



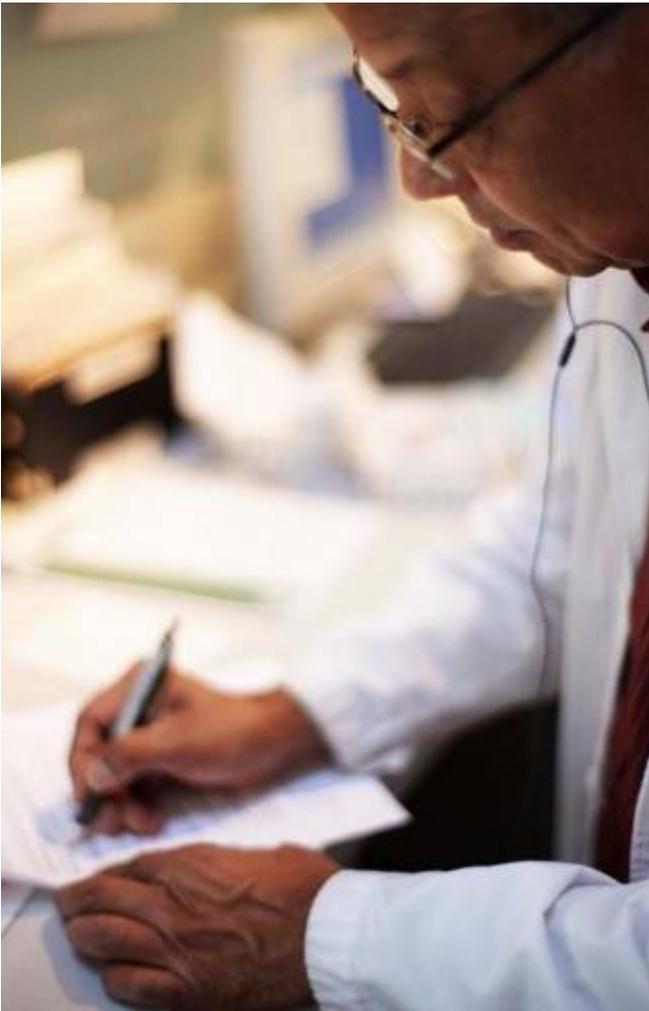
Security incidents – Lessons learned

Mikko Karikytö & Anu Puhakainen
Ericsson psirt



666

outline



Introduction

Past, present and lessons learned

Future – unpredictable?

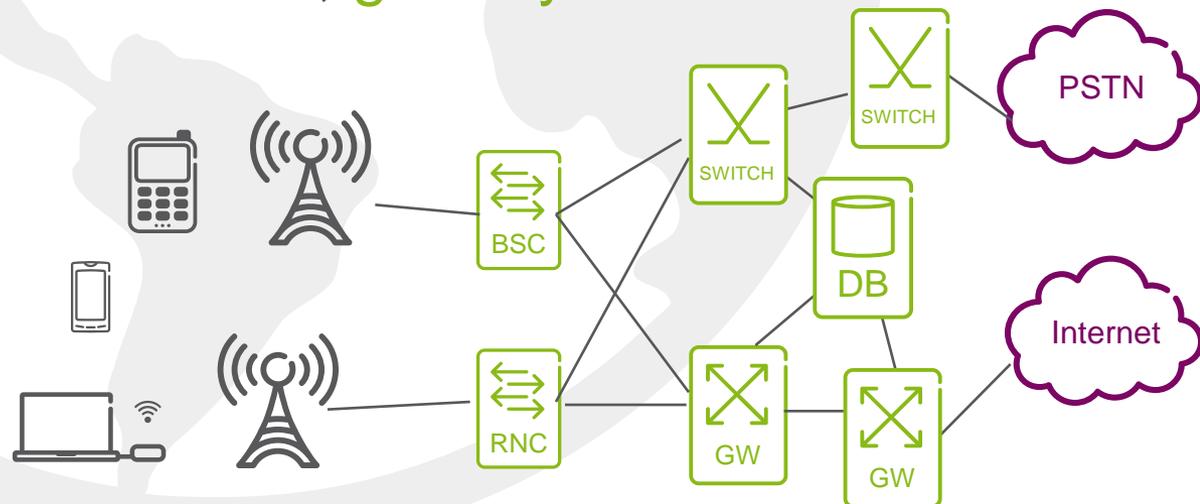
Conclusions



int r o d u c t i o n

Ericsson psirt

- › **Product** Security Incident Response Team
- › No – internal IS/IT network supervision and incidents
- › No – mobile terminals and mobile malware
- › Yes – operator mobile networks, **globally**



