Verji Secure Mobile Communication

Odd Helge Rosberg
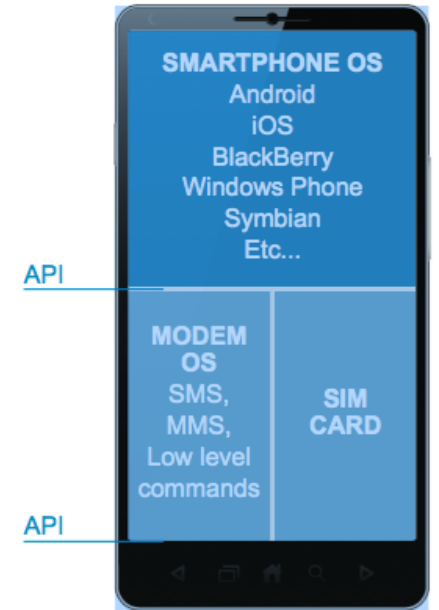CTO and Co-Founder

Rosberg System as

verji

What is an SMS-based attack?

- An SMS can contain code that can infect your smartphone, and can also be sent as a service SMS. A service SMS is not visible for the user of the smartphone.
- An SMS based infection can:
  - Monitor all activity and content on your smartphone.
  - Remote activation of your microphone and camera
  - Localizing you, geofencing.
  - Destroy the smartphone.
- Who are using this kind of infections?
  - Surveillance by military and government (MonkeyCalendar, Smurf attacks, BAE, Bull, Hacking Team…)
  - Industrial espionage
  - Financial crime
  - ID-theft, destroying other people's credibility
  - Private surveillance
- SMS's can also be used to control spy software installed in other ways.

WHERE CAN THEY ATTACK?

- Smartphones have three different processors and operating systems.
  - Main OS: iOS, Android, Windows Phone, Blackberry
  - The modem, typically running embedded Linux
  - The SIM-card, often using embedded Java
- All three levels can be infected using SMS
- Antivirus solutions can only monitor the OS, not the other two levels.

SMARTPHONE OS
Android
iOS
BlackBerry
Windows Phone
Symbian
Etc...

API

MODEM OS
SMS, MMS, Low level commands

SIM CARD

API

- Nordic Telco's are on the top of the list when it comes to security.

- Security Research Labs in Germany tests Telco security regularly, and Scandinavian Telco's are extremely good.

- Still, Telco's have to conform to GSMA standards, and since the SMS standard is now 21 years old, and the latest revision was in 1995, there is only so much they can do.

Categories of surveillance

- Smartphones can be put under surveillance in many ways, and we have separated the tools for doing so into three categories:
  - Military / Government
  - Industrial
  - Private
- After having studied these solutions, they seem to be quite similar in functionality, the main differences are:
  - How well they hide on the Smartphone
  - How well they handle encryption
  - Scalability

- These tools are easily accessible on the Internet.

- There are many such tools available, common for them is that they are very easy to insall and use.

- Most of them are cloud based services, meaning that the cloud service will collect data 24/7 while the buyer of the service can log on at their discression and check the results in a standard web-browser.

- There are solutions that does not require any install on the target device, solutions that do require an install on the target device, as well as solutions that can run either with or without jailbreak on iPhone. I have found no apps that require rooting on Android.

mSpy – surveillance on all kinds of devices, for iOS both with and without jailbreak. www.mspy.com

Flexispy – Please try the online demo
www.flexispy.com

There are many...

