IMSI-Catcher and Man-in-the-Middle attacks

Julian Dammann

Seminar Mobile Security
09 February 2011, b-it
Outline

1 Introduction
2 Man-in-the-Middle-Attacks
3 IMSI and SIM cards
4 IMSI-Catcher
5 GSM
6 UMTS
7 Mitigating Factors
8 Counter-measures
9 Conclusion
Scenario

- Wireless medium: Air
- Cryptography is used to ensure confidentiality and authenticity
- Attacks which circumvent cryptography all together are available
Threats and attacks

- Tracking of mobile services’ users
- Eavesdropping/Tapping
- Man-in-the-Middle
- Law enforcement may be more or less warranted
- (Organized) Crime has an interest as well!
- Internet threats apply: Spoofing, phishing, fraud, malware
Man-in-the-Middle-Attacks

The attacker

- positions himself between communicating parties
- stays invisible to his victims
- is able to eavesdrop
- may be able to manipulate messages
Man-in-the-Middle-Attacks

The attacker

- positions himself between communicating parties
- stays invisible to his victims
- is able to eavesdrop
- may be able to manipulate messages

Defense

- Authentication ensures the communication parties of their peers identities and of the message integrity
- Encryption ensures confidentiality
IMSI and SIM cards

- International Mobile Subscriber Identity (IMSI) number is used to identify a specific user.
- IMSI is usually stored on a Subscriber Identity Module (SIM), a smart card issued by the user’s provider, which also contains a shared secret.
IMSI and SIM cards

- International Mobile Subscriber Identity (IMSI) number is used to identify a specific user
- IMSI is usually stored on a Subscriber Identity Module (SIM), a smart card issued by the user’s provider, which also contains a shared secret
- IMSI is up to 15 digits long, consists of
  - 3 digit Mobile Country Code (MCC)
  - 2-3 digit Mobile Network Code (MNC)
  - 1-10 digit Mobile Subscriber Identification Number (MSIN)
IMSI and SIM cards

- International Mobile Subscriber Identity (IMSI) number is used to identify a specific user.
- IMSI is usually stored on a Subscriber Identity Module (SIM), a smart card issued by the user’s provider, which also contains a shared secret.
- IMSI is up to 15 digits long, consists of:
  - 3 digit Mobile Country Code (MCC)
  - 2-3 digit Mobile Network Code (MNC)
  - 1-10 digit Mobile Subscriber Identification Number (MSIN)
- MCC and MNC together form the Home Network Identifier (HNI):
  - which identifies the subscriber’s home network
  - in Germany: allocated by the Bundesnetzagentur
  - may allow provider identification
Tracking

Requirements

- To track a user, the attacker has to identify the user within the mobile cell
- Usually identified by the target’s IMSI, which the attacker got hold of before the attack
Tracking

Requirements

• To track a user, the attacker has to identify the user within the mobile cell
• Usually identified by the target’s IMSI, which the attacker got hold of before the attack

Countermeasures

• IMSI is transmitted as rarely as possible
• Temporary Mobile Subscriber Identity (TMSI)
  • is used instead to identify the user temporarily
  • is randomly assigned
  • is allocated after first location update
  • is local to the area of the cell
  • is changed periodically by the network
  • is changed on location changes
An IMSI-Catcher is a device used to:

- masquerade as a base station
- Works, as mobile phones are required to optimize the reception
An IMSI-Catcher is a device used to

- masquerade as a base station
  - Works, as mobile phones are required to optimize the reception

- collect the IMSIs of users in a target area
  - by indicating to the holder of an unknown TMSI that the TMSI is invalid
  - thus triggering the sending of the IMSI by the mobile phone user
An IMSI-Catcher is a device used to

- masquerade as a base station
  - Works, as mobile phones are required to optimize the reception
- collect the IMSIs of users in a target area
  - by indicating to the holder of an unknown TMSI that the TMSI is invalid
  - thus triggering the sending of the IMSI by the mobile phone user
- track/or locate a specific IMSI
  - using signal strength and signal propagation delay
An IMSI-Catcher is a device used to

- masquerade as a base station
  - Works, as mobile phones are required to optimize the reception

- collect the IMSIs of users in a target area
  - by indicating to the holder of an unknown TMSI that the TMSI is invalid
  - thus triggering the sending of the IMSI by the mobile phone user

- track/or locate a specific IMSI
  - using signal strength and signal propagation delay

- to place the attacker as a man-in-the-middle
  - user establishes a connection with the fake base station.
  - IMSI-Catcher establishes another connection to a real base station, to forward communication
GSM

- most wide-spread. 80% of global market mobile phone users use it
GSM

- most wide-spread. 80% of global market mobile phone users use it
- several flaws in the protocol as well as in the cryptography algorithms have been found
GSM

- most wide-spread. 80% of global market mobile phone users use it
- several flaws in the protocol as well as in the cryptography algorithms have been found
- newer and supposedly more secure protocols are available
GSM