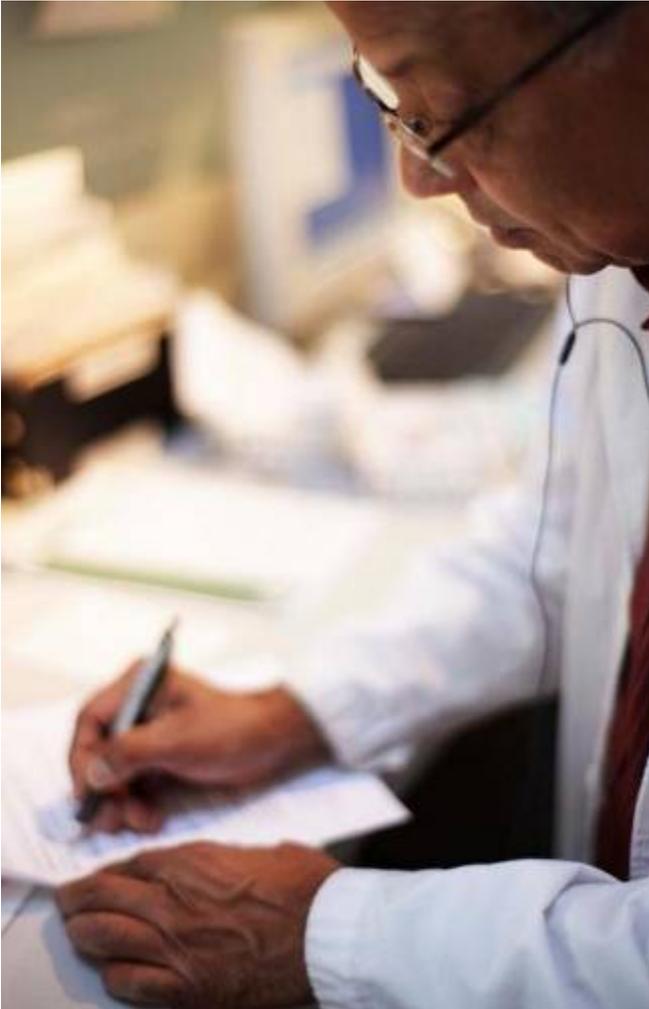
Incident environment for us - past

- › PSIRT receives filtered view of security incidents from operators
- › A case typically starts as
 - "ordinary issue" reported to Ericsson support
 - fraud case
- › Most cases related to (lack of) operational security as of today



Past, present & lessons learned

Case examples



Case 1: A-number spoofing

Case 2: Free surfing

Case 3: Prepaid fraud

Lessons learned

Case 1: A-number spoofing

- › Voicemail eavesdropping or fake SMS messages by spoofing the A-number
- › Most often resolved with proper configuration and number analysis in telecom networks

2010

Phone-hacking scandal: Andy Coulson 'listened to intercepted messages'

The prime minister's media adviser, [Andy Coulson](#), personally listened to the intercepted voicemail messages of public figures when he edited the [News of the World](#), a senior journalist who worked alongside him has said.

SpoofCard

Change Your Caller ID With This App!
Please Only Use 10 Digit Numbers

Your Number:

Number To Call:

Desired Caller ID:

Place FREE Sample Call

Hacking Voicemail!!

Call someone and when it gets to voicemail press * to interrupt the

Now enter one of the following network specific default pins

o2: 8705.
Vodafone: 3333
Orange: 1111
T-Mobile: 1210
Virgin: 7890

SpoofPro

Fake your Caller ID with SpoofPro. SpoofPro, the cheapest caller ID spoofing app in the Android market, allows you to show any number you want on the Caller ID when you make a call. Our industry-leading voice changer allows you to change

SpoofCard
HIDE YOURSELF! BE SOMEONE ELSE!

Your Number

Number To Call

Spoof Caller ID

Place Call Now

Case 2: Free surfing

- › Bypass charging rules for 3G mobile networks
- › Surf free of charge in the Internet

- › How does it work?
 - Use a proxying tool installed on the laptop
 - Exploit zero-rated URLs to bypass charging rules
 - Modify http headers to reflect both 0-rated URL and full URL of the site to be visited
 - › E.g. www.operator_x.com.www.t9space.com

- › How to mitigate?
 - Proper configuration rules for mobile data networks

Case 3: free calls, prepaid fraud

- › Prepaid (roaming) customers making free calls
- › Prepaid balance credits

- › Insiders involved taking illegitimate actions
 - Leaked passwords and group accounts
 - Segregation of duties does not exist

- › How to mitigate?
 - Enforce good user and password policies
 - Good fraud management system
 - Logging activated