1	2	3	4	5	6	7	8	9	10
MSPY	HIGHSTER MOBILE	FLEXISPY	SPYERA	TEENSAFE	MOBISTEAL TH	THETRUTH SPY	THEONESP Y	MOBILESPYA GENT	SPYPHONE TAP

Functionality

Check out all our great spy phone features

Spy on Calls
- Listen to live calls
- Record calls [1]
- Call logs
- VOIP Call logs [4]
- Listen to phone surroundings
- Record phone surroundings [8]
- Facetime Spy Cam [3]

Spy on Messages
- Read SMS messages
- Read MMS messages [8]
- Send fake SMS messages
- Delete SMS messages containing keywords [8]
- Read Emails

Spy on Passwords
- Spy on Passcodes [6]
- Spy on Application passwords [6]
- Spy on Email passwords [6]

Spy on GPS
- View & Track GPS location

Spy on IM Chats
- WhatsApp [5]
- Facebook / FB Messenger [6]
- Viber [6]
- LINE [6]
- Skype [6]
- WeChat [6]
- iMessage [4]
- BBM [9]
- Blackberry PIN [2]
- Yahoo Messenger [6]
- Snapchat [4]
- Hangouts [6]

Spy on Multimedia
- Video files
- Image files
- Audio files

Spy Remotely
- Take a picture using the camera [8]
- Restart Device [4]
- Check device battery status
- SMS Remote Commands

Spy on Internet
- Web pages viewed [6]
- Bookmarks [6]

Spy on Applications
- Address book
- Calendar [6]
- Notes [4]
- Installed Programs [8]
- Program Activity

Receive Alerts When
- Change SIM card
- Call specific contacts
- Alert Wizard

Spy in Secret
- Hide Jailbreak [4]
- Hide SuperSU [1]
- Hide from application list/task manager

Easy To Use
- Easy to install
- Online Remote Commands
- Upgrading
- Update [6]
- Renewing
- Deactivation
- Uninstallation

Compatibility

1 Android	3 iPad	5 Android, iPhone	7 Not available on iPad	9 Not available on Symbian
2 Blackberry	4 iPad, iPhone	6 Android, iPhone, iPad	8 Not available on Blackberry	Click here for details

Actual example of criminal usage
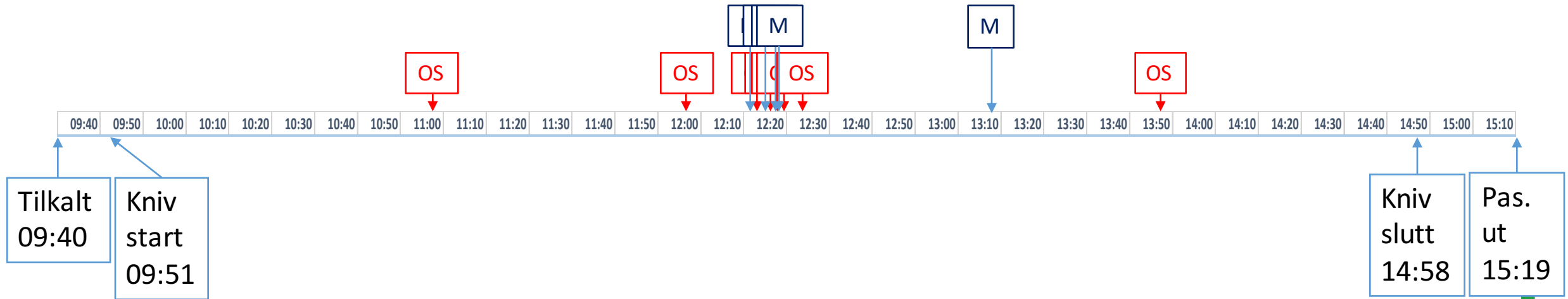
Government "hacking suites"

- NSA (USA): MonkeyCalendar, first launched in 2007
- GCHQ (Government Communications HQ, UK): Smurf suite
- BAE (UK): Professional surveillance systems
- Bull (France): Professional surveillance systems
- Hacking Team (Italy): Professional surveillance systems

IMSI catchers (Stingray)

Odd Helge Rosberg
CTO and Co-Founder

Rosberg System as

verji

En ny rapport fra norske myndigheter slår fast at det foregår ulovlig mobilovervåking i Norge. Men teleselskapene mangler utstyr og rutiner for å avsløre det.

