Session 2B
Security & Privacy
Privacy Leaks in Mobile Phone
Internet Access

Collin Mulliner
Security in Telecommunications
Technische Universität Berlin and
Deutsch Telekom Laboratories
Agenda

• Introduction
• Mobile Phone Web Access
• Collecting Data
• Results
• The MNO Privacy Checker
• Conclusions
• Q & A
Mobile web access is popular

- Most mobile phones have a browser
  - Web browser that displays HTML and supports JavaScript (WAP is dead!)
- Laptop “dial-up”
  - Tethering
- Mobile data is cheap around the world
  - Everybody is using it!
Privacy issue?

• I've read that some mobile phones leak private data through HTTP headers
  – Hard to believe – this would be really bad
• Searching for answers got me confused
  – People couldn't make up their minds if this is happening or not
• I decided to investigate myself
Mobile phones

• Everything that is NOT a smart phones
Mobile phone web access

• Comes pre-configured when phone is bought from operator
• Configuration can be done OTA when phone is bought from non-operator shop
• Example config from a German operator:
Collecting data

• I didn't believe anybody about what HTTP headers contain
  – This is basically the main point of this investigation

• I started to just log all HTTP headers
  – My site is mostly PHP so adding some logging is trivial
  – Images referenced by other sites are taken care of through an Apache's rewrite module
## Example dump

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST</td>
<td>mulliner.org</td>
</tr>
<tr>
<td>USER-AGENT</td>
<td>Mozilla/5.0 (X11; U; Linux armv71; en-US; rv:1.9.2alpre) Gecko/20090928 Firefox/3.5 Maemo Browser 1.4.1.15 RX-51 N900 image/png, image/*;q=0.8, <em>/</em>;q=0.5</td>
</tr>
<tr>
<td>ACCEPT</td>
<td>en</td>
</tr>
<tr>
<td>ACCEPT-ENCODING</td>
<td>*</td>
</tr>
<tr>
<td>ACCEPT-CHARSET</td>
<td>ISO-8859-1, utf-8; q=0.7, *; q=0.7</td>
</tr>
<tr>
<td>REFERER</td>
<td><a href="http://mulliner.org/blog/">http://mulliner.org/blog/</a></td>
</tr>
<tr>
<td>X-UP-SUBNO</td>
<td>1233936xxx-346677xxx</td>
</tr>
<tr>
<td>X-UP-FORWARDED_FOR</td>
<td>10.248.240.209</td>
</tr>
<tr>
<td>X-FORWARDED_FOR</td>
<td>10.248.240.209</td>
</tr>
<tr>
<td>X-UP-CALLING-LINE-ID</td>
<td>491522852xxxx</td>
</tr>
<tr>
<td>X-UP-SUBSCRIBER-COS</td>
<td>System, UMTS, SX-LIVPRT, A02-MADRID-1BILD-VF-DE, Vodafone, Prepaid, Rot</td>
</tr>
<tr>
<td>MAX-FORWARDS</td>
<td>10</td>
</tr>
<tr>
<td>VIA</td>
<td>1.1 rn2wwpsv161-ncl-0.wwp.vodafone.de</td>
</tr>
<tr>
<td>CONNECTION</td>
<td>close</td>
</tr>
<tr>
<td>REMOTE_ADDR</td>
<td>139.7.146.41</td>
</tr>
</tbody>
</table>
Getting traffic

- I'm a mobile devices guy and I have a website that shows it.
- I wrote some J2ME games a few years ago and a big site is embedding images from my web site.
- The website of our group (trifinite.org) is popular too...
- So yes, I get good traffic!
Needle in the haystack

- Now we got tones and tones of data
- How to find the interesting data?
  - Most likely: interesting equals rare
- Sort headers by occurrence...

