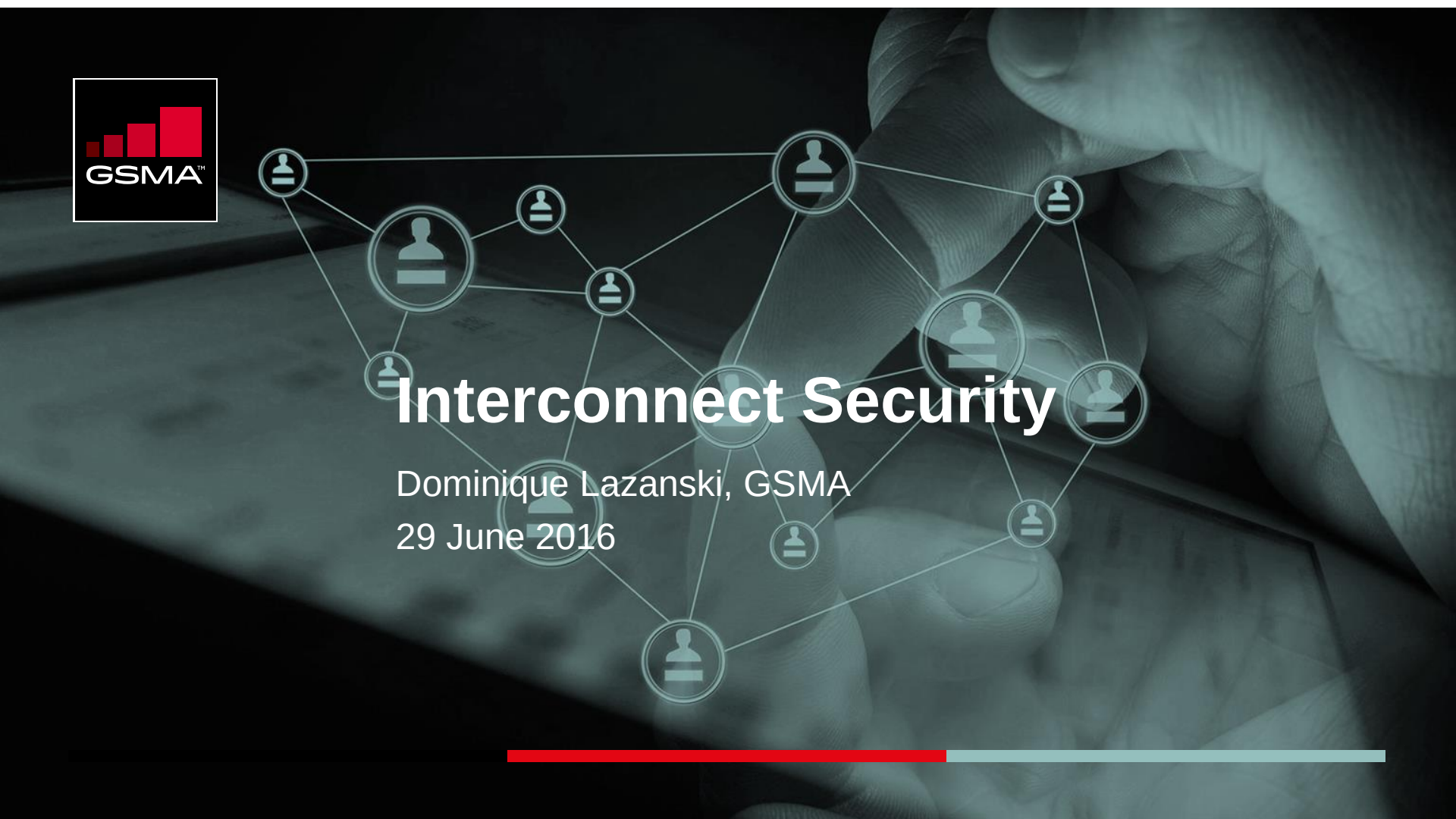


Interconnect Security

Dominique Lazanski, GSMA

29 June 2016

Executive Summary

- Risks to operators and customers from exploitation of SS7-based security vulnerabilities have increased
- Driving factors:
  - More research & publicly available information
  - Increased SS7 network access
- The mobile industry is responding
  - Individual and collective operator action being taken

Agenda

- About GSMA
- SS7 risks
- Implications for mobile services
- GSMA recommendations
- GSMA actions
- Remaining challenges