Kriminelle og fremmede stater overvåker mobilnettet

PER ANDERS JOHANSEN
ANDREAS BAKKE FOSS
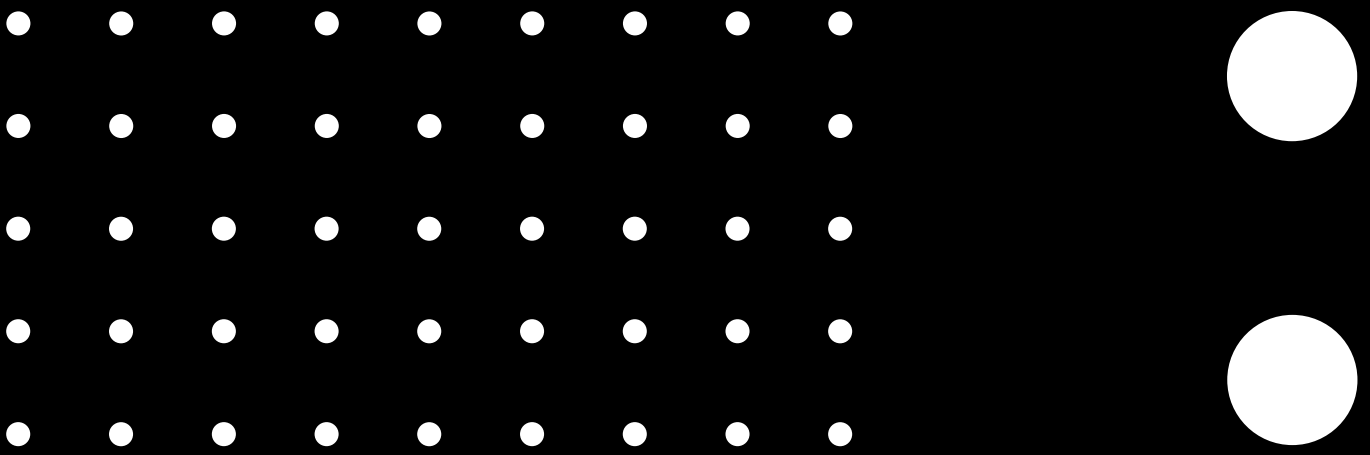FREDRIK HAGER-THORESEN

Den nye rapporten er utarbeidet etter Aftenpostens artikkelserie om mobilovervåking i vinter.

Onsdag sendte PST ut en pressemelding om at det var «ingen falske basestasjoner i Oslo». «Informasjonen vi har fått inn

Aftenposten
avslører MOBILSPIONASJE

- **Attacks, using silent service SMS (Silent SMS attacks)**

- **Attacks, using fake cell towers**
  - **IMSI Cathers, Stingray**

SIRKLET INN FRA UTLANDET

Nå kan hackere finne ut eksakt hvor du er til enhver tid, fra et hvilket som helst sted i verden, bare ved å kjenne mobilnummeret. Og du kan ikke gjøre noe med det. DN testet ut den nye overvåkningsmetoden – som allerede er til salgs.

TEKST OSMAN KIBAR FOTO MAXIM SERGIENKO
Berlin/Oslo

KRIMINELLE HAR GJORT MYE MER KOMPLISERTE TING FOR Å FÅ TILGANG TIL BANKKONTOER
ENN SS7-BASERTE ANGREP
TOBIAS ENGEL hacker og mobilsikkerhetsekspert

Spionutstyr plassert i Norges fremste finansmiljø

På Aker brygge og Tjuvholmen står det høyst sannsynlig avansert overvåkingsutstyr som gjør det mulig å spionere på næringsdrivende, advokater og andre som forvalter forretningshemmeligheter og millioner av kroner.

Not only in Norway

Fake phone masts installed across London to listen in on all mobile calls

Published time: 10 Jun, 2015 12:18

Get short URL

Reuters / Andrew Winning / Reuters

More than 20 fake phone masts have been tuning in to mobile phone conversations across the capital, with the police unable to confirm who is operating them.