Samples: 2105693

<table>
<thead>
<tr>
<th>Header</th>
<th>Count</th>
<th>Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP_X_WAP_FH_SUBSCRIBER_INFO</td>
<td>64</td>
<td>IP=10.142.249.144, MSISDN=60133972810, APN=post.wap.celcom3g,IP=10.163.132.2, ...</td>
</tr>
<tr>
<td>HTTP_X_MSP_MSISDN_ENC</td>
<td>5</td>
<td>X-MSP-MSISDN=&quot;R1yqtSXp6G5E/QB6L1u4Kg=&quot;.X-MSP-MSISDN=&quot;R1yqtSXp6G5E/QI...</td>
</tr>
<tr>
<td>HTTP_HUAWEI_HTTPMETHOD</td>
<td>75</td>
<td>MSISDN=2105754</td>
</tr>
<tr>
<td>HTTP_COOKIE</td>
<td>5720</td>
<td>PHPSESSID=ter3pp6gjgf1isggk31outa984, SS=Q0=cG9ybRhbGsuY29t; PREF=ID=d2e ...</td>
</tr>
<tr>
<td>HTTP_REFERER</td>
<td>992288</td>
<td>919723239170,919891354251,919718404920,989353431333,639088619980,919702020 ...</td>
</tr>
<tr>
<td>HTTP_UP_CALLING_LINE_ID</td>
<td>640</td>
<td>841214395386,27794646839,27721946573,966542014411,27726663157,27825321652,2 ...</td>
</tr>
<tr>
<td>HTTP_X_NETWORK_INFO</td>
<td>3712</td>
<td>GPRS,919877777210,airtelwap.com,unsecure,3G,10.36.94.187,447964548446,194.33.2 ...</td>
</tr>
<tr>
<td>HTTP_WAP_NETWORK_INFO</td>
<td>26</td>
<td>10.16.31.253,GPRS,919740016108,airtelwap.com,unsecure,GPRS,91987235655,airtelw ...</td>
</tr>
<tr>
<td>HTTP_X_NOKIA_MSISDN</td>
<td>956</td>
<td>919723239170,919891354251,919718404920,989353431333,639088619980,919702020 ...</td>
</tr>
<tr>
<td>HTTP_X_UA_CALLING_LINE_ID</td>
<td>640</td>
<td>841214395386,27794646839,27721946573,966542014411,27726663157,27825321652,2 ...</td>
</tr>
<tr>
<td>HTTP_HUAWEI_Networks</td>
<td>42</td>
<td>GPRS,919877777210,airtelwap.com,unsecure,3G,10.36.94.187,447964548446,194.33.2 ...</td>
</tr>
<tr>
<td>HTTP_IMSI</td>
<td>9</td>
<td>919723239170,919891354251,919718404920,989353431333,639088619980,919702020 ...</td>
</tr>
<tr>
<td>HTTP_X_LOGDIGGER</td>
<td>1</td>
<td>logme=0&amp; ...</td>
</tr>
<tr>
<td>HTTP_RIM_DEVICE_EMAIL</td>
<td>1</td>
<td>...</td>
</tr>
</tbody>
</table>

'10
Some abbreviations

- **MSISDN**
  - Mobile Subscriber Integrated Services Digital Network Number
    - A mobile phone number

- **IMSI**
  - International Mobile Subscriber Identity
    - Unique SIM card ID

- **IMEI**
  - International Mobile Equipment Identity
Results

• Some highlights from my logs...

• BIG FAT disclaimer
  – These are just “random” examples
    • Examples that contain interesting data
  – I don't want to discredit any operator!
  – These are just facts!
Rogers (Canada)

HTTP_USER_AGENT: MOT-V3re/0E.43.04R MIB/2.2.1 Profile/MIDP-2.0 Configuration/CLDC-1.1 UP.Link/6.5.1.0.0

HTTP_X_UP_UPLINK: rogerspush.gprs.rogers.com

HTTP_X_UP_SUBNO: 1239769412-53731234_rogerspush.gprs.rogers.com

HTTP_X_UP_LSID: 120472093XX <-- MSISDN
HTTP_USER_AGENT: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.7) Gecko/20060909 Firefox/1.5.0.7 Novarra-Vision/6.9

HTTP_XDEVICE_USER_AGENT: LG/U450/v1.0 Profile/MIDP-2.0 Configuration/CLDC-1.1 Novarra /5.2.25.1.12lgu450(J2ME-OPT)

HTTP_X_MOBILE_GATEWAY: Novarra-Vision/6.9 (3IT; Server-Only)

HTTP_X_SDC_NOVARRA_TRIAL_FLAG: 0
HTTP_X_SDC_NOVARRA_END_DATE: 31/12/2100 23:59
HTTP_X_H3G_MSISDN: 3939249093XX
HTTP_X_H3G_PARTY_ID: 1017030640 <--- ???
HTTP_USER_AGENT: Nokia6212 classic/2.0 (05.16)
Profile/MIDP-2.1 Configuration/CLDC-1.1

HTTP_X_UP_SUBNO: 1233936710-346677XXX <- customer id?

HTTP_X_UP_CALLING_LINE_ID: 49152285242XX <- my number!

HTTP_X_UP_SUBSCRIBER_COS: System, UMTS, SX-LIVPRT, A02-MADRID-1BILD-VF-DE, Vodafone, Prepaid, Rot
HTTP_USER_AGENT: Mozilla/5.0 (SymbianOS/9.3; U; ... 

