NOKIA

Nokia Networks

Attacking the Internet of Things via the Roaming Interface

Silke Holtmanns, Ian Oliver

Mobilfunktagung 2015

Existing Interconnection Network Vulnerability that made it to the news

…operators have identified vulnerabilities in interconnection at a global scale…

Since the alleged revelations on GCHQ hacking Belgacom…


SPIEGEL ONLINE INTERNATIONAL

Front Page | World | Europe | Germany | Business | Zeitgeist | Newsletter

Quantum Spying: GCHQ Used Fake LinkedIn Pag

By SPIEGEL Staff

Officials at LinkedIn say they "would not authorize such activity for any purpose".

Elite GCHQ teams targeted employees of mobile communications companies ar their company networks. The spies used fake copies of LinkedIn profiles as on

November 11, 2013 – 12:03 AM

Print | E-Mail

Feedback

The Belgacom employees probably pulled up their profiles on LinkedIn pages looked the way they alway than usual to load.


HACKER

Wie Merkels Handy abgehört werden konnte

Berliner Sicherheitsforscher haben die Verschlüsselung in UMTS-Netzen ausgehebelt. Möglicherweise hat die NSA auf diesem Weg einst das Zweithandy der Kanzlerin überwacht. VON PATRICK BEUTH

18. Dezember 2014 19:31 Uhr

30 Kommentare


The Register® Biting the hand that feeds IT

Data Centre | Software | Networks | Security | Policy | Business

SECURITY

Global vulnera

HELP NET SECURITY

NEWS | MALWARE | ARTICLES | REVIEWS | RISKS

The state of GRX security

by Zelika Zorz - Managing Editor - Thursday, 12 June 2014

BOOKMARK

Late last year, documents from Edward Snowden's NSA trove have revealed that Britain's GCHQ has mounted a successful attack against Belgacom (the largest telecom in Belgium) and its subsidiary BICS (Belgacom International Carrier Services), a Global Roaming Exchange (GRX) provider. Other GRXs have been targeted as well.

But how easy is it to breach the systems of existing GRX providers? Stephen Kho and Rob Kuiters, penetration tester and incident response handler (respectively) in the CISO team of the Netherland's largest telecoms provider KPN, have decided to check.

In this podcast recorded at Hack In The Box Amsterdam 2014, they explain what GRXs are, how they function, how vulnerable they are, and what their operators can do to secure them better.

Press the play button below to listen to the podcast:


CYBER security info

abilities | Mobile | Hacks | Cybercrime | Malware | Policy

ulnerabilities in the GRX

rs from Dutch telecom provider KPN have analyzed the GRX (GPRS systems of 23 GRX providers worldwide. GRX allows roaming calls even if providers do not have direct link between them. The systems of GRX accessible from the internet, run unnecessary services and contain erabilities. Access to the GRX from the internet allows any attacker (GPRS Tunneling Protocol) and exfiltration of sensitive data identifying ransmitted images, the user and his/her location.

