Abusing Over-The-Air Client Provisioning

My SMS to do your Settings

Artyom Skrobov
Slava Makkaveev
Old-school hack that remains relevant

- Using classic SMS as an attack instrument
  - a cheap USB GSM dongle can be used to send a custom SMS
  - any phone on earth could be the target of the message
- One SMS is enough to intercept your mobile traffic, steal your contacts, emails, and more.
- ~40% of mobile devices are vulnerable
- Flaw in the specification, not a software or hardware vulnerability
Mobile Client Provisioning
Basics
Client Provisioning (CP) Technology

- The **operator** sends a special **message** as soon as detects a new **device** on the network
- Used to deploy operator-specific settings, such as the address of MMS service center
- The message format defined by **Open Mobile Alliance**
Open Mobile Alliance (OMA)

- Standards body coordinating the mobile industry
- Members are equipment & software vendors, and network operators
- Board of Directors includes representatives (as of this year) from ARM, AT&T, Ericsson, Intel, Nokia, Orange, Qualcomm, Sierra Wireless & T-Mobile
OMA CP

- Does for mobile what IETF does for the Internet
- Specifications relevant to Client Provisioning
  - OMA-WAP-TS-WSP-V1_0-20020920-C “Wireless Session Protocol 1.0”
  - OMA-WAP-TS-PushOTA-V2_1-20051122-C “Push Over The Air”
  - OMA-WAP-TS-ProvBoot-V1_1-20090421-C “ Provisioning Bootstrap”
  - OMA-WAP-TS-ProvCont-V1_1-20090728-A “ Provisioning Content”
  - ...
Short Message Transfer Protocol (GSM 03.40)

- Any SMS is transmitted as Protocol Data Units (PDUs)

- **SM-TP Header**
  - recipient phone number
  - data coding scheme

- **User Data Header (UDH)**
  - destination port 2948 (wap-push)
  - source port 9200 (wap-wsp)
  - message concatenation (user data limited to 140 bytes)

- **Wireless Session Protocol (WSP) Header**
  - authentication

- **Payload**
  - WAP Binary XML (WBXML)
WBXML payload example

```xml
<wap-provisioningdoc>
  <characteristic type="BOOTSTRAP">
    <param name="NAME" value="Important update"/>
    <param name="PROXY-ID" value="pwdn"/>
  </characteristic>

  <characteristic type="NAPDEF">
    <param name="NAME" value="pwdn"/>
    <param name="NAPID" value="pwdn"/>
    <param name="BEARER" value="GSM-GPRS"/>
    <param name="NAP-ADDRESS" value="Orange"/>
    <param name="NAP-ADDRTYPE" value="APN"/>
  </characteristic>

  <characteristic type="PXLLOGICAL">
    <param name="NAME" value="pwdn"/>
    <param name="PROXY-ID" value="pwdn"/>
  </characteristic>

  <characteristic type="PXPHYSICAL">
    <param name="PHYSICAL-PROXY-ID" value="pwdn"/>
    <param name="PXADDR" value="1.2.3.4"/>
    <param name="PXADDRTYPE" value="IPV4"/>
    <param name="TO-NAPID" value="pwdn"/>
  </characteristic>

  <characteristic type="PORT">
    <param name="PORTNR" value="8081"/>
  </characteristic>
</wap-provisioningdoc>
```

Configuration name shown to user: Important update

Network type: GSM-GPRS

Access Point Name: Orange

WAP Proxy IP: 1.2.3.4

WAP Proxy port: 8081
OMA CP message

1. SM-TP Header
2. UDH
3. WSP Header
4. WBXML Payload
5. Proxy IP/Port
Mobile Client Provisioning

Security
What does the specification say?

OMA-WAP-TS-ProvCont-V1_1-20090728-A

4.3 Media Type Parameter

The connectivity media type may contain security information, which is transported as parameters to the media type application/vnd.wap.connectivity-wbxml. The security information consists of the message authentication code and the security method. The parameters MAC and SEC have been defined for this purpose and these MUST be supported by the WAP client.

Parameters

SEC

The parameter specifies the security mechanism used (if it is not present, no security is used). If present it MUST take one of the values USERPIN, USERPINMAC, NETWPIN, USERNETWPIN [PROVBOOT]. If the parameter MAC is provided, the parameter SEC MUST also be present.