The Stingray masts, which tap into the communications data of mobiles, are supposedly used to listen in on criminals by intercepting information intended for the network provider.

Tags

UK, Human rights, Security, Hacking, Intelligence

However, because the masts are unable to differentiate between criminal communications and regular users, they sweep all the information available to them, meaning millions of people are potentially having their telephone data sent to a third party.

VERJI

Not only in Norway

Chicago Cops Used Stingray to Intercept Protester's Conversations

👤 thefreethoughtproject.com   📅 December 2014   💬 comment | ⊕ ⌟ ↗

Not only in Norway

MYSTERIOUS 'FAKE' CELL PHONE TOWERS FOUND ACROSS AMERICA

Imposter towers discovered near U.S. Army bases

Paul Joseph Watson - SEPTEMBER 2, 2014   💬 526 Comments

TODAY

On the **Tuesd**
Attorney Gene
replacements

WATCH
Watch The A

IMAGE CREDITS: WIKIMEDIA COMMONS.

Equipment

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

It still happens, even here...

Høyres hus, Oslo
Wednesday February 17th
12:15:29
1st day of HackCon

Cell info

Cell status	Unknown
Source	
IMEI	
SIM Serial nr	
SIM Subscriber id	
Operator Name	N Telenor
Operator Number	24201
MCC	242
MNC	1
SIM Operator Name	Telenor
SIM Operator Number	24201
SIM MCC	242
SIM MNC	01
LAC	11901
Cell Id	20041
Short Cell Id	20041
Signal Strength	85
Cell scrambling code	-1
Network type	Unknown
Latitude	59.9138415
Longitude	10.7353108
Accuracy	24.0
Occurrence	1
Time update	20160217 12:15:29

EVRY mobile security suite concept

Mobile devices, sensors & IoT

Operating System, Apps and Content

Modem

Simcard

Mobile Security Suite from EVRY

|	Security consulting
Email & content	
OS & Apps	
Administration	
Message and Voice	
IMSI	
SMS	

EVRY
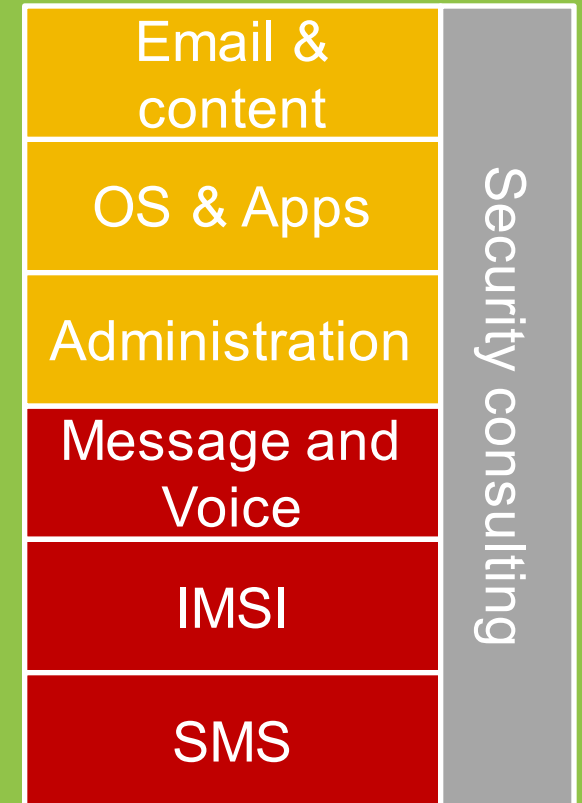
Secure Mobile Communication (SMC)

Secure Mobile Communication address security and privacy challenges on mobile phones for business that value their sensitive communication.