HTTP_X_NOKIA_MUSICSHOP_BEARER: GPRS/3G 
HTTP_X_NOKIA_REMOTESOCKET: 10.45.28.146:12990 
HTTP_X_NOKIA_LOCALSOCKET: 193.35.132.102:8080 
HTTP_X_NOKIA_GATEWAY_ID: NBG/1.0.91/91 
HTTP_X_NOKIA_BEARER: 3G 
HTTP_X_NOKIA_MSISDN: 4479801754XX 
HTTP_X_NOKIA_SGSNIPADDRESS: 194.33.27.146 

HTTP_X_NETWORK_INFO: 3G, 10.45.28.146, 4479801754XX, 194.33.27.146, unsecured 

HTTP_X_ORANGE_RAT: 1
HTTP_USER_AGENT: SonyEricssonW760i/R3DA
                Browser/NetFront/3.4 Profile/MIDP-2.1
HTTP_MSISDN: 9725077690XX
HTTP_IGCLI: 9725077690XX
HTTP_IMEI: 35706702308316XX
HTTP_IMSI: 4250300200079XX
HTTP_NETWORK_ID: pcl@3g
REMOTE_ADDR: 193.41.209.2
HTTP_SGSNIP: 91.135.96.33
Zain (Nigeria)

- Zain is a South African operator
  - This is a customer from/in Nigeria (using my Maemo repository)

HTTP_USER_AGENT: Debian APT-HTTP/1.3
HTTP_VIA: Jataayu CWS Gateway Version 4.2.0.CL_P1 at wapgw2.celtel.co.za

HTTP_X_ROAMING: Yes

HTTP_X_UP_CALLING_LINE_ID: 23480845524XX <-- MSISDN

HTTP_X_APN_ID: wap.ng.zain.com

HTTP_X_IMSI: 6212032203124XX
HTTP_COOKIE:
User-Identity-Forward-msisdn = 9194554314XX
Network-access-type = GPRS
Charging-id = 123792550
Imsi = 4045541600364XX
Accounting-session-id = DAF841A20760ECi
Charging-characteristics = Prepaid
Roaming-information = no_info
... boring stuff striped ...

HTTP_MSISDN: 10.184.0.48 9194554314XX

HTTP_USER_AGENT: Nokia1680c-2/2.0 (05.61) Profile/MIDP-2.1
Where does the data come from

- The phone doesn't have all the data that I find in the logs
  - i.e. the SUBNO
- Data must be added by network
- Best guess is the HTTP proxy/gateway at the operator
  - Theory is supported by the fact that I don't have any log entries from smart phones that don't have a pre-configured proxy (such as the iPhone or Android devices)
Data is added by the web proxy
Mobile phone web proxies

• Reasons:
  – Caching
  – Content compression: page + images
  – Optimization (change page layout for mobile browser)
  – Special mobile mini-browsers

• Types:
  – Explicit
  – Transparent
Collected Data

- **Common**
  - MSISDN
  - IMSI, IMEI
  - APN (access point name)
  - Customer/Account ID
- **Rare**
  - Roaming status
  - Account-type: post-paid or pre-paid
We have data, now what?

• Unique IDs can be used for tracking
  – MSISDN, IMSI, IMEI, customer ID, …
  • Fact: getting a new phone doesn't change your phone number → user tracking++

• Phone number (MSISDN)
  – Reverse lookup, get the name of your visitors
  – SMS spam

• Hopefully no one uses “secret” APNs for VPN-like network access anymore
# MSISDNs collected by country

![Graph showing the number of MSISDNs collected by country](image.png)

- Count
- Countries: Algeria, Australia, Bangladesh, Bosnia, Brazil, Brunei, China, Ecuador, Egypt, Fiji, Finland, Germany, Guadeloupe, Guyana, India, Iran, Ireland, Israel, Italy, Ivory Coast, Jordan, Kuwait, Kyrgyzstan, Libya, Malawi, Malaysia, Mauritius, Montenegro, Nepal, New Zealand, Nigeria, Pakistan, Paraguay, Peru, Philippines, Romania, Saudi Arabia, Singapore, South Africa, Sri Lanka, Thailand, Tunisia, Turkey, UK, USA/Canada, Ukraine, Uruguay, Uzbekistan, Venezuela, Vietnam
Why the MSISDN…

• …is not easy to find after all and why this privacy breach hasn't gotten any real attention yet

• Many different headers
  – Some headers seem operator and equipment manufacturer specific
The MNO privacy checker

- Website to check your mobile network operator for HTTP header privacy leaks
  - http://www.mulliner.org/pc.cgi
Conclusions

• We have shown that many mobile operators around the world leak private data of their customers through adding HTTP headers via proxies
• This data leakage is totally unnecessary
  – Operators
    • Need to fix their proxies
    • Make their contractors fix their proxies
Q & A

• Thank you for listening!
• Questions?

• Contact:
  http://www.sec.t-labs.tu-berlin.de
  collin@sec.t-labs.tu-berlin.de