- most wide-spread. 80% of global market mobile phone users use it
- several flaws in the protocol as well as in the cryptography algorithms have been found
- newer and supposedly more secure protocols are available
- due to superior GSM coverage, and high cost of new base station equipment, interoperation must be considered by future protocols
GSM

- most wide-spread. 80% of global market mobile phone users use it
- several flaws in the protocol as well as in the cryptography algorithms have been found
- newer and supposedly more secure protocols are available
- due to superior GSM coverage, and high cost of new base station equipment, interoperation must be considered by future protocols
- backwards-compatible protocol extensions are difficult to integrate without giving up the security gains of the newer protocol
GSM

- most wide-spread. 80% of global market mobile phone users use it
- several flaws in the protocol as well as in the cryptography algorithms have been found
- newer and supposedly more secure protocols are available
- due to superior GSM coverage, and high cost of new base station equipment, interoperation must be considered by future protocols
- backwards-compatible protocol extensions are difficult to integrate without giving up the security gains of the newer protocol
- user equipment has to support several protocols, which gives rise to more cases which have to be considered and analyzed
Network structure

Mobile Stations (MS) - mobile phones, etc.

- share IMSI with the Home Location Register (HLR) database
- share IMEI with the Equipment Identity Register (EIR) database
Introduction

Man-in-the-Middle Attacks

IMSI and SIM cards

IMSI-Catcher

GSM

UMTS

Mitigating Factors

Countermeasures

Conclusion

Network structure

Base Stations (BS)

- connect mobile stations to Mobile switching centers
- area covered by a base station is called a cell
- handle encryption and decryption of data transmitted between user and network
Network structure

Base Station Controllers (BSC)

- coordinate base stations
- may handle handovers
Network structure

Mobile Switching Centers (MSC)
- access Authentication Center (AuC) to handle authentication of mobile stations
- access EIR to detect stolen mobile station equipment
- maintain Visitor Location Register (VLR), which stores TMSI and data obtained from HLR
- route data between networks
- handover between base station controllers
Authentication Protocol
Weaknesses

- No base station authentication
- Encryption algorithms, A5 family, basically broken
- A5/0 - No Encryption algorithm is a valid choice
The attack

Introduction

Man-in-the-Middle-Attacks

IMSI and SIM cards

IMSI-Catcher

GSM

UMTS

Mitigating Factors

Countermeasures

Conclusion
UMTS

- Universal Mobile Telecommunications Standard - 3rd generation protocol
- Low coverage compared to GSM, as new base stations are required
- Interoperation with GSM possible
Changes compared to GSM

- Some architecture parts have been combined, renamed, etc.
  - Home Environment (HE) takes the role of MSC and HLR
  - Service Network (SN) takes the role of MSC and VLR
Changes compared to GSM

- Some architecture parts have been combined, renamed, etc.
  - Home Environment (HE) takes the role of MSC and HLR
  - Service Network (SN) takes the role of MSC and VLR
- New crypto algorithms, cipher Kasumi A5/3
Changes compared to GSM

- Some architecture parts have been combined, renamed, etc.
  - Home Environment (HE) takes the role of MSC and HLR
  - Service Network (SN) takes the role of MSC and VLR
- New crypto algorithms, cipher Kasumi A5/3
- HE has to authenticate itself to the mobile station
Changes compared to GSM

- Some architecture parts have been combined, renamed, etc.
  - Home Environment (HE) takes the role of MSC and HLR
  - Service Network (SN) takes the role of MSC and VLR
- New crypto algorithms, cipher Kasumi A5/3
- HE has to authenticate itself to the mobile station
- Sequence numbers are used to guarantee freshness of authentication
Changes compared to GSM

- Some architecture parts have been combined, renamed, etc.
  - Home Environment (HE) takes the role of MSC and HLR
  - Service Network (SN) takes the role of MSC and VLR
- New crypto algorithms, cipher Kasumi A5/3
- HE has to authenticate itself to the mobile station
- Sequence numbers are used to guarantee freshness of authentication
- Messages are integrity protected - MAC is used for the authentication process
Changes compared to GSM

- Some architecture parts have been combined, renamed, etc.
  - Home Environment (HE) takes the role of MSC and HLR
  - Service Network (SN) takes the role of MSC and VLR
- New crypto algorithms, cipher Kasumi A5/3
- HE has to authenticate itself to the mobile station
- Sequence numbers are used to guarantee freshness of authentication
- Messages are integrity protected - MAC is used for the authentication process
- Security capabilities of the mobile station included in final message
Interoperation with GSM

- GSM keys are computed from UMTS key material
- cipher mode command is last message - no security capabilities included
Authentication Protocol

