ITU Workshop on “SS7 Security”
Geneva, Switzerland
29 June 2016

POSITIVE TECHNOLOGIES

Statistics of Vulnerabilities in SS7 Networks

and Ways to Make them Secure

Dmitry Kurbatov
Head of Telecom Security
dkurbatov@ptsecurity.com

1956 2016
CCITT / ITU-T

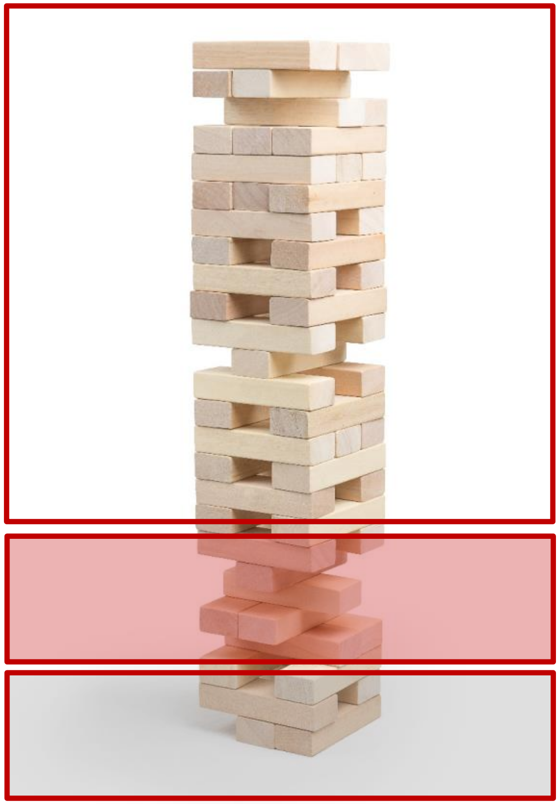
POSITIVE TECHNOLOGIES

ptsecurity.com

ITU

Technology from the 1970s

What we use today and
what technology lies
at the heart of it



Mobile internet
Social networks
Messengers
Online banking
Internet of Things

