Mobile Phones, Crypto and Mass Surveillance

Stig F. Mjølsnes
Department of Information Security and Communication Technology

Workshop on Crypto vs Mass Surveillance, Nov. 14, 2016

NTNU

Secret surveillance of Norway's leaders detected

Members of parliament and the prime minister of Norway are being monitored by means of secret espionage equipment.

Andreas Bakke Foss , Per Anders Johansen , Fredrik Hager-Thoresen

Norway's major secrets are being administered here, right in the centre of Oslo. A number of the most important state institutions are situated within a radius of one kilometer: The Prime minister's office, the Ministry of defence, Stortinget (parliament) and the central bank, Norges Bank. Ministers, state secretaries, members of parliament, state officials, business executives and other essential staff engaged in protecting the nation's security, our military and our oil wealth – totalling more than 6000 billion kroner (NOK) - are working within this area.

Aftenposten,
December 16, 2014

http://mm.aftenposten.no/stortinget-og-statsministeren-overvakes/

Aftenpostens kartlegging av mobilovervåking i Oslo

2014-2015

Per Anders Johansen per.anders.johansen@aftenposten.no
Andreas Bakke Foss andreas.bakke.foss@aftenposten.no
Fredrik Hager-Thoresen fredrik.hager-thoresen@aftenposten.no

Per A. Johansen

"Baseband firewall"

Gordon McKay

delma
Mobile Communications Security

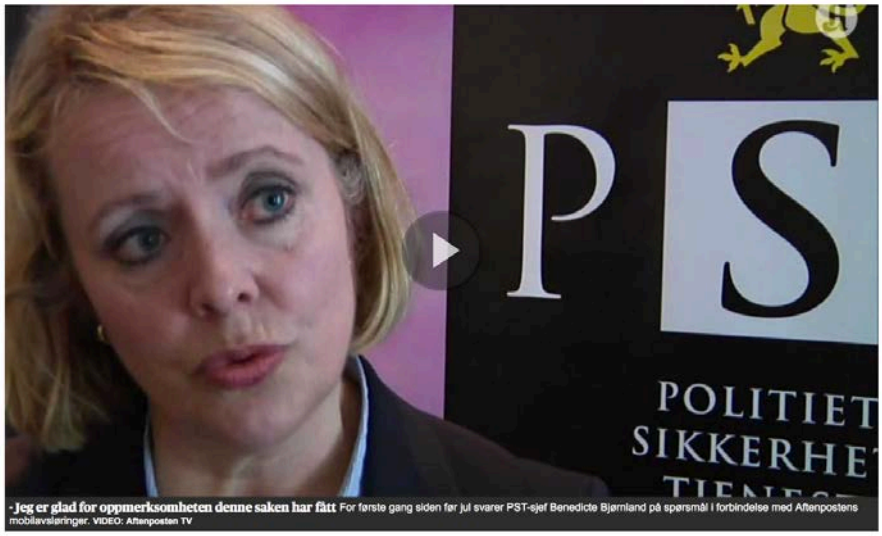
PST: Veldig mange aktører kan tenkes å stå bak falske basestasjoner

ANDREAS BAKKE FOSS | PER ANDERS JOHANSEN | PER BYHRING | FREDRIK HAGER-THORESEN

PST Norwegian Police Security Service

- Det er mange som har en intensjon om å få tilgang til andres mobiltrafikk, sier Arne Christian Haugstøyl, seksjonsleder ved forebyggende avdeling i Politiets sikkerhetstjeneste (PST).

NTNU



- Jeg er glad for oppmerksomheten denne saken har fått For første gang siden før jul svarer PST-sjef Benedicte Bjørnland på spørsmål i forbindelse med Aftenpostens mobilavsløringer. VIDEO: Aftenposten TV

PST: Aftenpostens funn har naturlige forklaringer

For første gang siden før jul svarte Politiets sikkerhetstjeneste på spørsmål om Aftenpostens mobilavsløringer.

Aftenposten hired Counter-intelligence expert Gordon McKay

- Vi ønsket en seriøs diskusjon om dataene med PST. Det viste seg at de ikke var interessert i det. Vi synes det er rart at så mange i Norge ble overrasket over at vi fant spor etter IMSI-catchere i Oslo. Slikt utstyr brukes i økende grad i en rekke ulike overvåkingsverktøy som er åpent til salgs, sier Gordon McKay, leder i sikkerhetsselskapet Delma.

FOTO: Per Anders Johansen

Gordon McKay mener det foregikk ren spionasje i Oslo før jul. Han er ikke overrasket over svaret og kritikken fra PST.

SOON MORE WILL BE REVEALED….

Forskere, professorer og eksperter har vurdert datamaterialet og den nye rapporten om mobilovervåking.

