Weaving Applications into the Network Fabric
The Transformational Challenge
11-14 October 2010, Berlin, Germany
icin 2010

Session 2B

Security & Privacy

Privacy Leaks in Mobile Phone Internet Access

Collin Mulliner

Security in Telecommunications

Technische Universität Berlin and

Deutsch Telekom Laboratories

SECT Security IN TELECOMMUNICATIONS

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:

Profilname	[redacted] Mobilportal
APN (Zugangspunkt)	access.[redacted].de
Benutzername	nicht notwendig
Passwort	nicht notwendig
Proxy IP-Adresse/Gateway-Server	[redacted]
Proxy (Port-Nummer für WAP 2.0)	80
Proxy (Port-Nummer für WAP 1.x)	9201
Verbindungssicherheit	aus
Startseite (Homepage)	wa[redacted]de

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

Header Name	Content
HOST	mulliner.org
USER-AGENT	Mozilla/5.0 (X11; U; Linux armv7l; en-US; rv:1.9.2a1pre) Gecko/20090928 Firefox/3.5 Maemo Browser 1.4.1.15 RX-51 N900
ACCEPT	image/png,image/*;q=0.8,*/*;q=0.5
ACCEPT-LANGUAGE	en
ACCEPT-ENCODING	*
ACCEPT-CHARSET	ISO-8859-1,utf-8;q=0.7,*;q=0.7
REFERER	http://mulliner.org/blog/
X-UP-SUBNO	1233936xxx-346677xxx
X-UP-FORWARDED_FOR	10.248.240.209
X-FORWARDED_FOR	10.248.240.209
X-UP-CALLING-LINE-ID	491522852xxxx
X-UP-SUBSCRIBER-COS	System,UMTS,SX-LIVPRT,A02-MADRID-1BILD-VF-DE,Vodafone,Prepaid, Rot
MAX-FORWARDS	10
VIA	1.1 rn2wwpsv161-ncl-0.wwp.vodafone.de
CONNECTION	close
REMOTE_ADDR	139.7.146.41

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

Header	Count	Value(s)
HTTP_X_WAP_FH_SUBSCRIBER_INFO	64	,IP=10.142.249.144, MSISDN=60133972810, APN=post.wap.celcom3g,IP=10.163.132.2
HTTP_X_MSP_MSISDN_ENC	5	,,X-MSP-MSISDN="R1yqtSXp6G5E/QB6L1u4Kg==",X-MSP-MSISDN="R1yqtSXp6G5E/QI
HTTP_X_HUAWEI_AUTHMETHOD	75	,MSISDN
REQUEST_URI	2105754	
HTTP_COOKIE	5720	,,PHPSESSID=ter3pp6gjgf1isggk31oota984,SS=Q0=cG9ybnRhbGsuY29t; PREF=ID=d2e CFTOKEN=10704760; CFGLOBALS=urltoken%3DCFID%23%3D43269011%26CFTOKEN %23hitcount%3D2%23cftoken%3D10758988%23cfid%3D36926260%23,PHPSESSID=bcc __utmb=213499286.1.10.1231669929; _csuid=4852ba93219c4963; zdPopup=1; __utmc=2
HTTP_REFERER	992288	
HTTP_X_NOKIA_MSISDN	956	,,919723239170,919891354251,919718404920,989353431333,639088619980,919702020
HTTP_X_UP_CALLING_LINE_ID	640	,841214395386,27794646839,27721946573,966542014411,27726663157,27825321652,2
HTTP_X_NETWORK_INFO	3712	,GPRS,919867777210,airtelwap.com,unsecured,3G,10.36.94.187,447964548446,194.33.2 10.16.31.253,GPRS,919740016108,airtelfun.com,unsecured,GPRS,919897235655,airtelw
HTTP_WAP_NETWORK_INFO	26	,mUserAlias:391983428950,mUserAlias:326098535988,mUserAlias:374768380228
HTTP_X_NOKIA_IMSI	33	,234334404264987,310260253349708,405799008186537,404870015671975,3102604937
HTTP_X_HUAWEI_IMSI	42	,617010001704747,617010011459391,274113090270788,641220001114181,6170100011
HTTP_IMSI	9	,425030020061487,425030020007928
HTTP_X_LOGDIGGER	1	,logme=0&
HTTP_RIM_DEVICE_EMAIL	1	,[redacted]va@unitos.com

