Security/FAS – Issues
How to guarantee Safe & Reliable Communications?

i3 forum Technical Workshop : "Collaborating for an IP Future"
Warsaw – June 15th & 16th, 2010

Vincent Hebbelynck – Chairman WS "Fraud"
BICS

international ip interconnection

i3 forum

Agenda

- **Introduction: Why Fraud in i3 Forum?**
- **Assessing the Anti-Fraud Organizations**
- **Securing the Interconnect**

  → Attacks/Misbehaviours to be protected from
- **Extending to FAS with Fight FAS Forum**
- **Conclusion**

Introduction : Why Fraud in i3 Forum?

- **Telecom Fraud is very diversified**
  →From physical subscriber identification to number hi-jacking
- **Lack of representation of international wholesale context in existing organizations**
- **Fraud didn't start with VoIP, but IP lowered entrance barrier for carriers**

→ Need for joined efforts from the carrier community regarding fraud fighting and security recommendations

Introduction : Why Fraud in i3 Forum?

Fraud Workstream established Q4 2009 in the context of i3 Forum

Fight FAS Forum under i3 Forum steering since Q1 2010

Assessing the Anti-Fraud Organizations

- 1st Workstream Task → Identifying the wholes in non-covered international wholesale and VoIP

- Identified Organizations: GSMA FF, ETNO, FIINA, CFCA, Fight FAS Forum

Name	Region	Focus	VoIP focus	Description
GSMA Fraud Forum	Global	Mobile	No	(yet)
FIINA	Global	Incumbents	No	Not specific to international wholesale, major carriers are represented here. From our current understanding, there is no specific workgroup around VoIP international wholesale here.
CFCA			No	Give additionally the possibility to create working
TRMA	North-America	Legal/Finance	No	focus
ETNO	European		No	European centric
Fight FAS Forum	Global	FAS	No	International wholesale focused on FAS

Assessing the Anti-Fraud Organizations

Fraud	Scope	
Category	International wholesale	VoIP
TECHNICAL FRAUD		
Mailbox Hacking (CLI Spoofing)	NA	NA
IMEI Reprogramming	NA	NA
Call Forwarding Fraud	NA	NA
Call Conference /Multi -Party Calls	NA	NA
HLR Tampering / Switch Manipulation	NA	NA
SIM Card Cloning	NA	NA
False Base Station Attack	NA	NA
Spamming (SMS & IP services)	x	x
Phishing and Pharming	x	x
Mobile Malware	NA	NA
GPRS Over-billing	NA	NA
Voice over IP Fraud	x	x
Attacks on Network Interfaces and Components	x	x
Protocol Manipulation	x	x
Client Software	NA	x
False Answer Supervision	x	NA

Securing the Interconnect

- **Fraud Workstream communicated to Technical Workstream uncovered Security Topics**
- **Drafted in Chapter 10 of**

Technical Interconnection Model for International Voice Services (Release 3.0) May 2010

10 SECURITY ISSUES

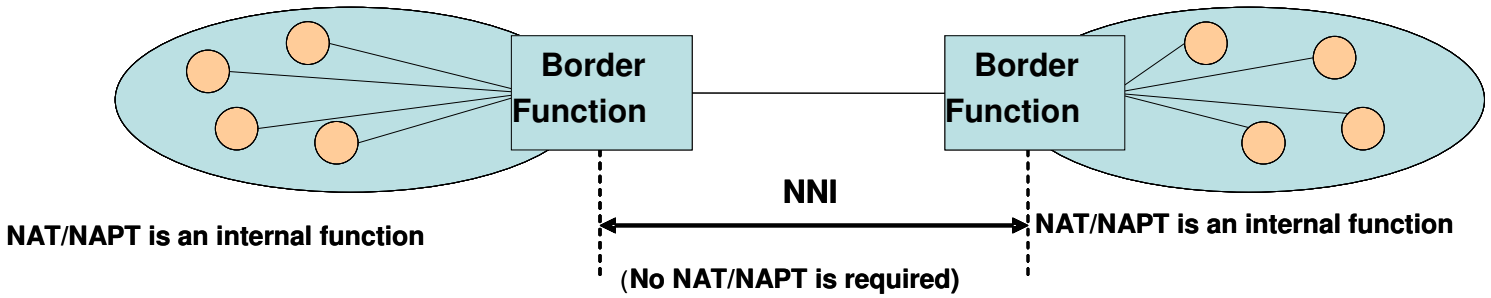
10.1 Network elements for border function