- End to end encryption of messages

- End to end encryption of attachments

- End to end encryption of voice

- Protects against IMSI catcher attacks

- Protect against SMS attacks

Secure Mobile
Communication
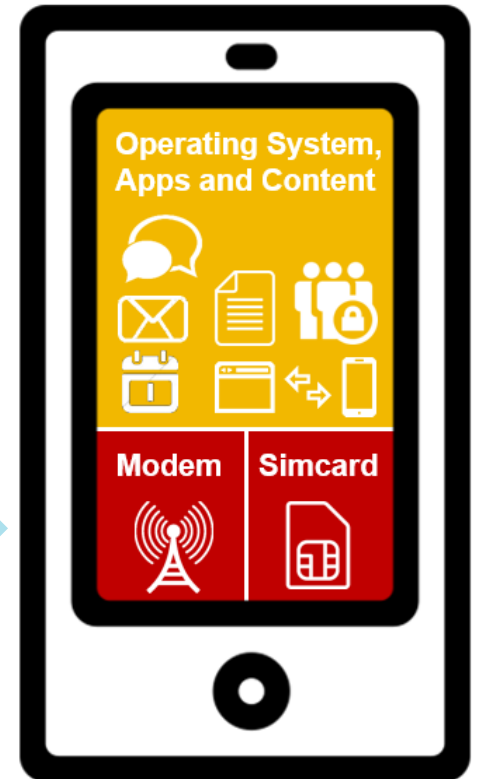
Quick overview

Verji SMC

Encrypted voice

Encrypted messaging

Option: IMSI

Protects you against fake base stations

Option: SMS

Encrypted SMS to any recipient

Protection against SMS based attacks

EVRY

Communicate securely and with ease

- Chat securely with your colleagues anywhere
- Transfer sensitive data with ease, without worry
- Simple, use your existing contact list
- Share documents, spreadsheets, presentations...
- Use the full potential of your mobile as a collaboration tool

Conversations

Jan Martin Kristiansen 16/10/2015 09:24
Great meeting!

Alf Kenneth Braathen 16/10/2015 09:22
Anything new regarding IMSI...

4759440166 16/10/2015 09:17
Can we move the meeting to ...

Healthcare: Transfer sensitive information securely and quickly
Law: Communicate securely with your clients and colleagues
Journalists: Communicate with colleages and informants securely
Donate: Give the app to external contacts and let them know you take their security seriously

Verji SMC

Encrypted voice

Encrypted messaging

EVRY
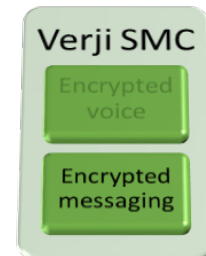
Talk when only one is listening

- Talk securely with your colleagues anywhere
- Low cost, easy to use and hassle free alternative to crypto phones

Healthcare: Discuss with colleagues or patients securely
Law: Show your client you take security seriously and strenghten your image
Journalists: Talk with informants without risk
Donate: Give the app to external contacts and let them know you take their security seriously

Verji SMC

Encrypted voice

Encrypted messaging

EVRY
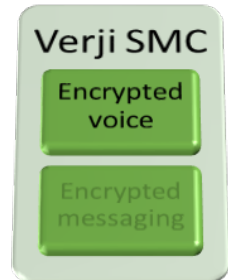
Know if you are unsafe

- **Be alerted** of IMSI-catcher attacks
- **Stay safe** in foreign countries
- Hassle free **invisible protection** of your phone

Healthcare: Protect your sensitive information
Law: Make sure you and your client are not spied upon
Journalists: Stay safe in turbulent areas, or when traveling abroad
Donate: Give the app to external contacts and let them know you take their security seriously

IMSI
Protect you against fake base stations

EVRY

Encrypt even your SMS's

- Know no one can listen in on your messages
- Seamlessly integrated with our messaging app
- Send any kind of file even to people without the app
- Easy and intuitive to use

Healthcare: Protect your sensitive information
Law: Make sure you and your clients are not spied upon
Journalists: Stay safe in turbulent areas, or when traveling abroad
Donate: Give the app to external contacts and let them know you take their security seriously