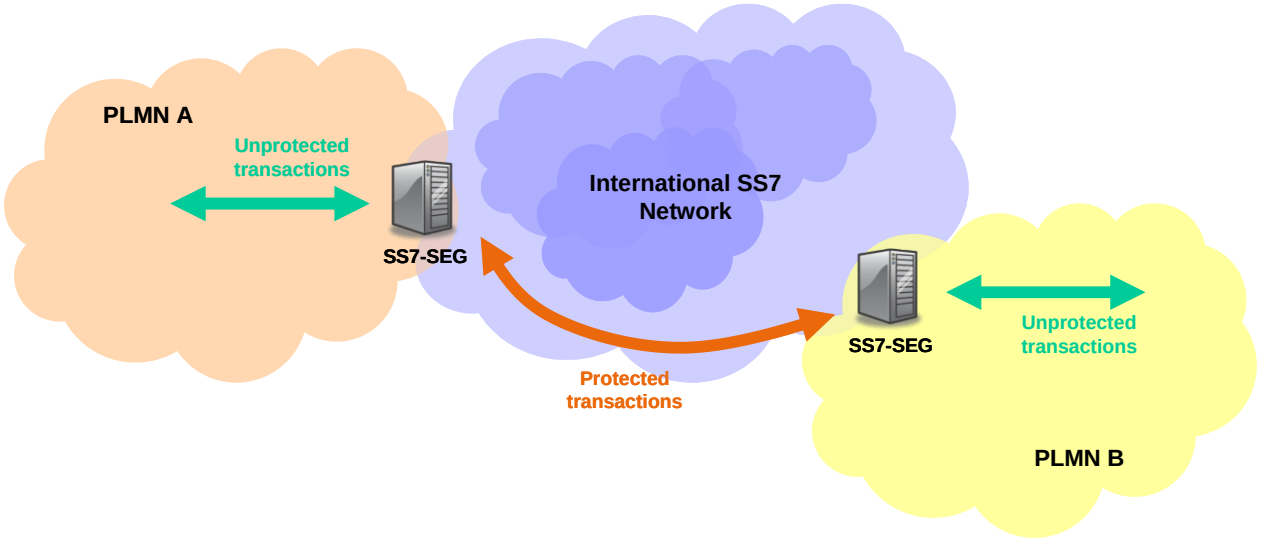
h links the roaming

hosts visible to the

NOKIA

Background – SS7

The vision – Usage of TCAP Security (GSMA IR.8220)



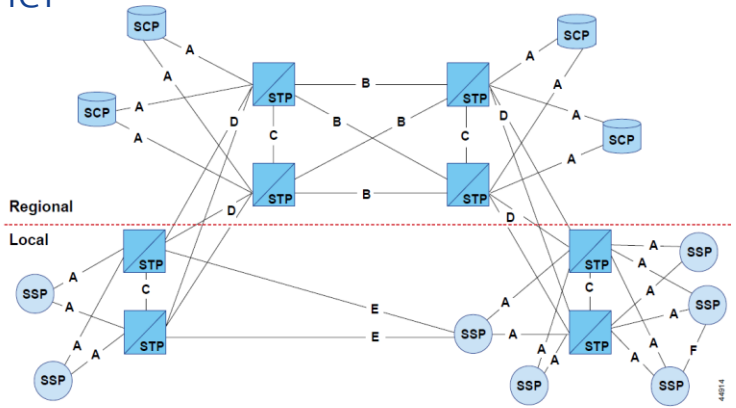
SS7 Reality

SS7 was taken into use, when there were few State-owned operators that trusted each other