E-tjenesten: - Ikke bevis for falske basestasjoner

STINE BARSTAD · ANDREAS BAKKE FOSS
OPPDATERT: 25.JUN. 2015 10:10 | PUBLISERT: 24.JUN. 2015 18:03

- Våre analyser er fullt og helt i samsvar med PSTs konklusjoner i saken, sier generalløytnant Kjell Grandhagen i Etterretningstjenesten.
FOTO: Pedersen, Terje

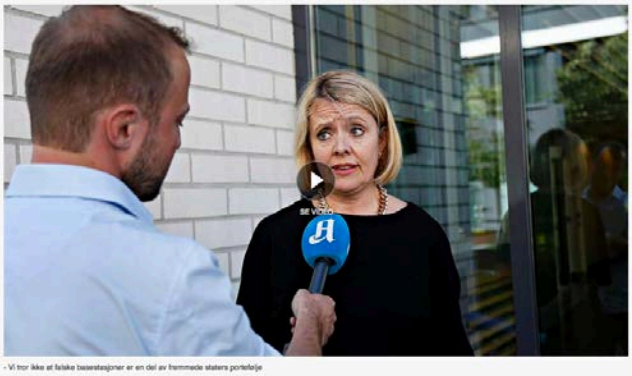
Etterretningstjenesten støtter PST i konklusjonen om at det ikke er noe som tyder på at falske basestasjoner er blitt brukt i Oslo.

NTNU

PST henlegger sak om falske basestasjoner

ANDREAS BAKKE FOSS · ANDREAS SLETTHOLM · NINA SELBO TORSET · EIVIND NICOLAI LAURITSEN
OPPDATERT: 02.JUL. 2015 17:59

July 2015



- Vi tror ikke at falske basestasjoner er en del av fremmede staters portefølje

Politiets sikkerhetstjeneste (PST) konkluderer med at det ikke finnes bevis for bruk av falske basestasjoner eller IMSI-fangere i Oslo.

NTNU

Eldbjørg Løwer, leder i Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, vil gå nye runder om utvalgets sikkerhetsrutiner etter Aftenpostens avsløringer. FOTO: Monica Strømdahl

Mobilovervåkingssaken:

EOS-utvalget: Skal granske PSTs bruk av basestasjoner

Stortingets EOS-utvalg undersøk
Oslo på lovlig måte.

Andreas Bakke Foss , Per Anders Joh

Oppdatert: 08.apr. 2015 17:00

Del Tweet E-post Lagre artikkelen i leselisten

Norges I
end

The Norwegian Parliamentary Intelligence Oversight Committee

Vi er ikke ferdig med denne saken, og kommer tilbake med grundig oppfølging når vi er ferdig, sa EOS-utvalgets leder Eldbjørg Løwer da hun

TNU

Få dager etter Aftenpostns avsløringer innkalte Nasjonal kommunikasjonsmyndighet (NKom) teleselskapene og Nasjonal sikkerhetsmyndighet (NSM) til krisemøte. FOTO: Junge, Heiko

Revidert nasjonalbudsjett: Skal jakte mer på falske basestasjoner

Regjeringen bevilger mer penger for å gjøre Nasjonal kommunikasjonsmyndighet i stand til å avdekke falske basestasjoner.

Per Anders Johansen, Andreas

Oppdatert: 12.mai. 2015 12:49

Del Tweet

Før jul avslørte Af
var i bruk flere ste

Vi brukte avansert kontraetterretningsutstyr, som benyttes til å oppdage mobiloverv åkingsutstyr i en rekke land.

Også Nasjonal sikkerhetsmyndighet og PST gjorde egne undersøkelser

May 2015 Revised national budget:
Funds allotted to track down the false basestations

Bevilger 11,6 millioner for å avdekke falske basestasjoner

Aftenposten Torsdag 8. oktober 2015

ANDREAS BAKKE FOSS
OPPDATERT: 07.OKT. 2015 18:52

OVERVÅKING

12 millioner til avdekking

Regjeringen vil bruke 12 millioner kroner på å styrke Nasjonal sikkerhetsmyndighets (NSM) arbeid med å avdekke falske basestasjoner.

I revidert statsbudsjett ble det satt av 2,5 millioner kroner til NSMs arbeid.

Aftenposten oppdaget i desember i fjor det som trolig var flere falske basestasjoner rundt sentrale bygninger i Oslo. NSM og PST uttalte da at avisens funn høyst sannsynlig var reelle. Men senere sa PST at det var «naturlige forklaringer» bak målingene og funnene, og NSM har ikke vilket si hva deres funn gikk ut på. (NTB)

12 millions to buy Mobile Countersurveillance equipment

Justis- og beredskapsminister Anders Anundsen i Stortinget 7. januar i år da han redegjorde for falske basestasjoner etter Aftenpostens sine saker. Nå bevilger regjeringen nesten 12 millioner kroner til å kjøpe nytt utstyr som kan avsløre falske basestasjoner.

FOTO: Jan T. Kjeldal

- Viser at regjeringen tar Aftenpostens funn på alvor, sier medlem av justiskomiteen.

Pengene skal gå til en engangsinvestering i utstyr på seks millioner kroner og årlige driftsutgifter på 5,6 millioner kroner.