10.2 Security features and capabilities

10.3 Attacks / Misbehavior to be protected from

Securing the Interconnect

- Strongly recommended that all voice traffic coming into / leaving a carrier's network passes through Border Function



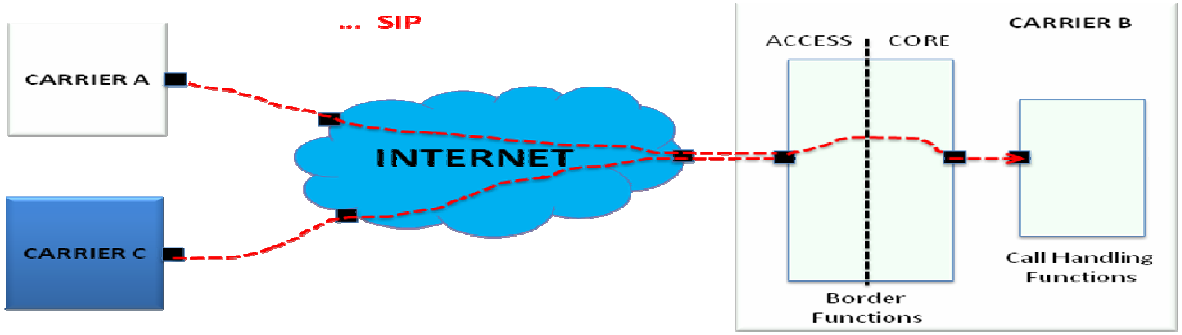
- Encryption
  - Private interconnection: NO
  - Public interconnection: signalling only

Attacks/Misbehaviours

→ **TO BE PROTECTED FROM DOS ATTACKS FROM NOT TRUSTWORTHY IP-ADDRESSES**

- **Impact**

→ Regular traffic between carrier A and carrier B can be impacted because of traffic overload caused by carrier C



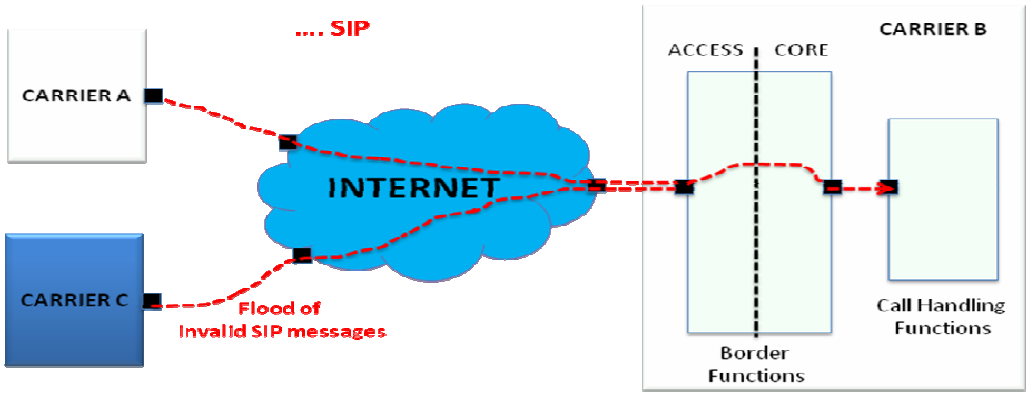
- **Proposed security functions as remedy:**

→ Use of ACL in the SBC which blocks the traffic coming from not trustworthy IP-addresses.