MS

GSM BS

SN

HE

Security Capabilities

Identity Request

IMSI

IMSI

Auth. Parameter Request, IMSI

AV = RAND||XRES||CK||IK||AUTN

RAND, AUTN

RES

RES

RES $\neq$ XRES

Compute $K_C$

TMSI

GSM Cipher Mode Command

GSM Key $K_C$
The attack

Step 1

IMSI Catcher

SN

HE

Security Capabilities
Identity Request
IMSI
Save RAND and AUTN
disconnect

Auth. Parameter Request, IMSI
Authentication Vector AV

GSM
UMTS
Mitigating Factors
Countermeasures
Conclusion
The attack

Step 1

<table>
<thead>
<tr>
<th>IMSI Catcher</th>
<th>SN</th>
<th>HE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Capabilities</td>
<td>Auth. Parameter Request, IMSI</td>
<td></td>
</tr>
<tr>
<td>Identity Request</td>
<td>Authentication Vector AV</td>
<td></td>
</tr>
<tr>
<td>IMSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>save RAND and AUTN</td>
<td>RAND, AUTN</td>
<td></td>
</tr>
<tr>
<td>disconnect</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 2

<table>
<thead>
<tr>
<th>MS</th>
<th>IMSI Catcher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Capabilities</td>
<td>GSM BS</td>
</tr>
<tr>
<td>Identity Request</td>
<td>IMSI</td>
</tr>
<tr>
<td>IMSI</td>
<td>RAND, AUTN</td>
</tr>
<tr>
<td>verify AUTN compute RES</td>
<td>RES</td>
</tr>
<tr>
<td>GSM Cipher Mode Command</td>
<td></td>
</tr>
</tbody>
</table>
Mitigating Factors

- mobile phone must be in standby mode
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
- IMSI must be known beforehand, or by observation and elimination
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
- IMSI must be known beforehand, or by observation and elimination
- Real base stations signal power may be too high for the IMSI-Catcher to surpass
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
- IMSI must be known beforehand, or by observation and elimination
- Real base stations signal power may be too high for the IMSI-Catcher to surpass
- Call is made using the IMSI-Catchers phone number
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
- IMSI must be known beforehand, or by observation and elimination
- Real base stations signal power may be too high for the IMSI-Catcher to surpass
- Call is made using the IMSI-Catcher’s phone number
- Mobile phones may alert the user when no encryption is used
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
- IMSI must be known beforehand, or by observation and elimination
- Real base stations signal power may be too high for the IMSI-Catcher to surpass
- Call is made using the IMSI-Catchers phone number
- Mobile phones may alert the user when no encryption is used
- Other mobile phones in the vicinity have no network connectivity
Mitigating Factors

- mobile phone must be in standby mode
- user’s network operator must be found out
- IMSI must be known beforehand, or by observation and elimination
- Real base stations signal power may be too high for the IMSI-Catcher to surpass
- Call is made using the IMSI-Catchers phone number
- Mobile phones may alert the user when no encryption is used
- Other mobile phones in the vicinity have no network connectivity
- Victim may get an extra phone to detect IMSI-Catcher setups
Mitigating Factors

• mobile phone must be in standby mode
• user’s network operator must be found out
• IMSI must be known beforehand, or by observation and elimination
• Real base stations signal power may be too high for the IMSI-Catcher to surpass
• Call is made using the IMSI-Catcher’s phone number
• Mobile phones may alert the user when no encryption is used
• Other mobile phones in the vicinity have no network connectivity
• Victim may get an extra phone to detect IMSI-Catcher setups
• Victim may change her SIM card regularly, or even the phone
Countermeasures

- Authenticate the 'identity request', made by the base station
Countermeasures

- Authenticate the 'identity request', made by the base station
- Generate cipher mode command in the Service Network, to be able to authenticate it, and include mobile station’s original security capabilities
Conclusion

- Feasible attacks which invade user privacy and are a security threat are out there
Conclusion

- Feasible attacks which invade user privacy and are a security threat are out there
- Changes to protocols are necessary
Conclusion

- Feasible attacks which invade user privacy and are a security threat are out there
- Changes to protocols are necessary
- Socio-economic factors make this hard to fulfill
Conclusion

- Feasible attacks which invade user privacy and are a security threat are out there
- Changes to protocols are necessary
- Socio-economic factors make this hard to fulfill
- Adapting protocols without introducing new problems or security flaws is not trivial
Conclusion

- Feasible attacks which invade user privacy and are a security threat are out there
- Changes to protocols are necessary
- Socio-economic factors make this hard to fulfill
- Adapting protocols without introducing new problems or security flaws is not trivial
- Welcome to the future, welcome to the past!
Credit where credit is due

- Seminar on IMSI Catcher, Daehyun Strobel
  http://www.cryptorub.de/imperia/md/content/seminare/itss07/imsi_catcher.pdf
- Ulrike Meyer and Susanne Wetzel
- The authors of \LaTeX{} and the excellent ”beamer” class
Questions?