SISTE ARTIKLER OM

mobilspionasje:

12.12.2014 - UTVALGT SAK:
Stortinget og statsministeren overvåkes

14.12.2014 - UTVALGT SAK:
Spionutstyr plassert i Norges fremste finansmiljø

100 artikler om #mobilspionasje:

12.5.2015
Revidert nasjonalbudsjett: Skal jakte mer på falske basestasjoner

5.5.2015
Tajik ber Anundsen tydeliggjøre ansvarsforholdene om mobilsikkerhet

8.4.2015
EOS-utvalget: Skal granske PSTs bruk av basestasjoner

27.3.2015
Aftenposten mener: Arbeidet med mobilsaken må fortsette

26.3.2015
Harald Stanghelle: Ekspertenes kamp

26.3.2015
PST avviser mobilovervåking - slik svarer spionjegerne

26.3.2015
Aftenposten vil fortsette å skrive om mobilovervåkning

26.3.2015
PST: Aftenpostens funn har naturlige forklaringer

26.3.2015
PST avviser Aftenpostens mobilavsløringer

21.3.2015
Så enkelt bryter han seg inn på mobilen din

VIS 5 TIL VIS ALLE

MORE THAN 100 ARTICLES

Aftenposten Torsdag 2. juli 2015

NTNU studenten valgte en noe uvanlig masteroppgave.

Bygget spionutstyr på universitetet

MOBILSPIONASJE

PER ANDERS JOHANSEN
ANDREAS BAKKE FOSS

Trondheim/Oslo

Torjus Bryne Retterstøl (24) bygget sin egen falske basestasjon som lokket til seg medstudentenes mobiltelefoner.

– Vår professor Stig Mjølsnes foreslo at vi skulle prøve å lage en falsk basestasjon ved hjelp av en radio styrt av programvare. Jeg ble interessert i temaet etter å ha lest Aftenpostens saker før jul i fjor, og bestemte meg for å prøve, sier Torjus Bryne Retterstøl.

Han har akkurat levert sin masteroppgave etter fem år ved Norges teknisk-naturvitenskapelige universitet (NTNU) i Trondheim.

24-åringen startet med å gjøre research og lære mer om hva falske basestasjoner er.

– Deretter satt vi opp programvaren og hardwaren, og konfigurerte det som en falsk basestasjon. Det er relativt enkelt, sier han.

– Hva må til for lage en falsk basestasjon?

– Du trenger grunnleggende kunnskap om GSM-nettet og bør være garnske datakyndig. I tillegg trenger man den nødvendige hardwaren. Jeg brukte en programvarebasert radio til rundt 20.000 kr, sier han.

Utførte mobilangrep

Retterstøl instierte studenter og faglærere til å ta med seg sin mobiltelefon og være med på et halvtimes IMSI-catcher-eksperiment. I auditoriet på NTNU klarte Retterstøl å lokke cirka 30 medstudenters mobiltelefoner til å koble seg til den falske basestasjonen.

– Hva kunne du gjøre med den falske basestasjonen?

– Jeg utførte tjenestenekt-angrep, hvor mobilene til medstudentene koblet seg til min basestasjon. Da mistet de dekningen i det ekte mobilnettet, selv om mobilene fremsto som om de var koblet til Netcom eller Telenor. I tillegg langet den falske basestasjonen opp den unike identifikasjonen til mobiltelefonene som koblet seg til. Dette kan brukes til å overvåke hvem som befinner seg i nærheten.

– At mobilene våre automatisk kan koble seg til falske basestasjoner, er et stort sikkerhetshull. Jeg kunne tatt med den falske basestasjonen under armen og satt den opp hvor som helst, for eksempel i sentrum av Trondheim, sier Retterstøl.

Professor Stig Mjølsnes bekrefter eksperimentet, som ble gjennomført på initiativ og med aktiv deltagelse av ham.

- Lett å gjøre angrep mot GSM

Han sier en av de viktigste lærdommene av arbeidet er at GSM-nettet er veldig sårbart for overvåking.

– Det er veldig lett å gjøre angrep mot GSM, og du trenger ikke mye kunnskap. Dessuten er det også veldig rimelig.

– Det mest spennende var å bygge min egen IMSI-catcher og eksperimentere med den. Da lærte jeg mye om hvordan mobilteknologien fungerer.

Fikk Aftenpostens data

NTNU-miljøet er et av flere uavhengige forskningsmiljøer som har fått tilgang til datamateriale og rapporter fra Aftenpostens undersøkelser.

– At mobilene våre automatisk kan koble seg til falske basestasjoner, er et stort sikkerhetshull, sier Torjus Bryne Retterstøl. Her sammen med professor ved NTNU Stig Mjølsnes.
FOTO: OLE MARTIN WOLD

We Built Our Own IMSI-catcher!

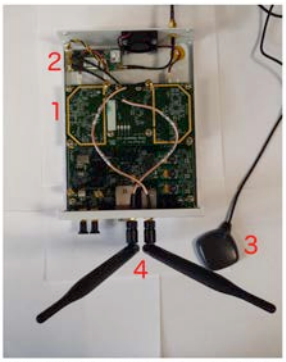
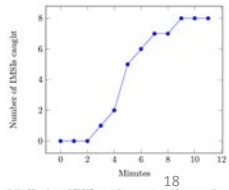


Figure 4.2: The USRP N200 with daughterboard, GPSDO kit, GPS antenna and two VERT900 antennas installed. In the figure, 1 is the daughterboard installed on top of the motherboard, 2 is the GPSDO kit, 3 is the GPS antenna connected to the GPSDO kit and 4 is the two VERT900 antennas.