The parameter SEC can have the following values:

“.. the **IMSI** must be used as the network specified shared secret.”

OMA-WAP-TS-ProvBoot-V1_1-20090421-C

“...The connectivity media may contain security information..”

6. Network Specific Adaptations

6.1. Adaptation to GSM/UMTS

In GSM/UMTS, if USERNETWPIN or NETWPIN is used, the IMSI MUST be used as the network specific shared secret. When used as input to the MAC calculation, the IMSI MUST be in semi-octet representation as defined in [GSM11.11][TS51.011] for the SIM and in [TS31.102] for the USIM. The length indicator byte and possible unused bytes (i.e., the IMSI is less than 15 digits) MUST NOT be used. If the IMSI consists of an even number of digits the filler 0xF MUST be inserted.
Authentication is optional

- **WSP header** has optional authentication field, containing SHA-1 HMAC
- The key for HMAC can be USERPIN, NETWPIN, or other, less common variants

```
Content-Type=application/vnd.wap.connectivity-wbxml

WSP Header

SEC=NETWPIN

MAC
```
International Mobile Subscriber Identity (IMSI)

- NETWPIN uses IMSI as the key
- **IMSI** isn’t exactly public, but *easily obtainable*:
  - via a mobile application,
  - or cooperation with *any* network operator,
  - or fake BTS sniffing IMSI out of the air,
  - or looking up ICCID on the SIM card - it often matches the IMSI
Stealing IMSI with Android application

- Requires `android.permission.READ_PHONE_STATE`
  - One out of three apps already have it granted!

- Android API

```java
TelephonyManager tm = (TelephonyManager) getSystemService(Context.TELEPHONY_SERVICE);
String imsi = tm.getSubscriberId();
String iccid = tm.getSimSerialNumber();
```
How hard is it to attack?

- **Tools**
  - USB GSM dongle (~10$) + SIM
  - Simple script to build and send CP PDUs
    - NowSMS or other tools can be used as well

- **Authentication**
  - Not required: Samsung
  - IMSI: Huawei, LG, Sony, ...
Remotely controlled settings

- **WAP Proxy**
  - IP/Port/User/Password

- **Synchronization**
  - Server URL/User/Password
  - Contacts/Calendar

- **E-Mail**
  - IMAP4/POP3/SMTP Servers

- **MMS**
  - Server URL

- **Browser**
  - Home Page URL

- etc.

---

- Man-In-The-Middle
- Contacts/Calendar leak
- E-Mails leak
- MMS leak
- Phishing
Mobile Client Provisioning
In Practice
Samsung Galaxy

- Accepts non-authenticated CP messages
- Lists suggested settings
  - Do users understand what they accept?
Huawei, LG, Sony

- IMSI is the authentication key
- No information about suggested settings
It’s the perfect phishing attack!

- User cannot verify whether the suggested settings originate from a network operator, or an imposter
- Protection does not exist or is based on easily accessible key
- No special equipment is required to attack
- Anyone connected to the cellular network may be the target of the attack
- User does not know or understand what actually will be configured
Possible mitigations

- Drop CP messages from unauthorized parties at network level (by mobile operator)
- Disable the CP feature (vanilla Android did not implement it at all)
- Improve user interface:
  - Allow inspecting the suggested settings
  - Warn the user about the adverse effects of installing untrusted settings
- Improve CP security. Persuade OMA to publish guidelines
## Adopted mitigations

<table>
<thead>
<tr>
<th>Company</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung</td>
<td>Patched in May: SVE-2019-14073</td>
</tr>
<tr>
<td>LG</td>
<td>Patched in July: LVE-SMP-190006</td>
</tr>
<tr>
<td>Huawei</td>
<td>Plans to release the UI fix in the next generation of Mate series or P series smartphones</td>
</tr>
<tr>
<td>Sony</td>
<td>“We have concluded that our devices follow the specification.”</td>
</tr>
<tr>
<td>OMA</td>
<td>Open Mobile Alliance HelpDesk / OPEN-7587&lt;br&gt;OTA CP advanced phishing&lt;br&gt;Issue Type: General Problems - Tier 1&lt;br&gt;PRIORITY: High</td>
</tr>
</tbody>
</table>
Thank you!

slavam@checkpoint.com
artyomsk@checkpoint.com

@_cpresearch_
research.checkpoint.com