We are all connected - Interconnection Attacks

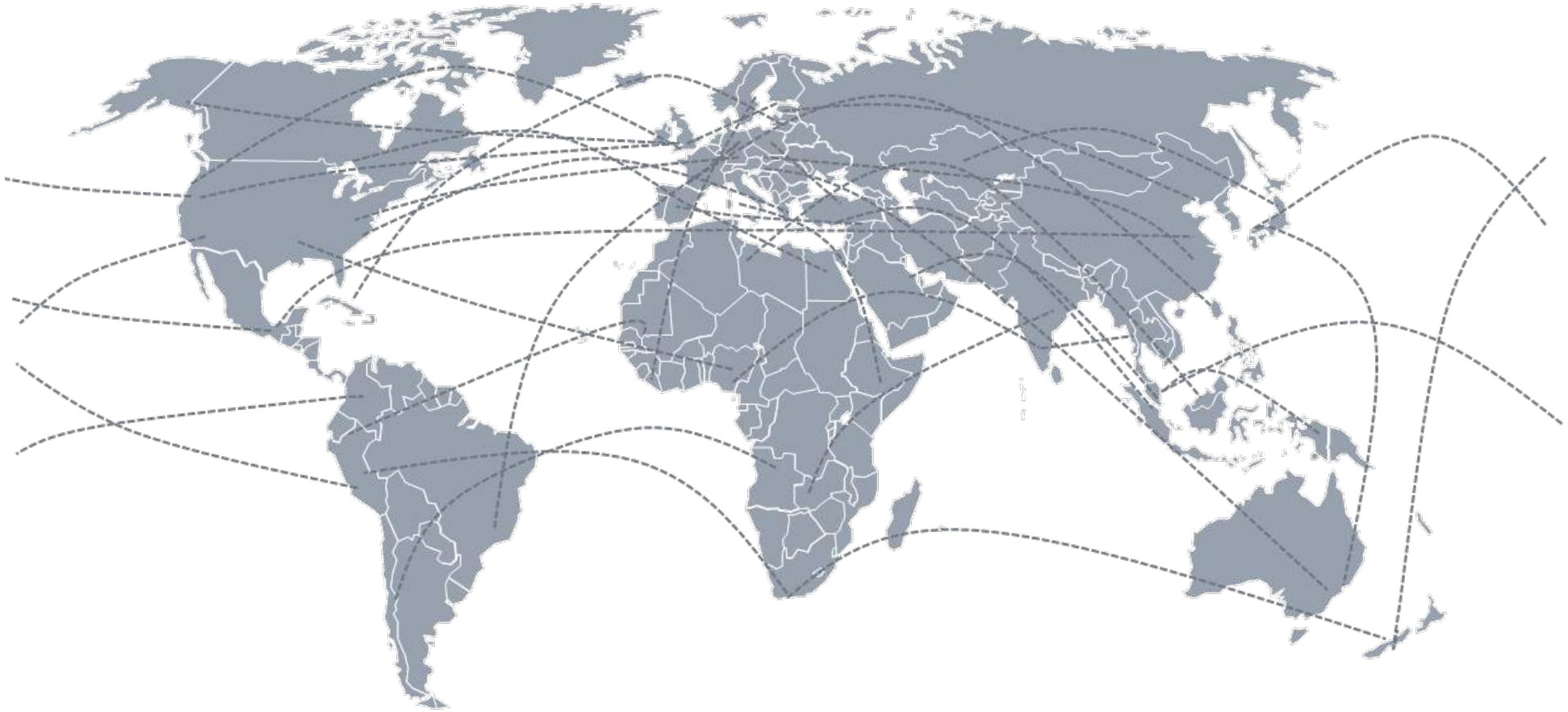
Silke Holtmanns
Nokia Bell Labs

One Highlight from WP4

DIMECC

Roaming Network – Interconnection Network

Not the Internet – but equally important



DIMECC

We are all connected to the Interconnection Network

DIMECC

History

- Established more than 35 years ago between a few state owned operators
- Build on trust (closed private network)
- No inbuilt security (in particular, no source authentication)
- SS7 protocol was constantly extended for new services and features
- New service providers connect all the time e.g. IPX roaming hubs, Application to user SMS, etc
- Now moving towards LTE / Diameter based protocols (4G/5G)

DIMECC

Closed & Private Network?

Three.ie

Login

Personal | Business

Shop | My3 | Help | 3Plus | 3Money | Search

Home. Explore. About three. Wholesale interconnect

› Why Three?
› About Three
› Media Centre

Wholesale Interconnect (Three Ireland (Hutchison) Limited).

The Intercept_

OPERATION SOCIALIST

The Inside Story of How British Spies Hacked Belgium's Largest Telco

One of the prime targets monitored under the AURORAGOLD program is the London-headquartered trade group, the GSM Association, or the GSMA, which represents the interests of more than 800 major cellphone, software, and internet companies from 220 countries.

Below you can see what I can provide. Contact information at the buttom page.