Mobile communication
developed in the 2000s

SS7 network
developed in the 1970s – 1990s

Summary of the last year

Incidents of attacks on cellular carriers and their subscribers

✓

Greater attention to (in)security in telecom

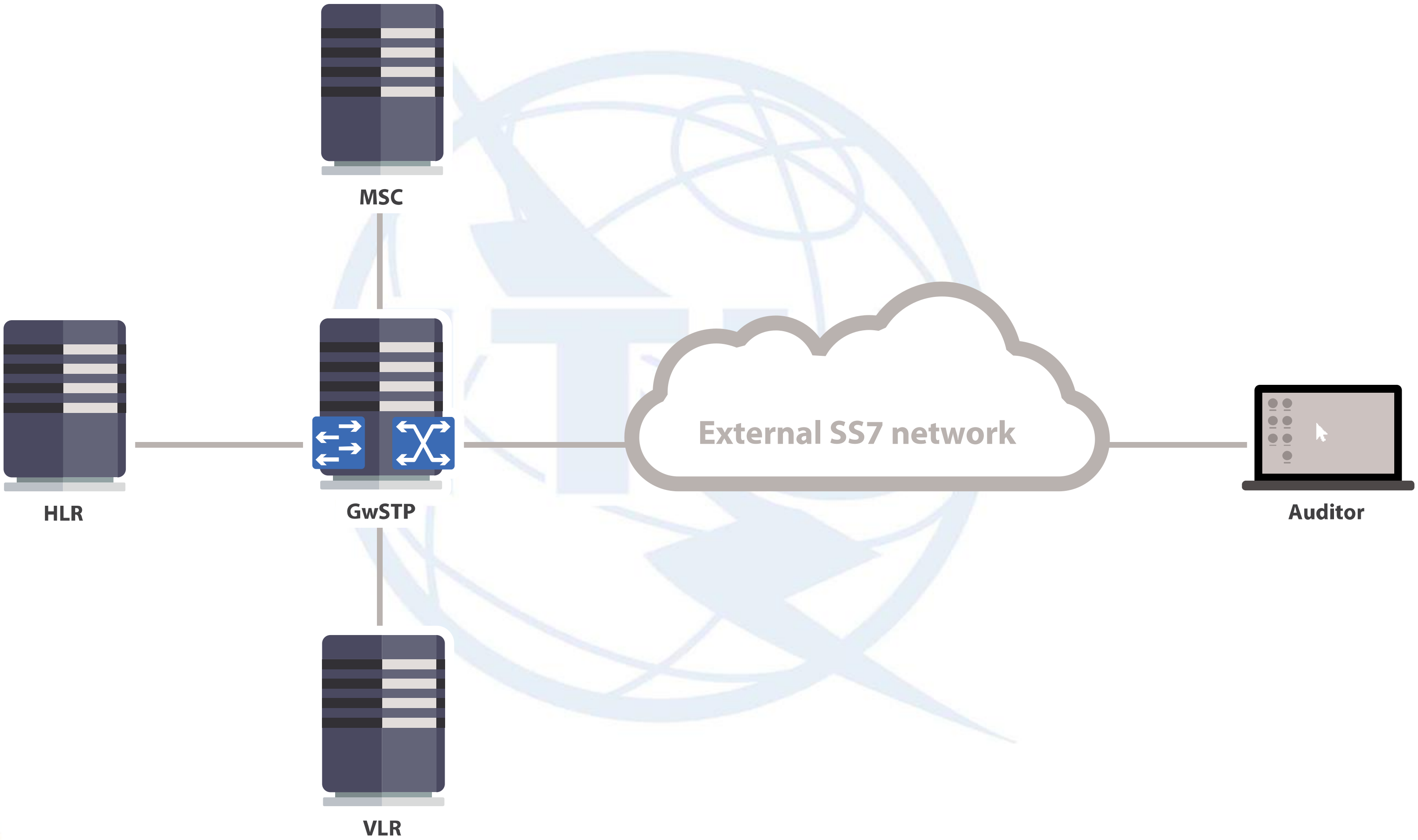
16

16 projects dedicated to security analysis of SS7 networks

!

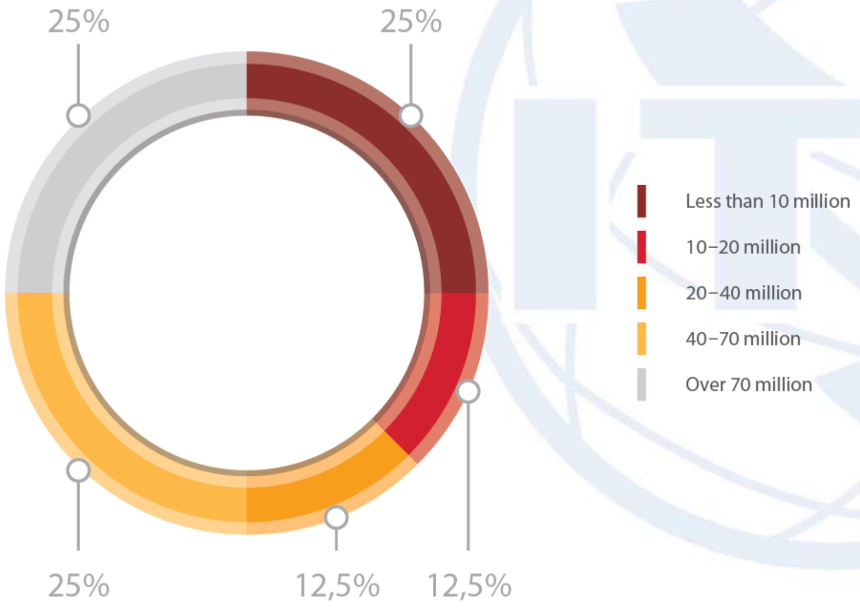
- No mobile network is secure
- Subscriber data is in jeopardy
- Multiple opportunities for fraud and attacks on infrastructure

