rotocol **Sec**urity
  - Confidentiality, data integrity, access control, and data source authentication
  - Recovery from transmission errors: packet loss, packet replay, and packet forgery
- Authentication
  - Authentication Header (AH) - RFC 4302
- Confidentiality
  - Encapsulating Security Payload (ESP) - RFC 4303
- **Key management**
  - Internet Key Exchange v2 (IKEv2) - RFC7296
- Two modes
  - Tunnel - used for connection to Gateway (EPDG)
  - Transport

IKEv2 weakness

- Initiates connection in two phases
  - IKE_SA_INIT
    - Negotiate cryptographic algorithms, exchange nonces, and do a Diffie-Hellman exchange
  - IKE_AUTH
    - Authenticate the previous messages, **exchange identities (e.g. IMSI),** and certificates, and establish the child Security Association(s) (SA)
- IKE_AUTH uses EAP-AKA to exchange identities
  - DH-encrypted IMSI exchange not protected by a certificate
  - Open to MitM attacks on identity exchange (e.g. IMSI) 😱
- IPsec ESP keys are not compromised
  - Call content still safe

EAP-SIM/AKA Formal Analysis

- Analysed EAP-SIM/AKA in *ProVerif* security protocol analyser
  - Modelled using a symbolic model based upon applied π-calculus
  - EAP-AKA is stateful, uses XOR, and SQN so it was simplified
- We used the models to formally verify untraceability of the IMSI for two users
- Attack found when IMSI is unhidden – as expected
- No attack found when IMSI hidden (encrypted/ pseudonym) without additional authentication material

EAP-SIM traceability attack

- When IMSI hidden and attacker knows n(=3) GSM authentication triplets for targeted IMSI
  - GSM Triplet: Signed Response [SRES] (32-bit), Random number [RAND] (128-bit), & Ciphering Key [Kc] (64-bit)
  - Using known GSM triplets, attacker sends challenge request to mobile device (Step 5 – Next Slide)
  - If mobile device accepts challenge

    ==> mobile is the targeted device

EAP-SIM Full Authentication

```
  Peer                                                 Authenticator
1.  |                               EAP-Request/Identity       |
    |<---------------------------------------------------------|
    |                                                          |
2.  | EAP-Response/Identity (e.g. IMSI)                        |
    |-------------------------------------------------------->|
    |                                                          |
3.  |                  EAP-Request/SIM/Start (AT_VERSION_LIST) |
    |<---------------------------------------------------------|
    |                                                          |
4.  | EAP-Response/SIM/Start (AT_NONCE_MT, AT_SELECTED_VERSION)|
    |-------------------------------------------------------->|
    |                                                          |
5.  |           EAP-Request/SIM/Challenge (AT_RAND, AT_MAC)    |
    |<---------------------------------------------------------|
 +-------------------------------------+                       |
 | Peer runs GSM algorithms, verifies  |                       |
 | AT_MAC and derives session keys     |                       |
 +-------------------------------------+                       |
6.  | EAP-Response/SIM/Challenge (AT_MAC)                      |
    |-------------------------------------------------------->|
    |                                                          |
7.  |                                             EAP-Success  |
    |<---------------------------------------------------------|
    |                                                          |
```

Operator/Vendor Mitigations

- Deprecate EAP-SIM in favour of EAP-AKA
  - EAP-SIM is weaker as it only uses GSM triplets
- Deploy EAP-AKA/SIM with conservative peer pseudonym
- Deploy Certificate based approach
  - Deploy certificates on suitable AAA infrastructure
  - Deploy certificate protected tunnelled EAP-AKA for WLAN access
    - E.g. EAP-TTLS+EAP-AKA on 802.1X
  - Deploy certificate protected IPsec/IKEv2 to EPDG
    - E.g. EAP-TTLS+EAP-AKA for IKE_AUTH, or multiple IKEv2 auth exchange
- (Re)investigate other potential solutions
  - IMSI encryption – 5G-ENSURE project has proposed an 'enabler'
  - E.g. 3GPPP TD S3-030081 – 'Certificate-Based Protection of IMSI for EAP-SIM/AKA'
- Standards bodies should re-evaluate approaches

Mobile OS Mitigations

- Support conservative peer for EAP-AKA/SIM with pseudonym support
  - Emerging in some OSes (e.g. iOS10)
  - iOS10 has conservative peer pseudonym support – due to us 😉
- Certificate based approach
  - Support for EAP-TTLSv0 + EAP-AKA in IKEv2 & EAPOL
- Allow for more user choice with automatic WiFi network access
  - Preferably allow for editing of all stored associations

User Mitigation

- WiFi Network Access Control
    - iOS
        - Turn off ‘Auto-Join’ toggle for Auto-WiFi networks
            - Only possible when network in range
        - iOS10 will provide better protection (once operators deploy pseudonym support)
    - Android
        - ‘Forget’ Auto-WiFi profiles
            - Depending on version only possible when network in range
- WiFi-Calling
    - Android/iOS: Selectively disable WiFi-Calling
- Switch off WiFi in untrusted environments

Summary

- Large scale IMSI exposure issues
  - Poor privacy mandates in standards
  - Widespread device pre-configuration with no opt out
  - Lack of checking by companies involved
- We’ve been working with Operators/Vendors/ OS companies to fix the issue
  - But it’s a complex issue requiring changes by all
  - iOS 10 conservative peer support due to this work
  - EAP-AKA is now starting to replace EAP-SIM
- We need stronger privacy protections

Conclusions & Future Work

- Investigating other uses of EAP-SIM/AKA
- Exploring use of USIM credentials in other WiFi based protocols
- Continuing work in 5GENSURE.EU Project
  - Security Architecture and enablers

5G-Ensure

5G Enablers for network and system security and resilience

5G-ENSURE: http://www.5gensure.eu

contact@5gensure.eu

@5GEnsure

European Commission

5G ENSURE receives funding from the EU Framework Programme for Research and Innovation H2020 under grant agreement No 671562 | Duration November 2015 – October 2017

5G PPP

The 5G Infrastructure Public Private Partnership (SG PPP)

Questions?