IR.21 (GSMA roaming database)
- About 400 operators

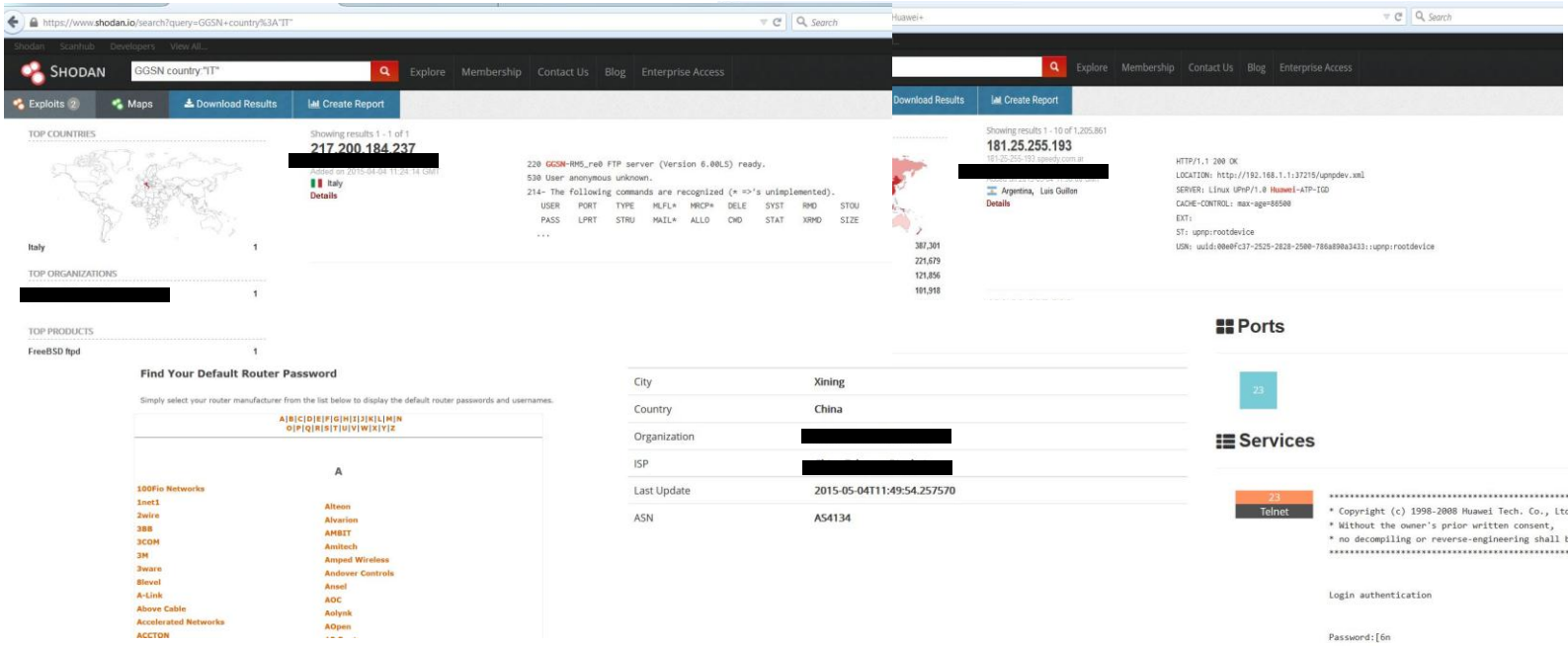
Backend access
- Nearly 1000 parties
- Several thousand accounts

Connections run often via hubs



Weak Points- Misconfiguration

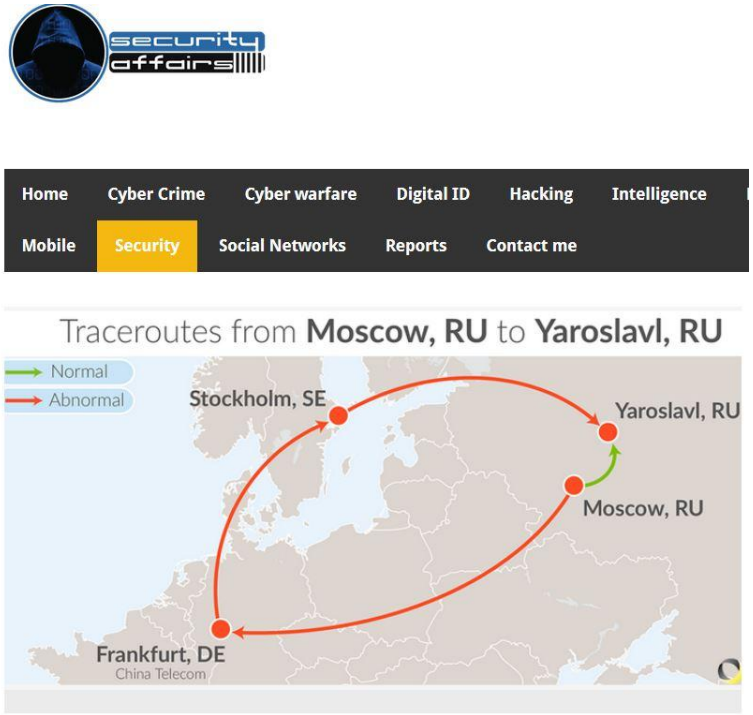
Nodes are visible and accessible



Weak Point - Usage of old unsecure protocols to maintain interoperability

- Border Gateway Protocol (BGP)
  - Untrustworthy routing tables
- SS7 without security
  - No GT authentication
- IP without IPSec

-> but the alternative would mean no roaming



Internal Internet traffic routed outside the Russia by a Chinese operator

Weak Point - Leasing out access – Interconnection Services

- SMS spoofing services
- Location tracking services

  ”Our system will query a mobile phone carriers network which a phone is operating on. If the phone is GPS enabled, we get assisted gps location data from that phone, which is usually very accurate. If our system does not get AGPS data from the phone, we check for location based on cell tower triangulation. Location accuracy via this method is less accurate. Location position information can range from a few hundred feet to several miles. Results are better in urban areas, as opposed to rural areas with few towers.”