SMS
Encrypted SMS
Protection against SMS based attacks

EVRY

Don't worry, we protect you

- Know it is impossible to infect your phone using SMS or MMS
- Works silently, in the background, protecting you
- Send any kind of file even to people without the app
- Easy and intuitive to use

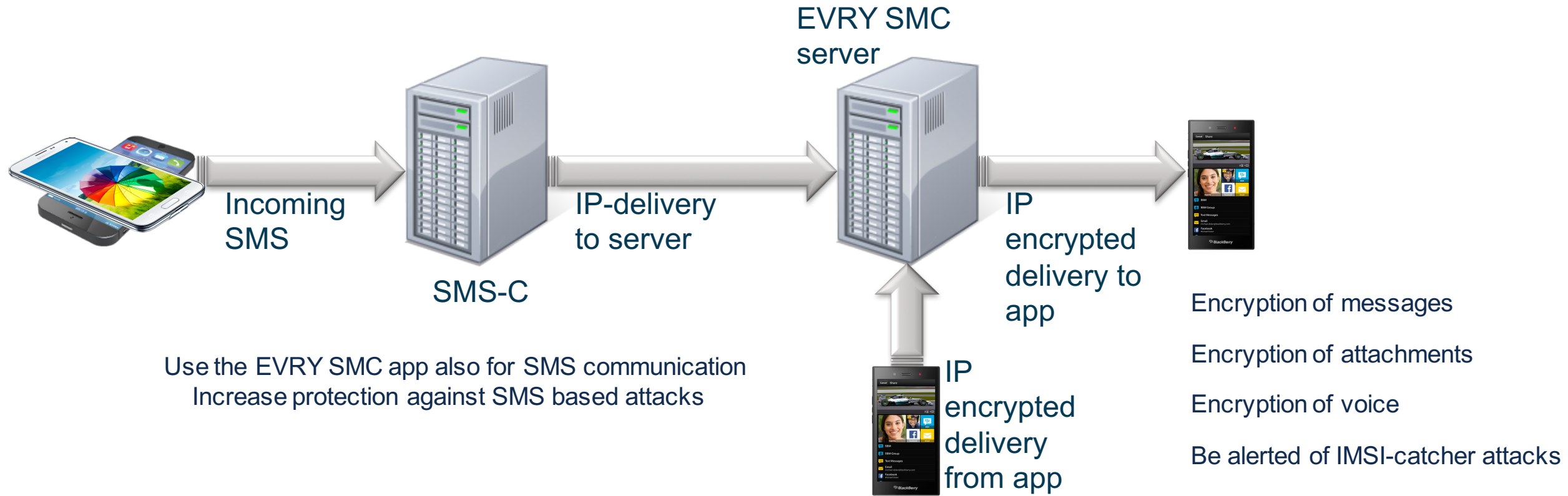Healthcare: Protect your sensitive information