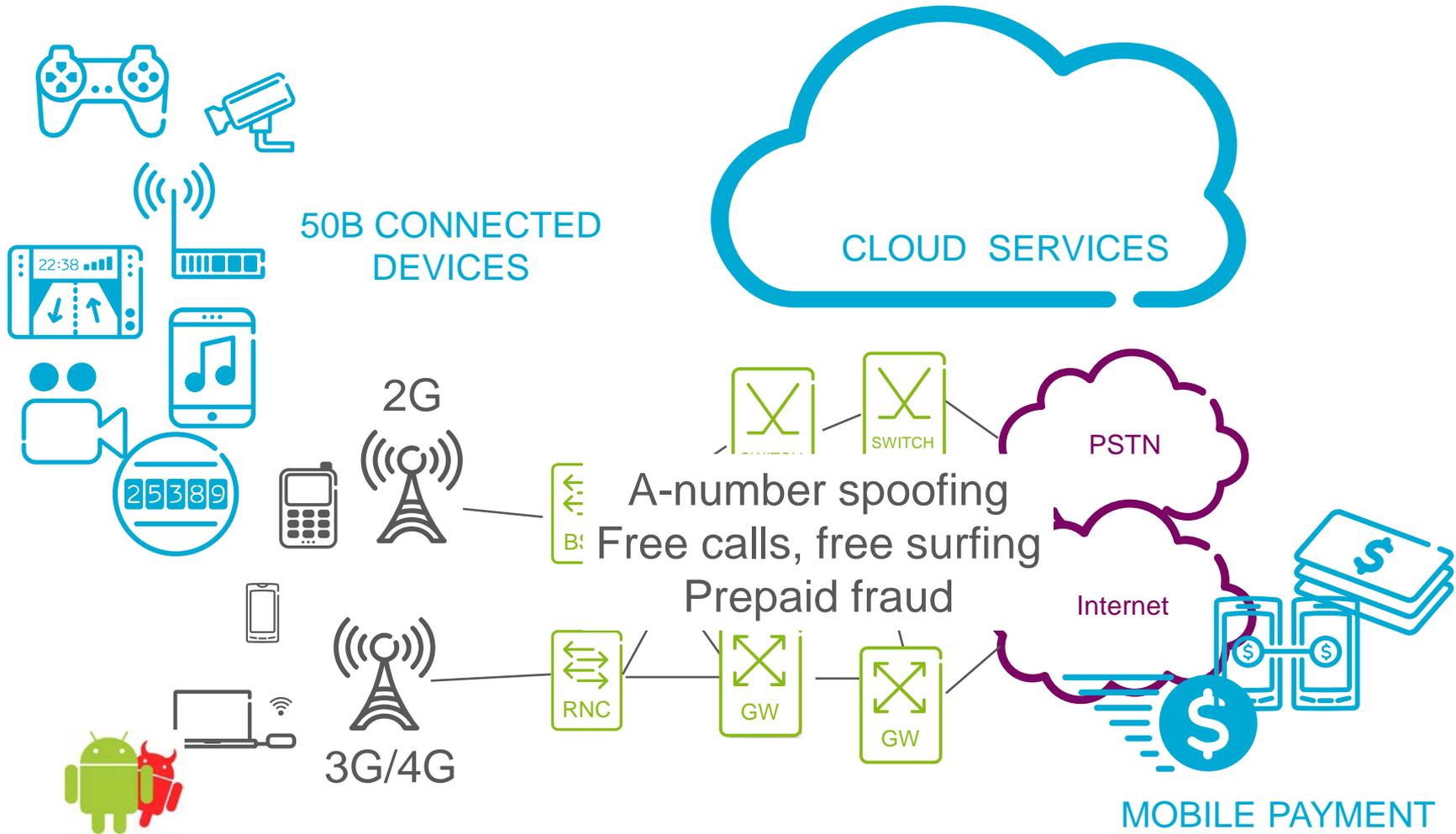
Lessons Learned

- › Main motivation as of today: free calls, free surfing
- › 90% of cases related to (lack of) operational security
- › Insufficient security policies
 - user account handling
 - segregation of duties
 - password policies
- › Logging and accountability not detailed enough
- › Evidence often destroyed during re-starts
- › Communication with other parties during incident investigation may be challenging



Future –
unpredictable?

FUTURE SCENARIOS





Conclusions

New challenges ahead

From one symptom to patterns and scenarios – wide attack surface

Get out of the silo

Lack of operational security will still be main reason for incidents

Co-operation across countries, legal regions and organizations crucial



Questions?





ERICSSON