Listing 5.4: Spoofing a Telenor BTS with OpenBTS

```
$ OpenBTS> config GSM.Identity.MCC 242
$ OpenBTS> config GSM.Identity.MNC 01
$ OpenBTS> config GSM.ShortName Telenor
$ OpenBTS> config GSM.Radio.C0 56
$ OpenBTS> config GSM.Identity.LAC 1111
```



re 5.5: Number of IMSIs caught over time when spoofing NetCom

A Mobile Perspective

1. NMT, in service from 1981 (Iceland joined in 1986)
   ”analog”
2. GSM first spec. 1987, operative from 1991.
   ”circuit switched”
3. UMTS first spec. 1999, operative from 2002
   ”packetswitched”
4. LTE first spec. 2008, operation from 2010
   ”all IP”
5. ”5G” around 2020?

Mobile Network Security Requirements

1. **Access control**
   - Identification of subscription/user
2. **Confidentiality**
   - Secure voice, data and sensitive signaling information against eavesdropping on the radio link
3. ***Privacy***
   - *Protect against identifying or linking calls by the same SIM by radio channel eavesdropping*
4. **Usability**
   - The security mechanisms must not reduce the usability of the system

Mobile Security Mechanisms

For each subscription in SIM and the home network:
IMSI: 15 digits identity
K_{IMSI} : permanent 128 bits crypto-key

1. Mutual Authentication
   - Challenge-response + Auth.Code protocol
2. Radio Link Encryption
   - Symmetric encryption with derived keys
3. Privacy
   - temporary identities TMSI (32 bits random)

The Privacy Mechanism

- *Permanent* unique **IMSI**, ideally sent only
  - when the SIM is used for the first time
  - when there is data loss at the network
- *Temporary* random **TMSI**
  - Provided over the authenticated encrypted radio link
  - Generated where? Renewed when and how often?

TMSIs prevent passive monitoring attack

"IMSI-catchers"

- **Active attacker devices** breaking the logic of radio communication protocols
- Hijack and block services
- "Man-in-the-middle" adversarial actions
- Is this "backdoor" a feature or security bug?
- Works for 2G, 3G, and 4G/LTE !

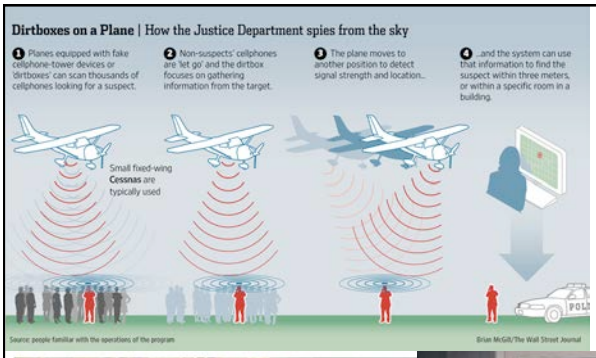
Easy 4G/LTE IMSI Catchers for Non-Programmers

Stig F. Mjølsnes and Ruxandra F. Olimid

Department of Telematics, NTNU, Norwegian University of Science and Technology, Trondheim, Norway
sfm@item.ntnu.no, ruxandra.olimid@ntnu.no

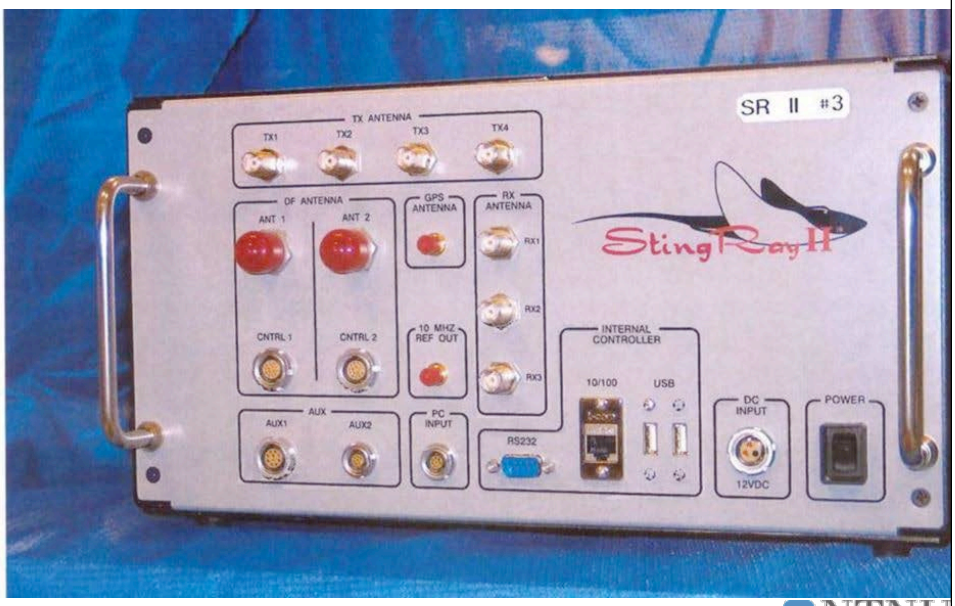
Abstract IMSI Catchers are active devices that act against the privacy of subscribers in commercial mobile networks, with high impact on both user and network side, because of credibility and financial looses. Recently, IMSI Catchers have been proved feasible in LTE networks by using modified versions of open source software projects. We now demonstrate their feasibility at large scale: low-cost LTE IMSI Catchers can be built by non-programmes, using commercial out-of-the-shelf hardware and unmodified publicly available software. Our IMSI Catcher collects the IMSIs of the targeted mobile operator within a specific area in a few seconds and denies access of subscribers to the commercial network.