Attacks/Misbehaviours

→ **TO BE PROTECTED FROM PROTOCOL FUZZING**

- **Impact**
  - → These malformed messages can cause overload, memory violation or even crash of the SBC
  - → Risk public/private connection: Risk is higher for public connection

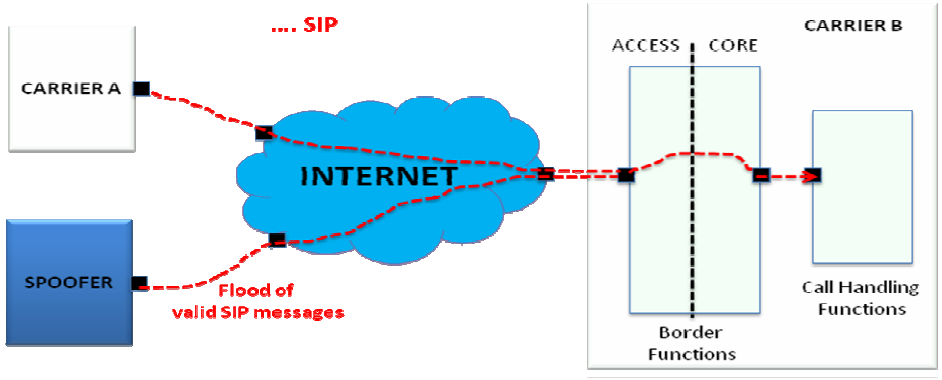


- **Proposed security functions as remedy:**
  - → Deep Packet Inspection

Attacks/Misbehaviours

→TO BE PROTECTED FROM ADDRESS SPOOFING – HIGH AMOUNT OF SIP MESSAGES

- **Impact**
  - → The high amount of SIP messages can overload the SBC.
  - → QoS is reduced

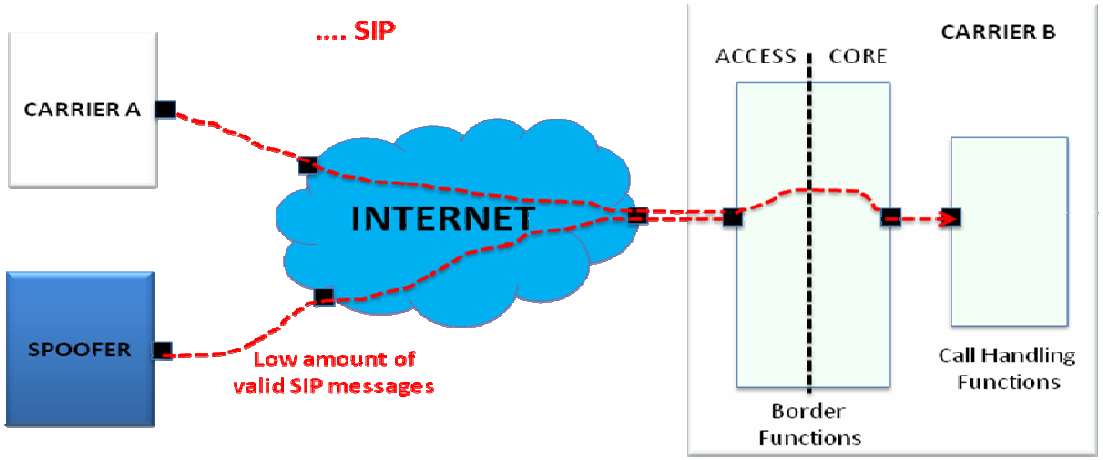


- **Proposed security functions as remedy:**
  - → Traffic policer. Difficulty is to define the threshold as of when to reject calls because this must be based on the traffic profile which is dynamic.
  - → Source authentication via IPSec.

Attacks/Misbehaviours

→TO BE PROTECTED FROM ADDRESS SPOOFING – LOW AMOUNT OF SIP MESSAGES

- **Impact**
  - → In this case, the spoofer uses resources of Carrier A. Since the amount of traffic sent is rather low, this type of fraud is difficult to detect.
  - → Risk public/private connection: Risk is higher for public connection.



- **Proposed security functions as remedy:**
  - → Source authentication via IPSec

Attacks/Misbehaviours

→TO BE PROTECTED FROM THEFT OF SERVICE

- **Impact**
  - → More bandwidth is consumed than indicated in the SIP signaling. E.g. in the SIP signaling it is negotiated that a voice call will be established but in reality a video call is established.
  - → Commercial Fraud: CDRs will indicate a service which does not correspond to reality.