- Unwanted advertisements
  - A Chinese user gets approximately 2 spam SMS per day
- Legal in many countries
- Gives access to interconnection system
- Encouraged ”involuntarly” by EU ”wholesale access”

Interconnection Security Standards
3GPP & GSMA

We are active in Security Standardization

- 3GPP SA3
  - Working on a technical specification for node hardening (SCAS)
- GSMA SG / RIFS
  - Working on a major updates of IR.77 and SS7 security guidelines (release scheduled in 2015)

Major Specifications

- GSMA PRD IR.77 “IPX Security Requirements”
- GSMA PRD IR.88 “LTE Roaming Guidelines”
- 3GPP TS 33.210 "Network Domain Security (NDS); IP network layer security"
- 3GPP TS 33.310 "Network Domain Security (NDS); Authentication Framework"
- 3GPP TS 29.272 "MME and SGSN related interfaces based on Diameter protocol“

NOKIA

How to hack?

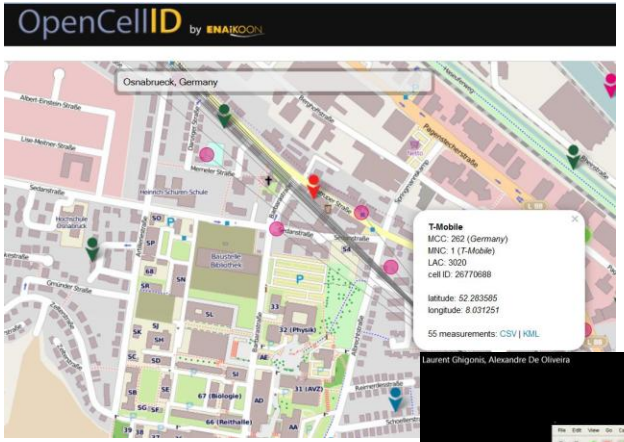
2008 Dec: 25C3 Chaos Communication Congress
Locating Mobile Phones using Signalling System #7 – Tobias Engel

2014 May: Cell Phone Hacking and how it is done - PT Security

2014 Dec: 31C3 Chaos Communication Congress
- SS7: Locate Track Manipulate – Tobias Engel
- Mobile self-defense – Karsten Nohl
- SS7 Map – Mapping vulnerability of international mobile roaming infrastructure - P1 Security

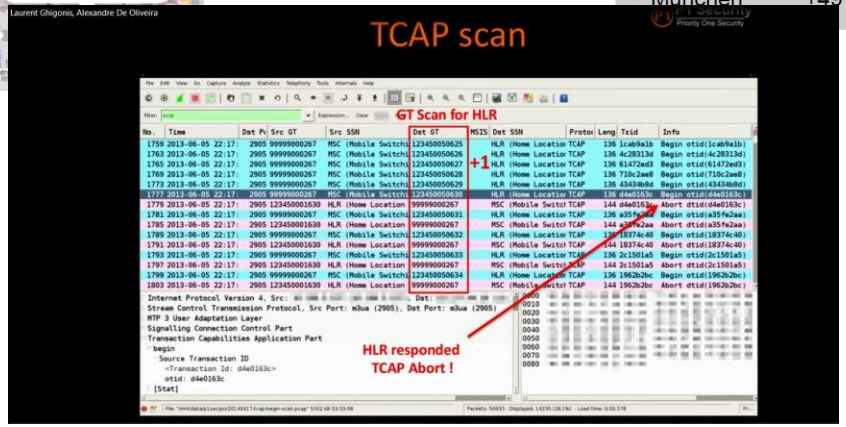
NOKIA

Phase I: Collecting Information



MSC global title (examples)