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
```

H3G S.p.a. (Italy)

```
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_X_DEVICE_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     <--- ???
```

Vodafone/BILDmobil (Germany)

```
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
```

Orange (UK)

```
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
```

Pelephone (Israel)

```
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:                    621032203124XX
```

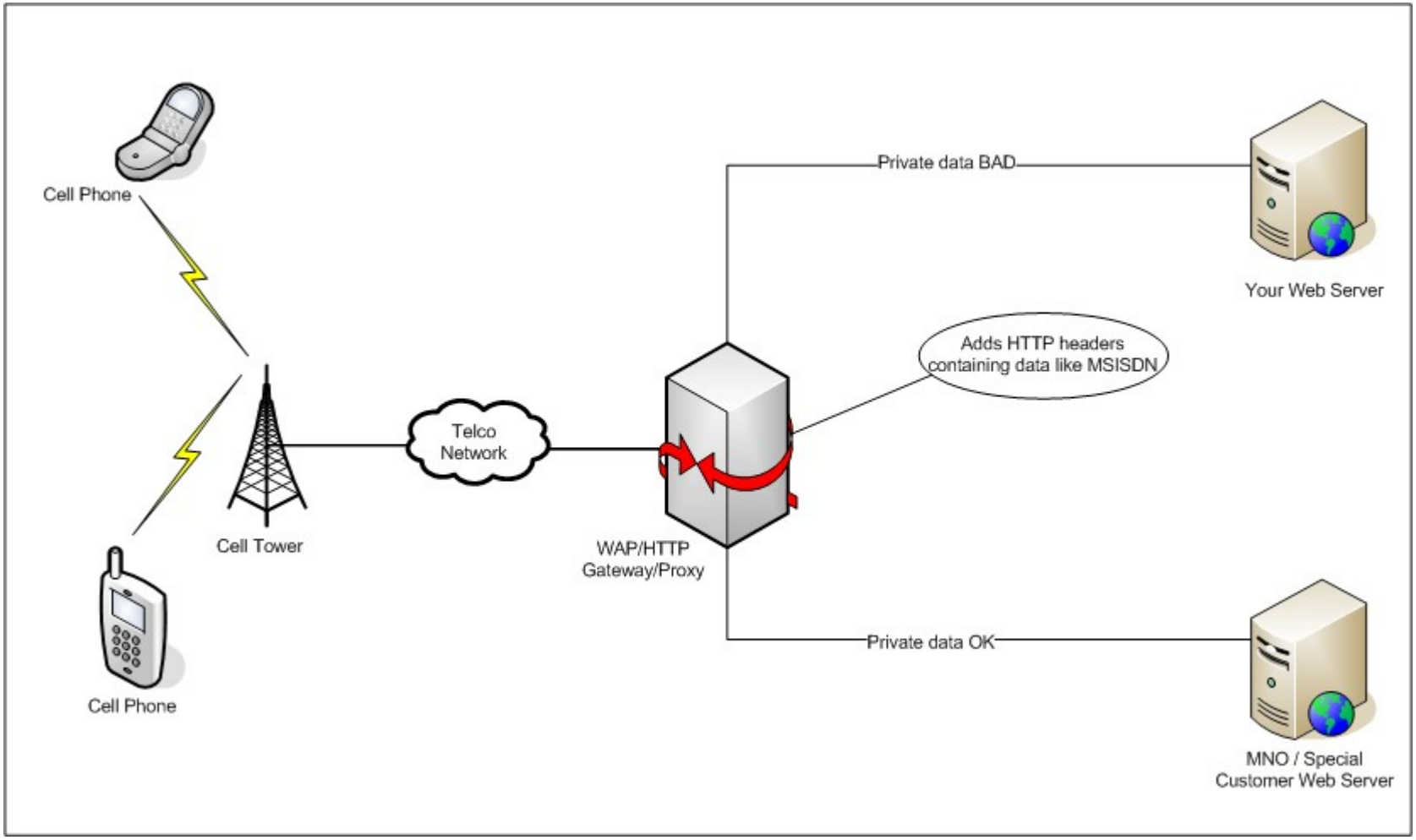
Bharat Sanchar Nigam Ltd (India)