Keywords: LTE security, IMSI Catcher, Denial-of-Service

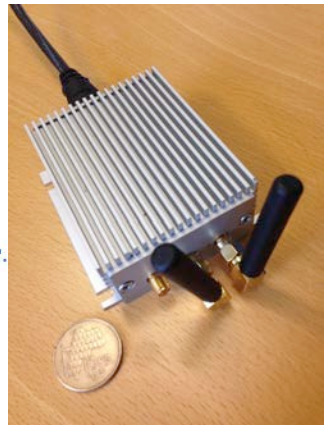

Dirtboxes on a Plane | How the Justice Department spies from the sky
1 Planes equipped with fake cellphone-tower devices or 'dirtboxes' can scan thousands of cellphones looking for a suspect.
2 Non-suspects' cellphones are 'let go' and the dirtbox focuses on gathering information from the target.
3 The plane moves to another position to detect signal strength and location..
4 ..and the system can use that information to find the suspect within three meters, or within a specific room in a building.
Small fixed-wing Cessnas are typically used
Source: people familiar with the operations of the program
Brian McGill/The Wall Street Journal


These are fake mobile base stations, whose only purpose is electronic surveillance and tracking of people's mobile phones, nearby.


PARKERING FORBUDT
INN OG UTKJØRING


SR II #3
TX ANTENNA
TX1
TX2
TX3
TX4
DF ANTENNA
ANT 1
ANT 2
CNTRL 1
CNTRL 2
GPS ANTENNA
10 MHZ REF OUT
RX ANTENNA
RX1
RX2
RX3
StingRay II
INTERNAL CONTROLLER
10/100
USB
RS232
AUX
AUX1
AUX2
PC INPUT
DC INPUT
12VDC
POWER

Figur 49 Det russiskproduserte mobilovervåkingsutstyret "White Russian".



Ettus URSRP B200mini

Over 130 different mobile surveillance equipment manufacturers

Smith Myers (UK) • Harris Corp (USA) • Rohde Schwartz (Tyskland) • Cell Antenna (USA) • Nice Systems (Israel) • CellXion (UK) • Verint (USA) • NeoSoft (Sveits) • Shogi/StratigN (India) • Thales – SUSI---systemet (Frankrike) • EXFO – blant annet det tidligere finskproduserte NetHawk. • White Russian (Russiskprodusert og til salgs via Ukraina/Sveits).

HTTP://RESOURCES.INFOSECINSTITUTE.COM/STINGRAY-TECHNOLOGY-GOVERNMENT-TRACKS-CELLULAR-DEVICES/

http://www.rayzoneg.com/en.piranha.html

WEB COMMERCIAL EXAMPLE

Piranha - 2G, 3G, and 4G IMSI Catcher

Nowadays, people always carry their phones with them. Having intelligence on a particular person's phone equates to managing info on a person. The Piranha system enables an organization to gather phone identity (IMSI, IMEI or MSISDN), while delivering advance tools to utilize the gathered information and to manipulate the phones.

The Uses of IMSI-catchers

Monitoring

- Mass-surveillance of individuals in a geographic location/area
- Observing a link between person, mobile, and IMSI
- Trace people with known IMSI
- Monitoring people movements
  - Example: entrance/exit of a building or area
- Communication eavesdropping

Active Interception

- Message and call generation
- Reconfiguring the mobile's software and SIM (baseband processor backdoors)
- Denial-of-service for network services/communications
- ….

Denial-of-Service

A dilemma for police use

- An IMSI-catcher will block regular network communication and services
- Including emergency numbers
  110, 112 and 113

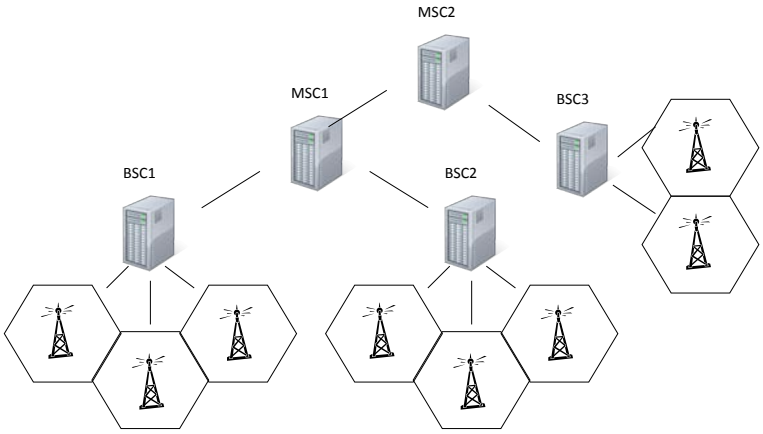
Where Are You?