Law: Make sure unseen surveillance can't infect your smartphone
Journalists: Protect you, the identity of and data from your informants
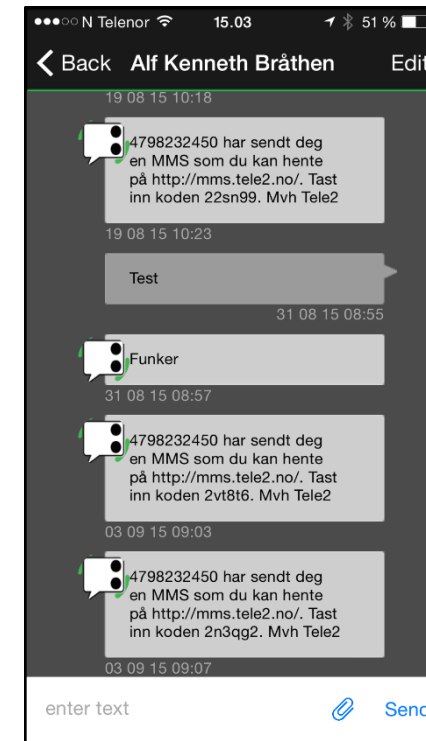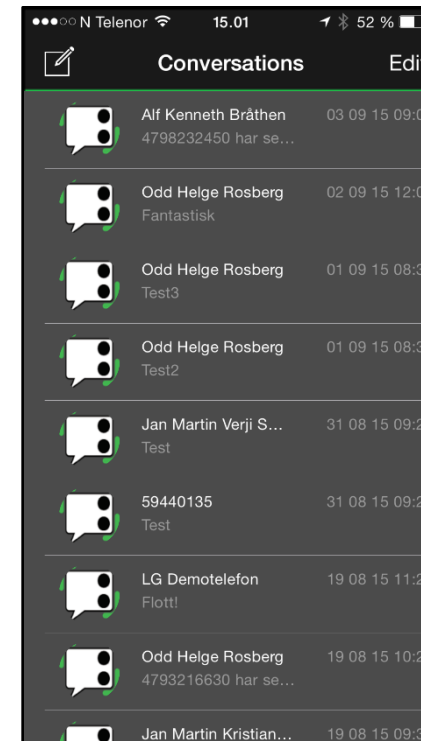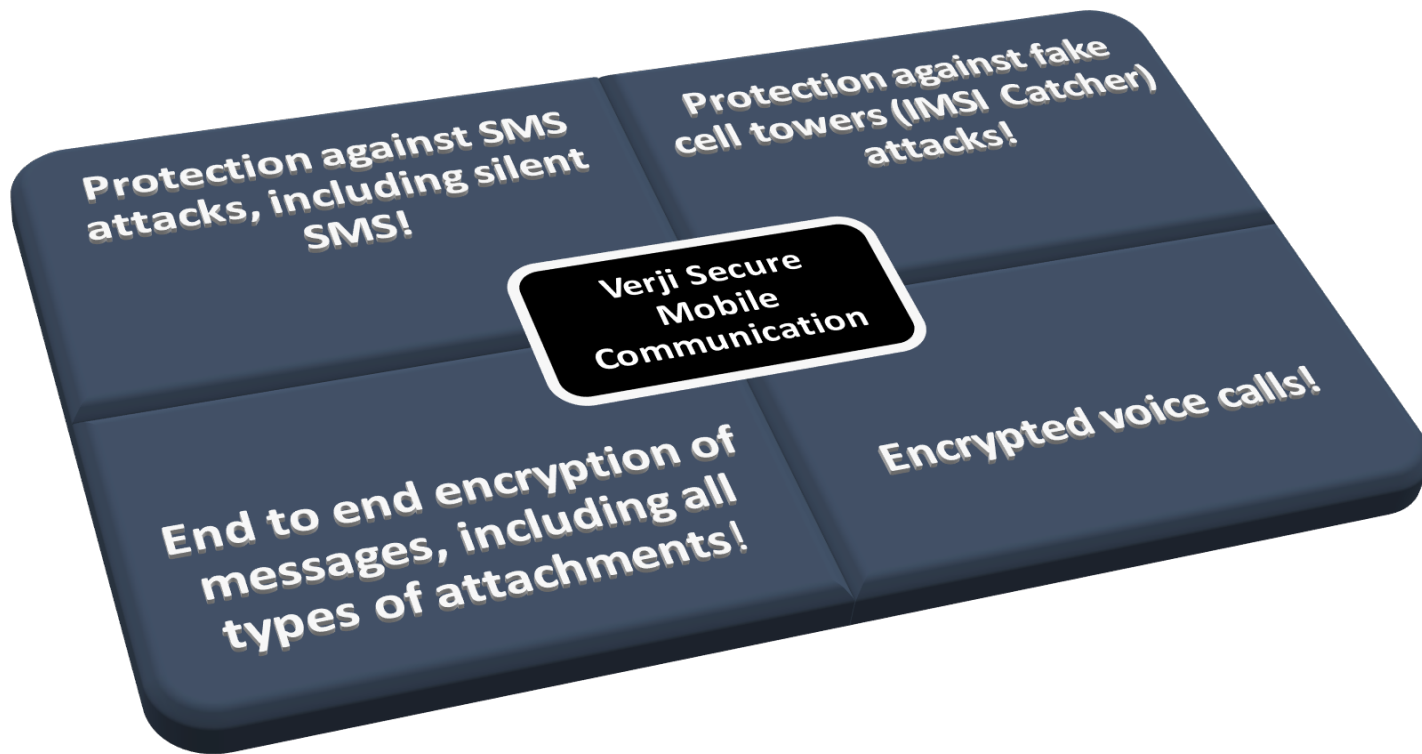Donate: Give the app to external contacts and let them know you take their security seriously

