WiFi-Based IMSI Catcher

Piers O’Hanlon
Ravishankar Borgaonkar

Overview

• What is an IMSI?
• Conventional IMSI Catchers
• WiFi-based IMSI Catcher
  • WiFi Network Authentication 🔴
  • WiFi Calling Authentication 🔴
• Operator/Vendor/OS Mitigations
• User Mitigations
• Demo
What is an IMSI?

- **International Mobile Subscriber Identity**
  - 15 digit number e.g. 234123456789012
  - Allows for mutual authentication of a device to the network
    - Using SIM’s secret authentication Key ($K_i$) and for 3/4G the Sequence Number (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
  - One of a few like WiFi/Bluetooth/NFC Hardware address (e.g. MAC), IMEI, MSISDN (Phone number), etc.
Conventional IMSI Catchers

• Typical features
  • Tracking: IMSI/IMEI, Location
  • Interception: Call/SMS/Data

• Operates on licensed Mobile Bands: GSM/3G/4G

• Acts as a fake base station to lure nearby mobile devices

• Operates in two modes
  • ‘Passive’ - mainly for tracking (interception when no/weak ciphering)
  • Active – interception and tracking

• Cost
  • Commercial solutions expensive - but now possible with Laptop+SDR board

• Been around since the early 1990s
  • Patented in Europe in 1993
Techniques in Conventional IMSI Catchers

2G

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

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
Protection against IMSI Catchers

- No protection for commercial non-rooted mobile devices
- Special phones (expensive though) and apps for rooted phones
- Turn off cellular connection or use WiFi platform for secure calls/data
WiFi-Based IMSI Catcher

• Features
  • Tracking: IMSI, Location
  • No interception (yet)

• 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 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
WiFi Network attachment

• Unencrypted WiFi access points
  • Captive Portal approaches
    • Wireless Internet Service Provider roaming (WiSPr) etc

• Normal Encrypted WiFi access points
  • Pre-shared password/credentials

• ‘Auto Connect’ Encrypted WiFi access points
  • 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
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 Auto/EAP supported WiFi SSIDs

• Our analysis of iOS9 profiles showed
  • More than 50 profiles for Auto/EAP WiFi
  • Also other config info
‘Manual’ Configuration

• Some Android devices require initial manual config
  • 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 WiFi Authentication

• Port Based Network Access Control [IEEE 802.1X]
  • Uses Extensible Authentication Protocol (EAP) [RFC3748] over LAN (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 Android, iOS, Windows Mobile, and Blackberry devices
  • We’ve reported the issue to them all and to operators & GSMA
    • No privacy bounties 😞
  • Apple included ‘conservative peer’ support due to our work

• 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 😱
- WiFi Access keys not compromised
  - All content still protected
- There are encrypted tunnel EAP methods
  - EAP-TTLSv0, EAP-TLS...
  - But support required in both mobile OS and operator
WiFi-Calling Connection

- 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

- **Internet Protocol Security**
  - 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) - RFC 7296
- **Two modes**
  - Tunnel - used for connection to Gateway (EPDG)
  - Transport
Internet Key Exchange (IKEv2)

• 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
  • IMSI exchange not protected by a certificate
  • Open to MitM attacks on identity (IMSI)

• IPsec ESP keys are not compromised
  • Call content still safe
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. 3GPPPP 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)

• Certificate based approach
  • Support for EAP-TTLv0 + EAP-AKA in IKEv2 & EAPOL
  • Other approaches?

• 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 may provide better protection (once operators deploy support)
      - It has conservative peer pseudonym support – due to us 😆
  - 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

• Exposed two IMSI catching new techniques
  • WiFi Network authentication protocols
  • WiFi-Calling authentication protocols

• Most of the world’s smartphones implement these protocols
  • Both techniques rely upon installed operator automatic configuration for these popular services

• We’ve been working with Operators/Vendors/OS companies to fix the issue
  • But it’s a complex issue
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
Demo and Questions...