The network needs to know where the mobile is in the network

Location Update transaction

- Connecting: selects a cell
- Periodic intervals while camping on a cell
- Reselecting to a new location/tracking area

Cell Reselection and Location Areas



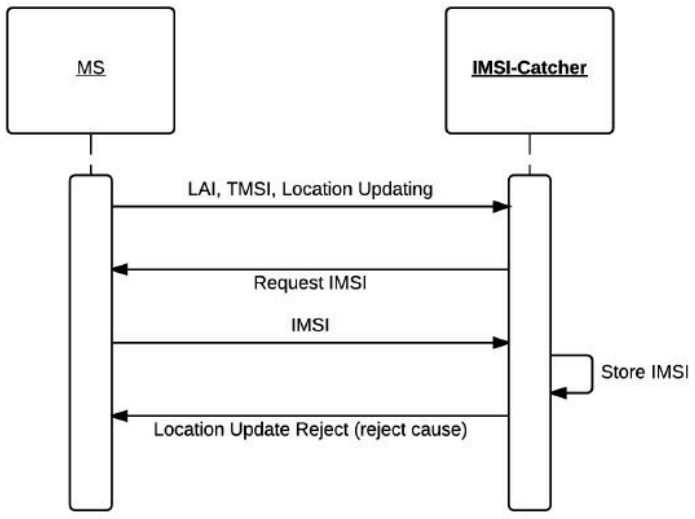


Figure 2.7: Message sequence chart of catching IMSIs with IMSI-catcher

Catching the IMSI-Catcher?

Counter Surveillance

This brings us back to the Aftenposten data

The Oslo data

- Journalists Per Anders Johansen, Andreas Bakke Foss og Fredrik Hager-Thoresen
- Radio measurements by Delma Ltd. (UK)
- 3 rounds in Dec.2014 and 1 round in April2015
- Ca. 42109 lines of measurement data
  - Telenor> 13 290 measurements
  - Netcom> 15 269 measurements
  - Network Norway> 13 550 measurements

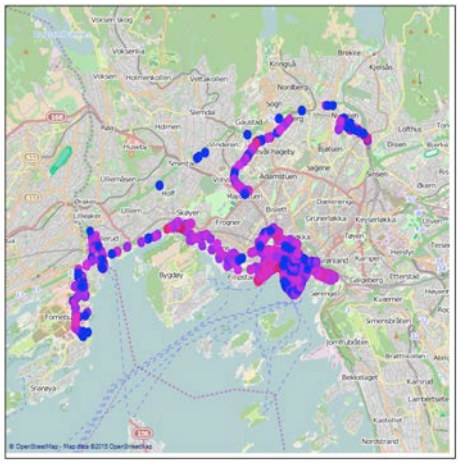
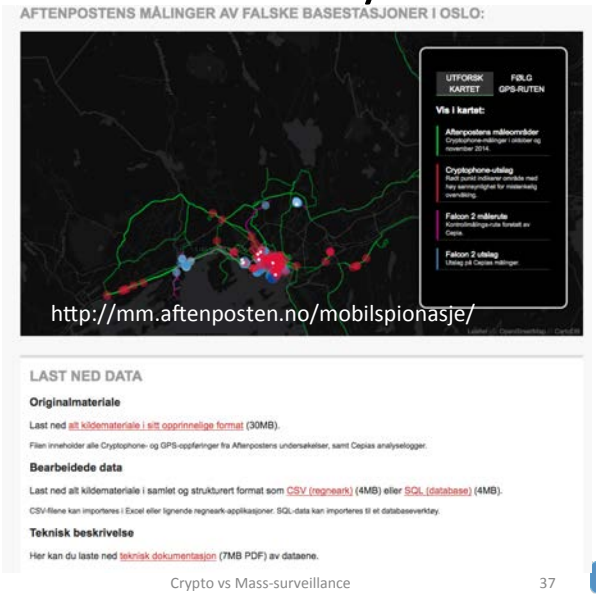


FIGURE 1. Locations covered by the survey work

Check the data yourself!



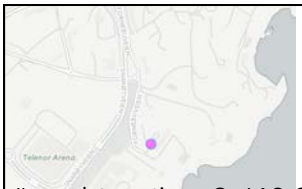
Figur 2 Fra Delma-måling ved Skansen i Oslo i april 2015. Utstyret får plass i en sekk, og består av en måleenhet, ant og en laptop.

Figur 1 Måleenhet og skjermbilde fra laptop. Foto: Delma

Til undersøkelsene ble seks sim-kort fra Aftenposten med Telenor, Netcom og Network Norway-numre koblet til målingsenheten, slik at alle de tre nettverkene kunne måles samtidig. Kontraetterretningsutstyret kan kartlegge ni ulike mobilnettverk på en gang.

Counter Surveillance Measurements

- Date
- Time
- GPS location
- Mobile Network Code (MNC)
- Location Area Code (LAC) 16 bits
- Cell Id (CID)
- Cell type
  (Serving-cell, Adjacent-cell)
- Abs. Freq.channel no (ARFCN)
- Rec. Power signal level
- C1 and C2 reselection values
- Alarm-type



