Security incidents – lessons learned

Mikko karikytö & Anu Puhakainen
Ericsson PSIRT
Outline

Introduction

Past, present and lessons learned

Future – unpredictable?

Conclusions
introduction
- **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
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

50B CONNECTED DEVICES

CLOUD SERVICES

PSTN

Internet

MOBILE PAYMENT

2G

A-number spoofing
Free calls, free surfing
Prepaid fraud

3G/4G

50B CONNECTED DEVICES

SWITCH

RNC

GW

GW

Internet

MOBILE PAYMENT

A-number spoofing
Free calls, free surfing
Prepaid fraud
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?