```
HTTP_COOKIE:
 User-Identity-Forward-msisdn = 9194554314XX
 Network-access-type = GPRS
 Charging-id = 123792550
 Imsi = 404554160036 4XX
 Accounting-session-id = DAF841A20760EC
 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

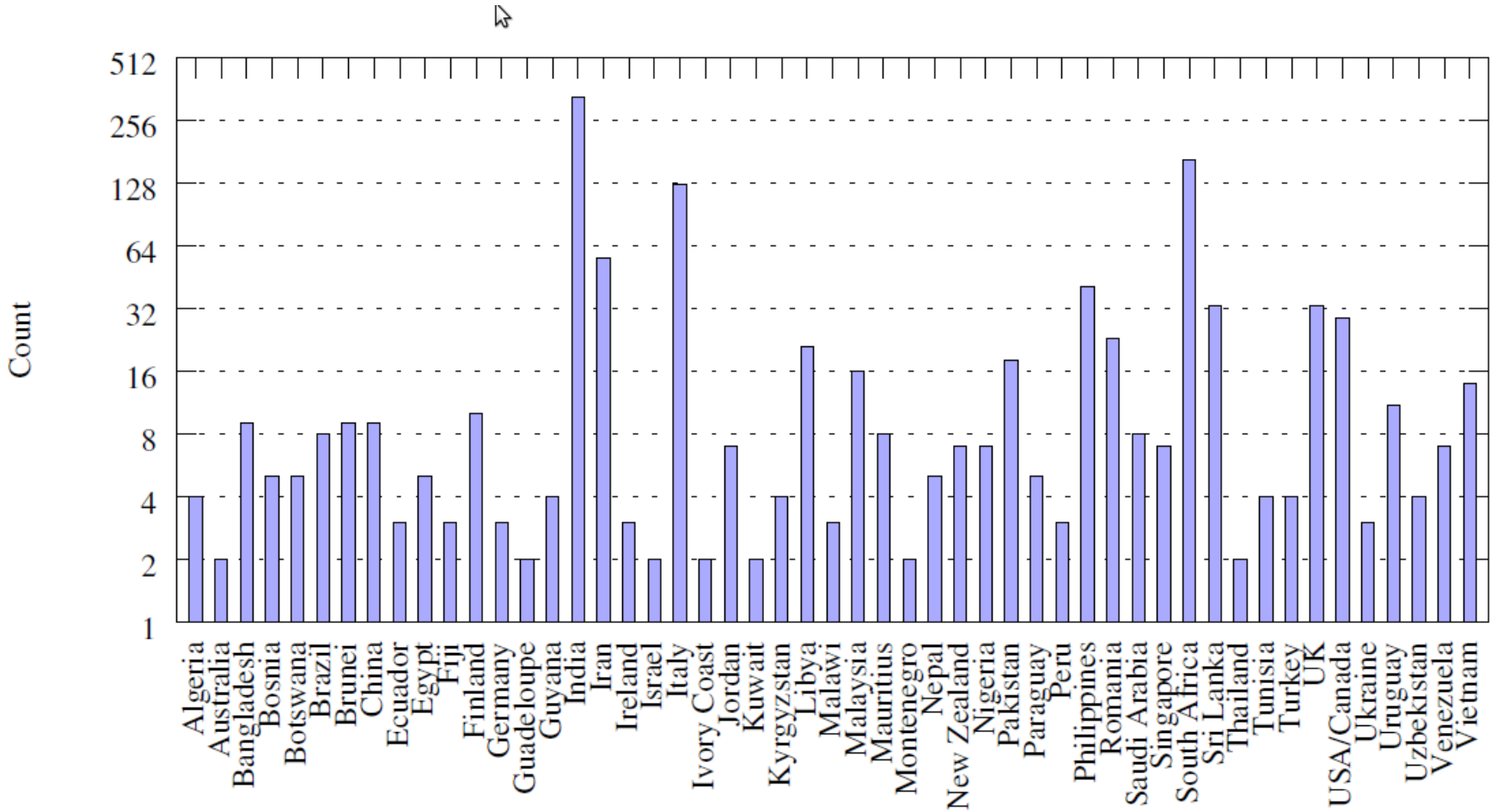
Collected Data

- 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



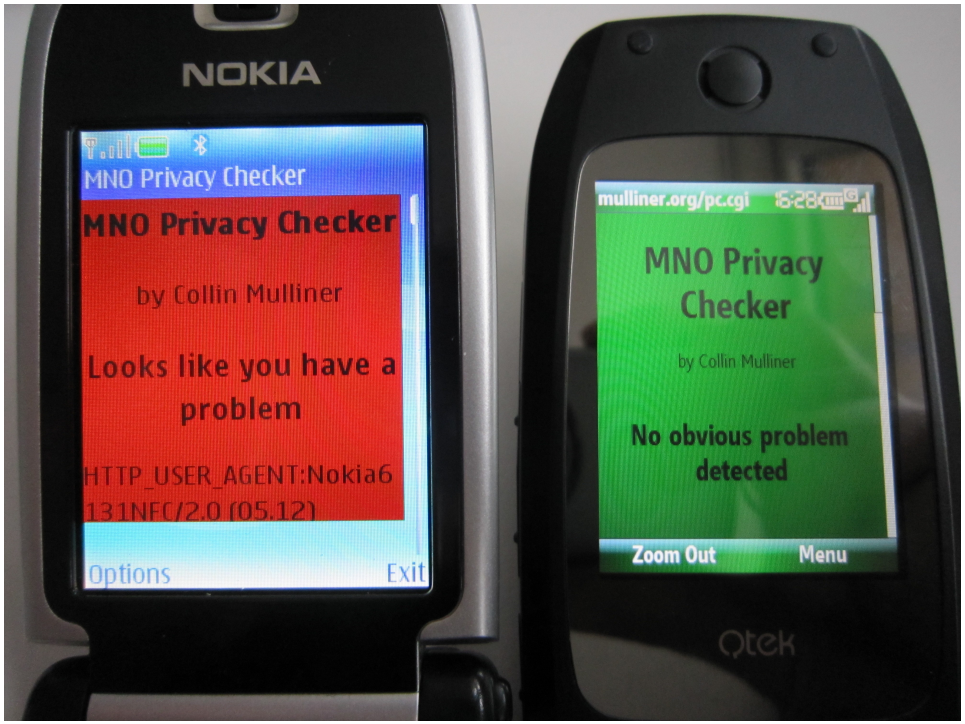
Why the MSISDN...

- ...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

Header Name	Count
X-UP-CALLING-LINE-ID	324
X-NOKIA-MSISDN	238
X-MSISDN	203
X-H3G-MSISDN	125
MSISDN	106
COOKIE	67
_RAPMIN	41
X-WAP-FH-SUBSCRIBER-INFO	16
X-FH-MSISDN	16
X-HTS-CLID	16
X-MSP-CLID	15
X-UP-LSID	12
X-JINNY-CID	7
X-NETWORK-INFO	5
X-MSP-MSISDN	4
X-NX-CLID	4
X-WAP-MSISDN	3
IGCLI	2
X-WSB-CLI	2
X-ORANGE-CLI	2

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