SS7 Security analysis procedure

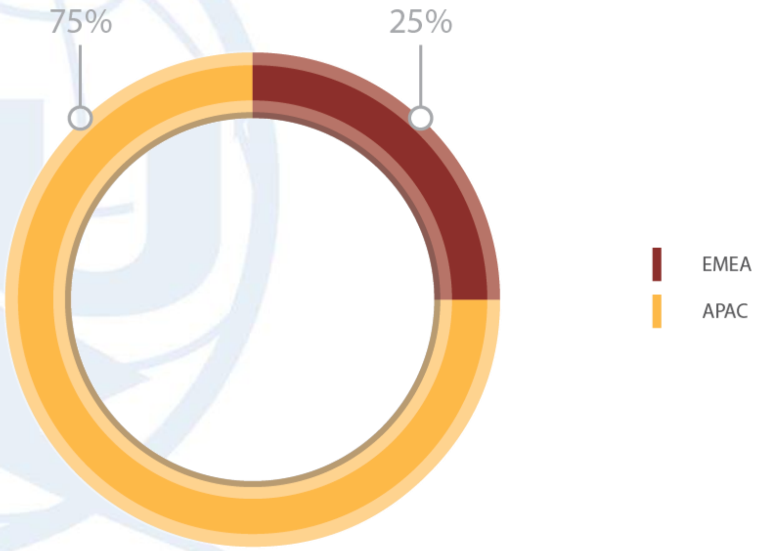


Participant Profile

Distribution by subscriber database



Distribution by region

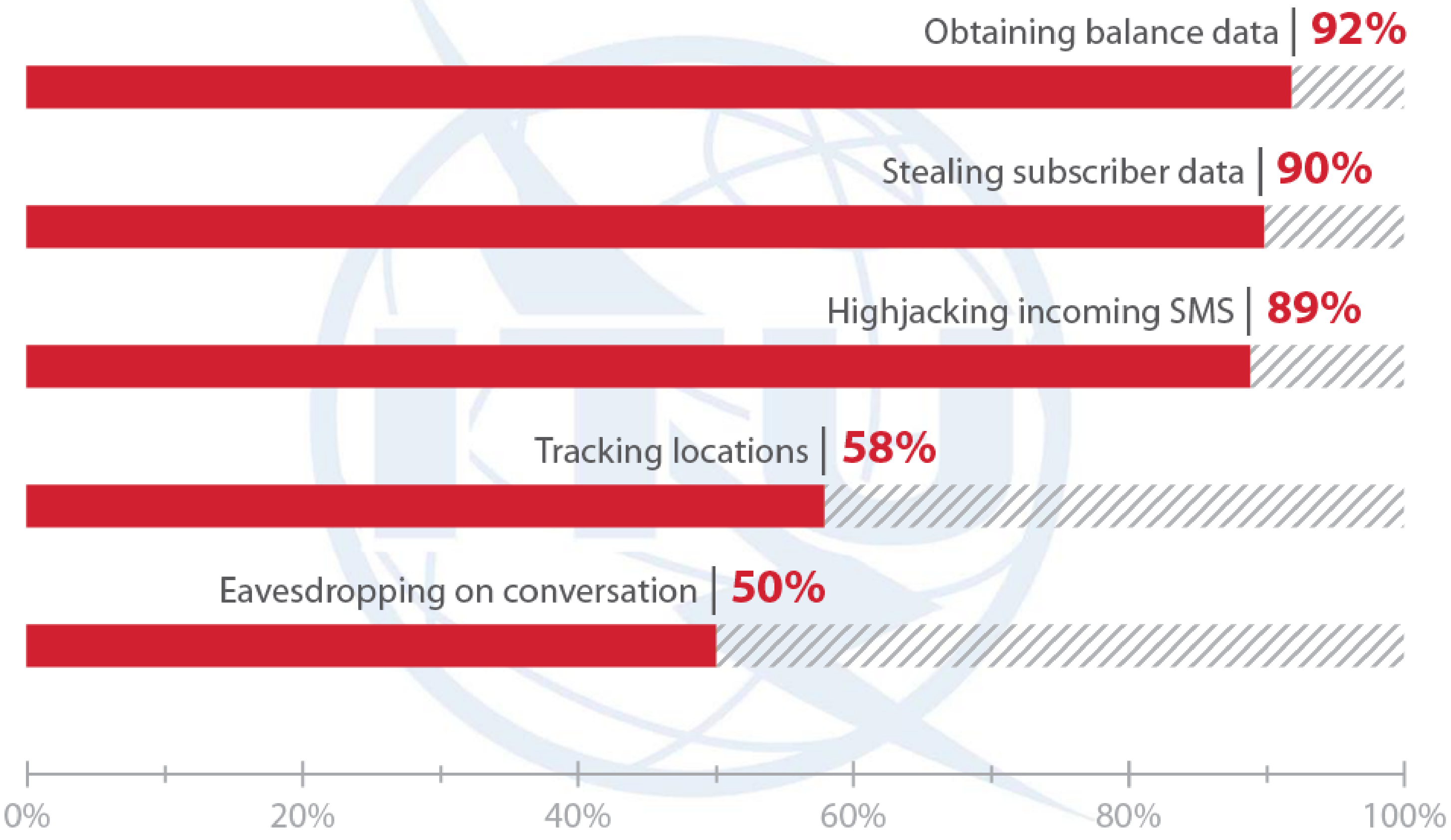


1956 2016 CCITT / ITU-T

POSITIVE TECHNOLOGIES

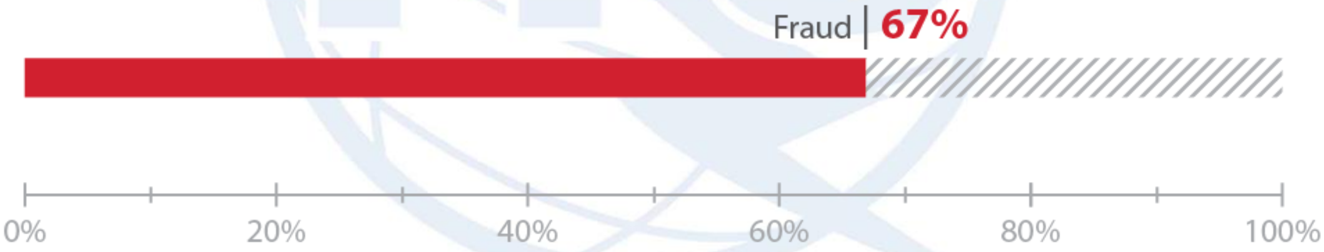
ptsecurity.com

Espionage, Wiretapping, and SMS Interception



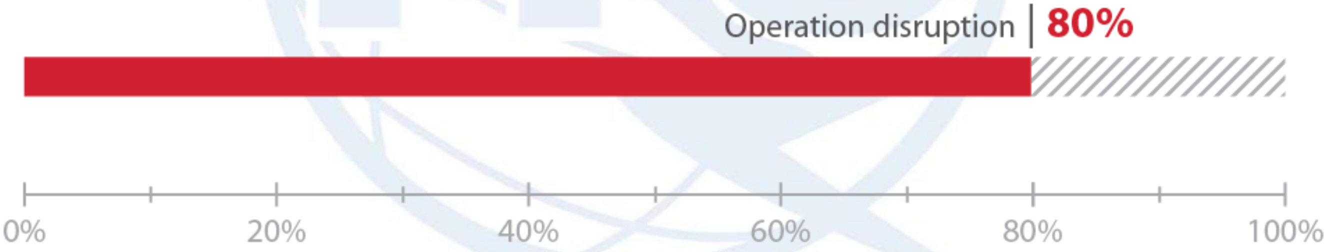
Fraud

- Transferring money using USSD forgery requests
- Stealing money using SMS banking
- Obtaining access to a digital wallet



Operation Disruption

- No access to mobile services (calls and SMS) for a victim subscriber
- No control over IoT devices
- Possibility of mass DoS



Mitigation Strategies / processes and tools

- Filter Cat 1 MAP Messages
- Filter Unused Messages
- Blacklist and Block “bad” GTs

- **Vulnerability management**

  Proactive identification of vulnerabilities by scanning SS7 network perimeter

- **Security monitoring**

  Passive detection of signaling attacks with further investigation and taking countermeasures

- **Compliance management**

  Security assessments and compliance checks of SS7 configurations

Vulnerability management

Conditions:

- Target - Externally addressable SS7 Elements and Subscribers
- Method – Active probing of SS7 elements for known SS7 vulnerabilities

Objectives:

- Determine which Network Elements may be vulnerable to malformed traffic or signaling attacks. Identify the SS7 signaling elements' possible vulnerabilities, attack vectors, and associated issues.