	T-Mobile Germany	Vodafone Germany
	First digit of area code	First digit of ZIP code
Berlin	+491710360000	+491720012097
Hamburg	+491710400000	+491720022097
Frankfurt	+491710650000	+491720061097
Stuttgart	+491710700000	+491720076097
München	+491710870000	+491720082097



References and sources on slide 17

Actual Attacks

Attack types known:

-Denial of Service against user or network nodes

-Credential theft

-Eavesdropping

-Location tracking

-SMS / call spoofing

-Subscription manipulation

-Fraud

Techniques:

-Using network internal / partner MAP commands (ATI, SP, SRI-SM, etc)

- Impersonation of network nodes

- Impersonation of roaming partners

- Overwriting user specific data

Internet of Things

Typical characteristics:

-Unattended

-Resource constraint

-Long life

-Low update fequency

-No or MSISDN based authentication and authorization

-Low revenue for operator

Risks:

-Silent SMS or failed calls even more unlikely to detect

-Self defense software can not be installed and used

-Patches can not be deployed

-Gaining access, sending commands or fraud scenarios are unlikely to be detected fast and easier then for the ”normal phones”

Why does it matter? – Cellular control in all areas

British Gas
Looking after your world

At Home | Business | Corporate

Products & services

amazon

G5 Home Security Wireless GSM SMS Burglar Alarm & Access Control System 50 Zones Touch Keyboard RFID Support Smart Phone App
by Chuango
2 customer reviews | 5 answered questions

› Help & advice › More › Remote Heating Control™ › Controlling your heating

Back to More

Remote Heating Control™

Controlling your heating

How do I use SMS text messages with Remote Heating Control™?

(4 ratings)

Print this page

The industry leading solution to connect your car to the cloud.

Viper SmartStart enables a "Cloud-Connected Car" like never before, providing an entirely new level of 2-way interaction with your vehicle. Connectivity is managed through our cloud services network linking car and app.

Product details

Response miGuard G5 GSM/SMS/RFID/Touch Controlled Wireless Home Alarm System

- GSM / SMS Communicating Alarm with integrated Mobile Phone Technology
- Controlled by SMS Text, App, Control Panel, Remote Control, RFID or Free Call
- Self-Monitoring with SMS notifications for Alarm, Emergency & Tamper
- Remote Monitoring with "Listen In" Feature
- Remote Arm and Disarm by SMS, App or Free Phone Call
- Arm, Part Arm, Disarm Modes (home arm has silent arming delay)
- Supports up to 50 wireless sensors, 10 remotes, 50 RFID tags
- RFID SMS notification number (up to 4 named tags)
- SMS arming/disarming
- SMS tamper alert for all accessories (first 9 named)
- SMS alerts for power failure, power recovery, low back up battery in CU
- SMS intruder alert including zone (first 9 named)

Summary

IoT requires more (and better) security

”Old” technology needs improvements

Thank you

References

PT Security, http://blog.ptsecurity.com/2014/08/cell-phone-tapping-how-it-is-done-and.html

Der Spiegel, Belgacom ”Geheimdienst GCHQ hackte belgische Telefongesellschaft”, http://www.spiegel.de/netzwelt/web/belgacom-geheimdienst-gchq-hackte-belgische-telefongesellschaft-a-923224.html

Shodan (IoT search engine), http://www.shodan.io

List of default username / passwords for routers, http://portforward.com/default_username_password/

SMS Spoofing services: http://www.digimessaging.com/test_system.php, http://www.smsgang.com/?send-sms-from-any-number

Cell Phone Tracking: http://www.mobilephonelocate.com/cell-phone-tracking.html

BGP Routing, http://securityaffairs.co/wordpress/30089/security/russia-interne-traffic-rerouted.html

Cell Map, http://www.opencellid.com/

Tobias Engel, 25C3, http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf, 31C3, http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

P1 Security, 31C3, http://labs.p1sec.com/2014/12/05/ss7map-mapping-vulnerability-of-the-international-mobile-roaming-infrastructure-at-31c3/

Karsten Nohl, 31C3, http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

Textport, Virtual Phone Number, http://www.textport.com/virtual_mobile_numbers.aspx