About GSMA

+ Fraud and Security Group

Fraud and Security Group (FASG)

Drive industry management of mobile fraud and security matters in order to maintain or increase the protection of

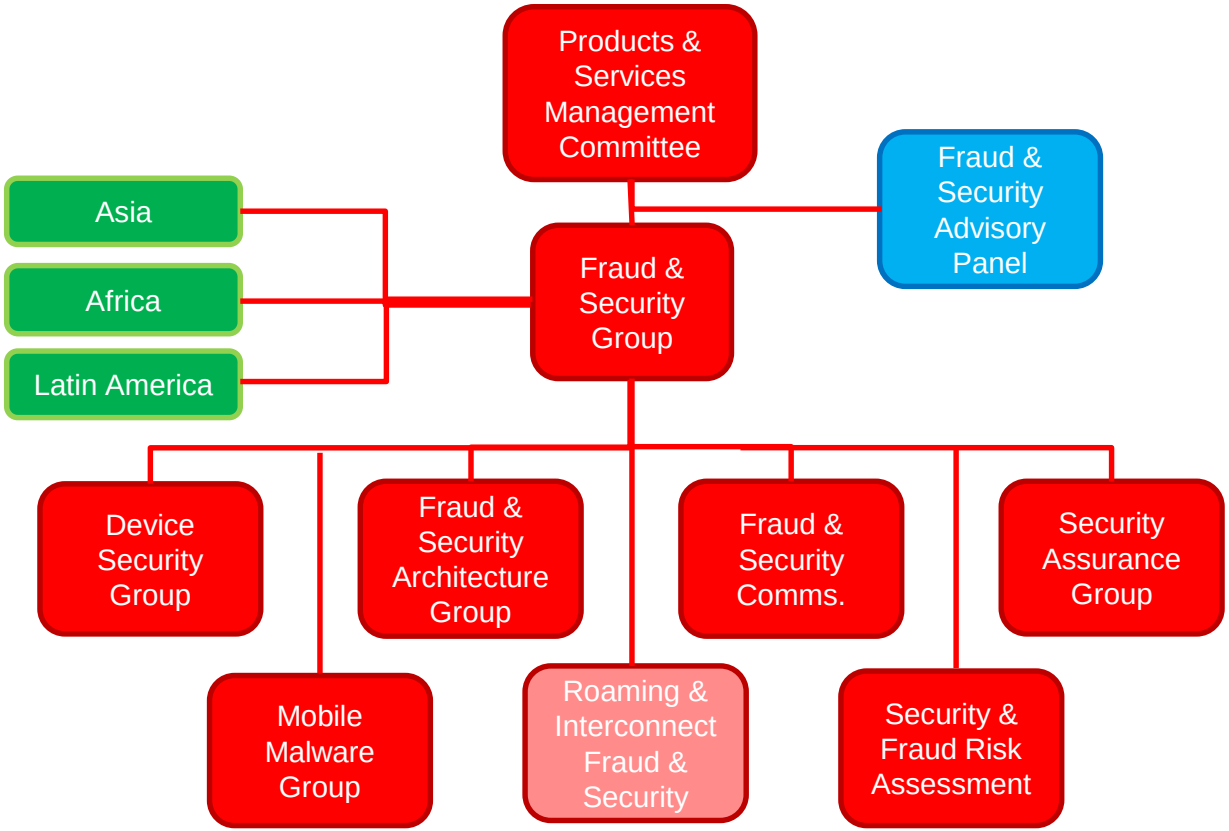
- mobile operator technology and infrastructure
- customer identity, security and privacy

so that the industry's reputation stays strong and mobile operators remain trusted.

FASG Membership

	Total
Individual members	1200
Companies	
Operators	279
Associate members	104

FASG Structure



Interconnect Security Risks

SS7 Vulnerability Research & Awareness

2008: HLR lookups and SMS routing to locate users

2010: Improved user location using false base stations

Aug 2014

The Washington Post

Article on commercial surveillance equipment and services

Dec 2014: CCC Berlin

- Locate Track Manipulate
- Mobile self-defence
- SS7 Map

Aug 2015: Australian TV "60 minutes"

Aug 2015: CBS USA "60 minutes" feature

Media Coverage Sample

The Washington Post

German researchers discover a flaw that could let anyone listen to your cell calls.