Example 1

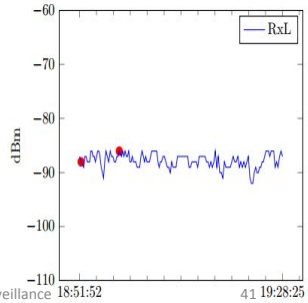
#	date	time	Op	LAC	Cid	RxL	CN		Lat	Long	type	C1	C2	BSIC		m
1425246	2014-12-03	14:19:18	1	11801	2174	3	-59	56	mobile-1214	59.9037095	10.6314283	38	S Cell	52	52	1	Normal	0	56.58
1425252	2014-12-03	14:19:42	1	11801	2174	3	-52	56	mobile-1214	59.9035273	10.6310227	38	S Cell	59	59	1	DL	0	30.36
1425264	2014-12-03	14:20:00	1	11801	2174	3	-51	56	mobile-1214	59.9035368	10.6310133	38.5	S Cell	60	60	1	DL	0	1.18
1425276	2014-12-03	14:20:17	1	2311	2174	3	-51	56	mobile-1214	59.9035354	10.6310152	38.5	S Cell	60	60	1	XDL	0	0.19
1425287	2014-12-03	14:20:45	1	11801	2174	3	-51	56	mobile-1214	59.9035336	10.631017	38.5	S Cell	60	60	1	DL	0	0.22
1425298	2014-12-03	14:21:04	1	11801	2174	3	-52	56	mobile-1214	59.9035321	10.6310189	39	S Cell	59	59	1	DL	0	0.2
1425314	2014-12-03	14:21:38	1	11801	2174	3	-53	56	mobile-1214	59.9034632	10.6309599	39.5	S Cell	58	58	1	DL	0	8.34
1425325	2014-12-03	14:21:57	1	11801	2174	3	-52	56	mobile-1214	59.903461	10.6309646	39.5	S Cell	59	59	1	DL	0	0.36
1425337	2014-12-03	14:22:15	1	11801	2174	3	-54	56	mobile-1214	59.9034604	10.6309654	40	S Cell	57	57	1	DL	0	0.08
1425349	2014-12-03	14:22:32	1	11801	2174	3	-51	56	mobile-1214	59.90346	10.6309667	40	S Cell	60	60	1	DL	0	0.09
1425361	2014-12-03	14:22:51	1	11801	2174	3	-53	56	mobile-1214	59.9034599	10.6309679	40	S Cell	58	58	1	DL	0	0.07
1425374	2014-12-03	14:23:09	1	11801	2174	3	-58	56	mobile-1214	59.903459	10.6309698	40	S Cell	53	53	1	DL	0	0.15
1425387	2014-12-03	14:23:27	1	11801	2174	3	-79	56	mobile-1214	59.9035105	10.6298303	42.5	S Cell	32	32	1	Normal	0	63.8

Figur 52 Måleresultatene utenfor Radisson Blu Park hotell på Fornebu. Viser hvordan Telenor-celle 2174 på kanal 56 skifter LAC innen for en radius av 10 meter.

Cell/Channel LAC Change

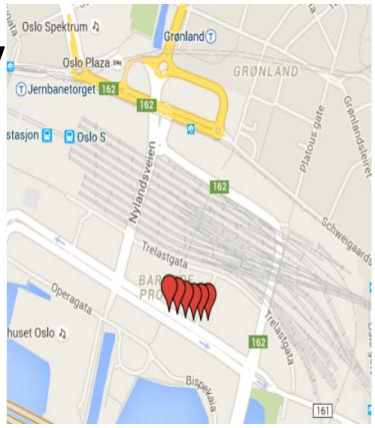
- Only LAC changes, all other values static
- LAC changes only for one measurement (seconds)
- RxL does not fluctuate: very likely the same transmitter
- Earlier observations with similar RxL and configuration
- LAC changes to another operators LAC

time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:51:52	11901	3218	-87	53	S Cell	24	24
18:52:08	2311	3218	-88	53	S Cell	23	23
18:52:36	11901	3218	-89	53	S Cell	22	22
18:52:50	11901	3218	-87	53	S Cell	24	24
18:53:03	11901	3218	-87	53	S Cell	24	24

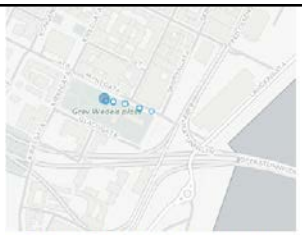


Provider Anomaly

- Two Telenor cells appear in the neighbour list of a Network Norway cell
- Not typical IMSI-catcher behavior
- Network Norway and Telenor roaming agreement?



time	lac	cellid	mnc	rxl	arfcn	celltype	c1	c2	slot
10:52:30	2311	1091	5	-78	986	S Cell	27	27	3
10:52:30	2311	41922	5	-80	987	A Cell	23	23	3
10:52:30	11901	59403	1	-72	68	A Cell	38	38	3
10:52:30	11901	58135	1	-81	66	A Cell	29	29	3
10:52:30	2311	1032	5	-83	984	A Cell	14	14	3



Figur 47 En ny LAC og en ny celle på en ny kanal og til slutt tjenestenekt. Funnet i Myntgata er et av de klareste i dataene.