SMS
Encrypted SMS
Protection against SMS based attacks

EVRY

EVRY SMC (Secure Mobile Communication) system overview

EVRY SMC
server

Incoming
SMS

SMS-C

IP-delivery
to server

IP
encrypted
delivery to
app

IP
encrypted
delivery
from app

Use the EVRY SMC app also for SMS communication
Increase protection against SMS based attacks

Encryption of messages

Encryption of attachments

Encryption of voice

Be alerted of IMSI-catcher attacks

EVRY

Verji SMC
Secure Mobile Communication

Protection against SMS attacks, including silent SMS!

Protection against fake cell towers (IMSI Catcher) attacks!

Verji Secure Mobile Communication

End to end encryption of messages, including all types of attachments!

Encrypted voice calls!

Awarded as "Best ICT Security Innovation" in the prestigous EU prize European Cyber Security Award!

IPACSO AWARDS — WINNER OF THE 2014 EDITION
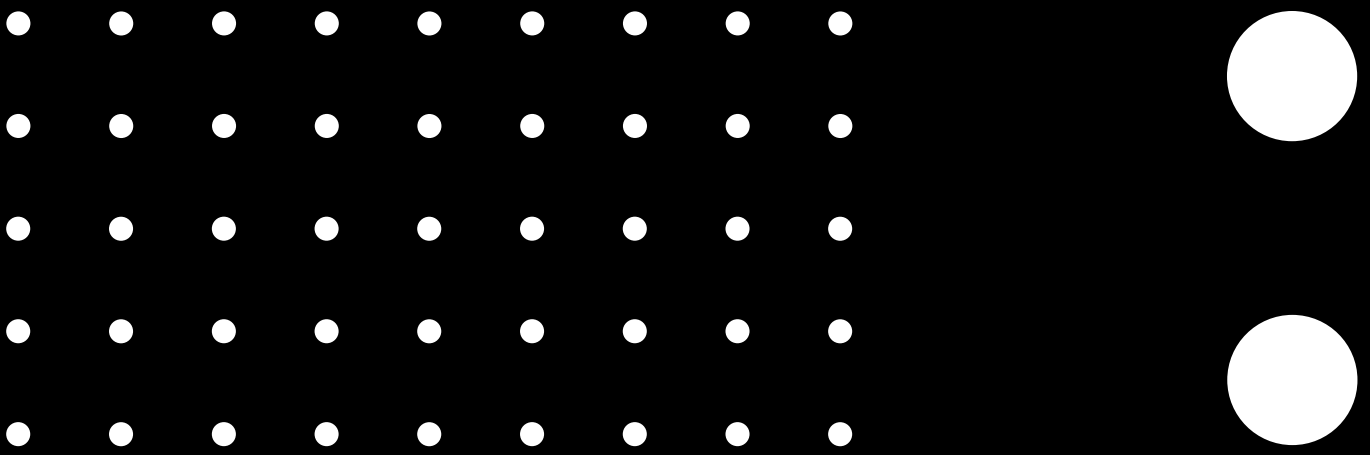
Thank you for your attention

Odd Helge Rosberg
Phone: +47 9321 6630
E-mail: odd.helge@rosberg.com
E-mail: sales@rosberg.com
Skype: odd.helge.rosberg

Rosberg System as

verji