SERVICES

CELL PHONE REPORTS	CELL PHONE INTERCEPTION	SPOOFED SMS MESSAGING/CALLING	SS7 API
A cell phone report contains network information, such as MCC, MNC, IMSI, TMSI and location information(real-time) - You can request more, like the encryption keys of the current session.	This service is simple and easy. I only require you to provide the target MSISDN(number), along with a destination number that I can redirect the incoming/outcoming requests to.	You will be provided with a web panel and an access code, then you can send SMS messages and make calls without any restrictions, just by clicking a button.	With this, you can do everything I can, just by logging into an SSH server I have open. API Access Includes the following: Tracking, subscription modifying, jamming, intercepting, SMS/Call Spoofing.
3 LOOKUPS: $150	CALLS: $100	1 MONTH: $20	1 MONTH: $250
	SMS MESSAGES: $250		3 MONTHS: $500
			12 MONTH: $1250

SHODAN

221.177.247.252
China Mobile
Added on 2016-09-22 15:34:36 GMT
China
Details

ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.13(1.0.0)

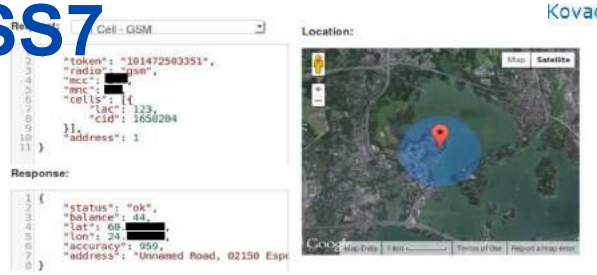
MIDDLE EAST 21:21 24.09.2016 (updated 22:22 24.09.2016) Get short URL 1 476 0 0

DIMECC

Existing Attacks for the ”old” SS7

If no protection is deployed

- Location Tracking
- Eavesdropping
- Fraud
- Denial of Service user & network
- Credential theft
- Data session hijacking
- Unblocking stolen phone
- SMS interception
- One time password theft and account takeover for banks, Telegram, Facebook, Whatsapp, g-mail (bitcoin)



SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

ile Security

Hackers Exploit SS7 Flaws to Loot Bank Accounts

Kovacs on May 04, 2017

Bulgarian company - Global Innovator in Wiretapping

"Circles Bulgaria" has listed itself as a virtual operator to intercept encryption keys from the SS7 inter-operator network

December 15, 2015

The Little Black Book of Billionaire

JUN 15, 2016 @ 08:00 AM 71,405 VIEWS

Hackers Can Steal Your Facebook Account With Just A Phone Number

hers has been shaken

Thomas Fox-Brewster.

WIRELESS

Telenor mobile network hit by international signal

Monday 22 February 2016 | 16:03 CET | News

etwork outage for several hours on 19 February due to ional operator. Services were affected from 11.30 to

WhatsApp SS7 attack

SOCIETY

Media: officials fired for using WhatsApp, Viber and Telegram

Security

Someone checked and, yup, you can still hijack Gmail, Bitcoin wallets etc via dirty SS7 tricks

Two-factor authentication by SMS? More like SOS

By John Leyden 18 Sep 2017 at 23:37 16 SHARE

DIMECC

All will be better with LTE and Diameter……

DIMECC

All will be ~~better~~ different with

LTE and Diameter……

DIMECC

Diameter Attacks researched under the CyberTrust Project

- Location Tracking (NATO CyCon Conference, 2015)
- Downgrading attacks (Troopers TelcoSec 2016)
- Denial of Service & Fraud (Blackhat, 2016)
- SMS and one time password interception (IEEE ICC 2017) (e.g. g-mail, MS, Twitter, Facebook, Amazon, etc)
- Subscriber Profile Modification (Network and System Security 2017)

To come

- Data interception for GPRS & LTE (potentially December 2017)

DIMECC

Countermeasures for operators

Detect Monitor network traffic Penetration & re-testing Tenant monitoring	**Mitigate** Filter, filter, filter Signaling Firewall SMS Home Routing
Cooperate Share experiences (GSMA) IPSec with partners e.g. TW Cooperation with legislators	**Prepare** Follow FS.11,FS.19,FS.07 Find weak spots Node hardening/procedures

CyberTrust WP4 Impacts – Academic Locally

- ✓ D4.4 A report, submitted publication, or thesis on escalation paths of targeted attacks, detection and mitigation approaches, technical viewpoint
- ✓ Academic impacts:
  - ✓ Two theses on DoS in mobile LTE networks / Location tracking in LTE
  - ✓ Workshop organization on 5G Security
  - ✓ Close academic – industry collaboration between F-Secure, VTT, Aalto, Abo University and Nokia
  - ✓ Blackhat / Troopers / IEEE ICC / NATO presentations (key ones)
    - ✓ Follow up request from operators and legislators -> Market creation with finnish leading expertise

CyberTrust WP4 Leaves a World Impacts

- ✓ Nokia impact:
  - ✓ Nokia Firewall product mitigation and detection enhancements
  - ✓ Nokia Security service enhancements (penetration testing)
  - ✓ Improvement of various products (hardening)

- ✓ Global and Industry impact
  - ✓ Finland recognized worldwide expertise on security (worldwide requests e.g. Taiwan regulator tomorrow)
  - ✓ GSMA standards (worldwide roaming security standards)
    - ✓ Attack scenarios, forensic analysis information, countermeasures input
    - ✓ Firewall configuration technical details
  - ✓ US FCC guideline 3/2017 given to congress, work continues in a new Working Group
  - ✓ US DHS guideline to be given to congress
  - ✓ Nordic regulators proactively work on diameter security
  - ✓ Worldwide security deployments and customers
  - ✓ SOME & News coverage

Contact us!

Silke.holtmanns@Nokia-bell-labs.com