Example 2

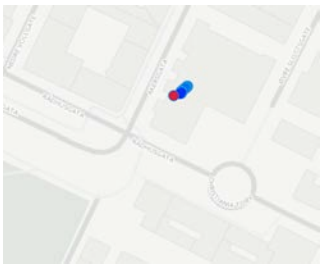
#	date	time	Op	LAC	Cid		RxL	CN		Lat	Long		type	C1	C2	BSIC		m	
1460724	2014-12-22	14:14:47	1	11901	23488	1	-98	672	mc	59.907436	10.7438405	41	A Cell	12	12	22	Normal	0	0
1460725	2014-12-22	14:14:47	1	11901	3732	1	-106	68	mc	59.907436	10.7438405	41	A Cell	4	4	49	Normal	0	0
1460728	2014-12-22	14:15:06	1	11901	23488	1	-88	672	mc	59.907511	10.7433669	47.5	S Cell	23	23	22	Normal	0	27.69
1460729	2014-12-22	14:15:06	1	11901	3295	1	-102	63	mc	59.907511	10.7433669	47.5	A Cell	8	8	57	Normal	0	0
1460732	2014-12-22	14:15:25	1	11901	23488	1	-92	672	mc	59.9075488	10.7429685	48	S Cell	19	19	22	Normal	0	22.61
1460733	2014-12-22	14:15:25	1	11901	3783	1	-100	61	mc	59.9075488	10.7429685	48	A Cell	10	10	47	Normal	0	0
1460734	2014-12-22	14:15:25	1	11901	3732	1	-105	68	mc	59.9075488	10.7429685	48	A Cell	5	5	49	Normal	0	0
1460739	2014-12-22	14:15:44	1	11901	23488	1	-91	672	mc	59.9075502	10.742733	49	S Cell	15	15	22	Normal	0	13.13
1460740	2014-12-22	14:15:44	1	11901	3783	1	-103	61	mc	59.9075502	10.742733	49	A Cell	7	7	47	Normal	0	0
1460741	2014-12-22	14:15:44	1	12901	32478	1	-94	679	mc	59.9075502	10.742733	49	A Cell	8	43	0	Normal	35	0
1460745	2014-12-22	14:16:03	1	12901	32478	1	-83	679	mc	59.9075988	10.74268	48.5	S Cell	32	83	0	Cc	51	6.16
1460749	2014-12-22	14:16:21	1	0	0	1	-200	0	mc	0	0	0	No GSM	0	0	0	Normal	0	0

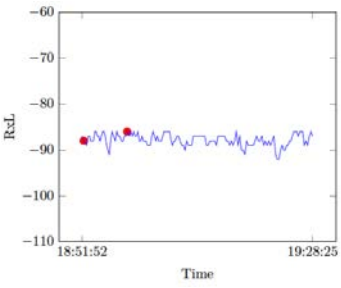
Cell 32478 Myntgata

- «Strongest evidence» of IMSI-catcher activity
- This LAC not used by any other cell in Oslo
- Abnormal high C2 values
- The **C** difference is an odd number – Should not be possible!

time	mnc	lac	cellid	rxl	arfcn	celltype	c1	c2
14:15:44	1	11901	23488	-91	672	S Cell	15	15
14:15:44	1	11901	3783	-103	61	A Cell	7	7
14:15:44	1	12901	32478	-94	679	A Cell	8	43
14:16:03	1	12901	32478	-83	679	S Cell	32	83
14:16:21	1	0	0	-200	0	No GSM	0	0
14:31:56	1	11901	23013	-102	682	S Cell	9	-11

Example 3





time	lac	cellid	rxl	arfcn	celltype	c1	c2
18:51:52	11901	3218	-87	53	S Cell	24	24
18:52:08	2311	3218	-88	53	S Cell	23	23
18:52:36	11901	3218	-89	53	S Cell	22	22
18:52:50	11901	3218	-87	53	S Cell	24	24
18:53:03	11901	3218	-87	53	S Cell	24	24

(a) Cell 3218 switches LAC at 18:52:08.

18:58:22	11901	3218	-88	53	S Cell	23	23
18:58:35	11901	3218	-87	53	S Cell	24	24
18:58:48	11901	3218	-87	53	S Cell	24	24
18:59:01	2311	3218	-86	53	S Cell	25	25
18:59:25	11901	3218	-87	53	S Cell	24	24
18:59:38	11901	3218	-86	53	S Cell	25	25

(b) Cell 3218 switches LAC at 18:59:01.

Figure 3.17: The two LAC changes observed on cell 3218.

Who Did It?

Real World Crypto Questions

- *What does end-to-end authenticated encryption really solve in mobile systems?*
- *Solve the privacy problem of 4G, 5G ?*
- *Surveillance-proof identification?*
- *Crowdsourced counter-surveillance system?*
- *Or, leave it to the law makers….*

Master thesis projects based on USRP

[1] Glendrange, Hove and Hvideberg: *Decoding GSM*.
Master thesis, NTNU, June 2010.
[2] Maxim Suraev: *Denial-of-service attack resilience of the GSM access network*.
Master thesis, NTNU June 27, 2011.
[3] Francois Ponsgen: *GSM attacks using OsmocomBB*,
Master thesis, NTNU, June 2015
[4] Torjus Bryne Retterstøl: *Mobile network basestation experimentation using USRP and OpenBTS*, Master thesis, NTNU June 2015
[5] Eirik Fosser: *Detecting IMSI-catchers and false mobile stations*,
Master Project, NTNU Dec 2015
[6] Andre Mruz: Mobile Network Security Experiments with USRP, Master thesis, NTNU June 2016.
[7] Jonathan Hansen: Wireless USRP Testbed for DSRC Applications, Master thesis, NTNU June 2016.