Deliverables:

- Information about existing and potential vulnerabilities
- Recommendations for improving SS7 network security

Security monitoring

Conditions:

- Target - SS7 Network
- Method – Introduction of Security Monitoring (IDS) into the signaling network and analysis of data

Objectives:

- Precise monitoring of the perimeter to get network visibility and investigate if you have experienced, or are experiencing SS7 attacks.

Deliverables:

- **Understanding**
  - What was the attack?
  - What was the target?
  - Where was the source?
  - What was the dynamic and results?
- **Knowledge**
  - Whom to abuse
  - What to block
  - How to plan security investments

Compliance management

Conditions:

- Target - SS7 Network nodes
- Method – Compliance checks across all SS7 Network nodes

Objectives:

- Get automated security configuration assessments and detailed compliance checks across all SS7 Network nodes according to configuration changes introduced by Vulnerability Management Recommendations and Black Lists updated by Security monitoring for attacks

Deliverables:

- Control over vulnerable and misconfigured systems
- Maintain security posture and compliance management of network/services

Total outcome - Threats mitigation

Properly tuned, this activity allows to:

- Prevent degradation or unavailability of service
- Stop leakage of sensitive data
- Investigate and prevent fraud
- Preserve corporate reputation
- Keep revenue

Thank you!

POSITIVE TECHNOLOGIES

ptsecurity.com

1956 2016

CCITT / ITU-T