- **Proposed security functions as remedy:**
  - → Deep packet inspection

Attacks/Misbehaviours

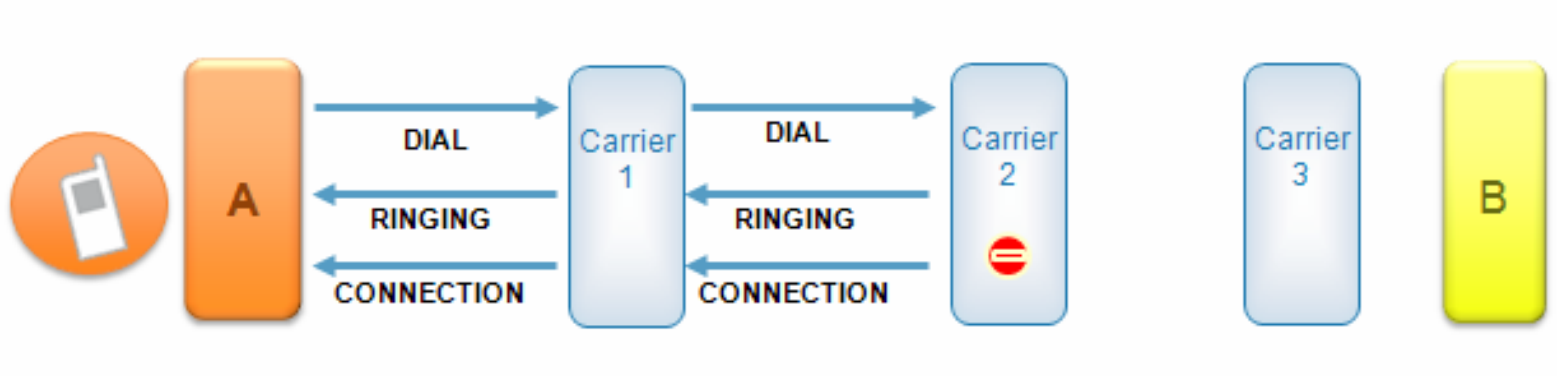
→TO BE PROTECTED FROM ROGUE MEDIA

- **Impact**
  - → Commercial Fraud: CDRs will indicate a call duration which does not correspond to reality. Proposed security functions as remedy
  - → Media traffic filtering

- **Proposed security functions as remedy:**
  - → Deep packet inspection

Extending to FAS with Fight FAS Forum

❑ *WHAT IS FAS?*



- Carrier 2 answers call
- Often disguised message
  - Ring tone
  - “Your call can not be connected” (in language of B party)
  - “Hello.... Hello..... Can you hear me?....”
- Calling party pays
- Very difficult to trace

Extending to FAS with Fight FAS Forum

❑ *THE CHARTER*

- **Provide executive commitment that member will not be involved in the deliberate addition of FAS to calls passing their network and will make every attempt to remove routes with FAS from their network.**
- **Share testing processes and/or methods to detect and resolve FAS supply, as well as test results and the identity of underlying carriers amongst forum members, as well as protect confidentiality of such testing methods from carriers/ operators that are not Forum members.**
- **Use commercially reasonable efforts to adopt recommended basic testing methodologies as well as commit to share test results in a way so defined by the Forum.**
- **Agree to route away from routes testing positive for FAS and only route back to that 3rd party supplier once the FAS has been removed and tests have proven the FAS is removed.**
- **Agree to take immediate action if testing reveals FAS on a route passing through Forum Members' network (this should mean that no member should ever have to remove another member from route for FAS but the problem will get dealt with at the source).**
- **Participate in Forum-led discussions both internally and with equipment vendors / application providers to define tools and systems that allow for the real time detection of FAS.**

Next steps

FIGHT IPRS FRAUD

- Identify fraudulent carriers
- Agree on common liability of carriers and contractual clause

FIGHT FAS FRAUD

- Share tool experience
- Implement common platform for fraud identification

Conclusion

Fraud new workstream since Q4 2009

First tackled subjects:

- Mapping of related industry organizations
- Non-covered security subjects wrt VoIP/International wholesale, recommendations added in interconnection document

Fight FAS Forum under i3 Forum steerco since Q1 2010

Next steps identified

Thank you!