ZDNet

Invasive phone tracking New SS7 research blows the lid off mobile security

tom's HARDWARE

Call Privacy Virtually Non-Existent Because Of Poor SS7 Security

60 MINUTES

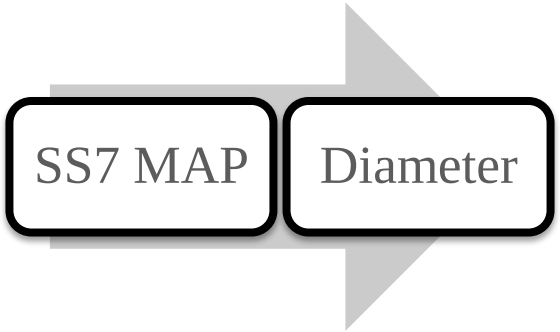
Special Investigation: Bugged, Tracked, Hacked

Increased Risk: Contributing Factors

- SS7 designed without access authentication or integrity protection
- Access easy to obtain
  - Some entities providing SS7 access to others without due diligence, protection or monitoring
- Uncontrolled Global Title leasing
- Unsecured network equipment
- Network misconfiguration causing suspicious traffic
- Lack of home routing deployment
- Inadequate filtering capabilities available & deployed

Results

- Inter-operator signalling connections and packets cannot be trusted
  - Ability to alter, inject, delete messages
- Surveillance potential attracted security agencies
  - Fraud potential is attracting criminals
- Some legacy issues have been taken forward to Diameter security for 4G (LTE/IMS)



Risk Mitigation

- SS7 opportunities are not new but more information now in the public domain than ever before, with:
  - Increased risk of exploitation
  - Anomalies already detected – some leading to financial gain
- Issues need to be identified and isolated
- Impossible to prevent SS7 network access – detection is key
- Industry responding in a comprehensive and coherent way
- Coordination necessary between various stakeholder groups
- Plan of activities developed and undertaken by GSMA

Interconnect Security Implications

Implications for Mobile Services (1)

- Security
  - Location and tracking of mobile users
  - Eavesdropping via man in the middle attack – 2G and 3G
  - Traffic diversion
  - De-anonymization (disclosure of IMSI)
  - Spam

Implications for Mobile Services (2)

- Denial of service
  - Overloading a network node
  - Disconnect customers
  - Send malformed messages
- Fraud
  - Avoid service charges
  - Resell service (e.g. SMS termination)
  - Impersonate a customer

Interconnect Security Recommendations

GSMA Recommendations to Mobile Operators

- Start monitoring:
  - Received MAP messages
  - Messages from non-roaming partners
- Use Home Routing
  - Disrupt location tracking and IMSI discovery
- Filter Incoming Messages
  - Allow only necessary messages
  - Check support at MSC, HLR or STP

Interconnect Security Action

GSMA Actions to Date (1)

SS7 is not broken and it never has been secure

GSMA work is focussed on workaround solutions to compensate for the lack of inherent security

- Alert and briefing paper produced for members
- Educational material on SS7, SIGTRAN & Diameter security
  - SS7 monitoring guidelines
  - Risk mitigation recommendations
- Assessment of current level of exploitation
  - Discussion of operators' monitoring results
  - Understanding senders' motivations

GSMA Actions Ongoing (2)

- Identifying detection capability requirements
  - Support solution development
- Assessing need to amend standards
- Producing guidelines/rules for Global Title access
- Reviewing interconnect contractual and liability issues
- Considering industry compliance programme

Focussed on producing set of defences to protect the industry and mobile users

Interconnect Security Challenges

Remaining Challenges (1)

- Identifying attacks and anomalies is complex
- Security/fraud depts. need to increase signaling knowledge
- Interconnect messaging needs to be accessible & understood
- Investment in tools needed
  - SMS & SS7 firewalls, MAP screening capabilities, trace analysis tools

Remaining Challenges (2)

- Filtering limitations
  - Not all network equipment supports filtering
  - Processing load
  - Not all SS7 messages can be blocked
  - Plausibility checks online/offline
- Not enough to secure your own network
  - Your customers may be vulnerable on roaming partner networks

Why and what's next?

- SS7 access has been, and is, too easy to obtain
- Global Title leasing has gone uncontrolled
- Unsecured network equipment vulnerable
- Network misconfiguration causing suspicious traffic
- Lack of home routing deployment facilitating attack building blocks
- Inadequate filtering capabilities available to & deployed on networks
- Some legacy issues have been taken forward to Diameter security
- Inter-operator signalling connections and packets cannot be trusted

Questions / Discussion

?