INTERNATIONAL INTERCONNECTION FORUM
FOR SERVICES OVER IP

(i3 FORUM)

(www.i3forum.org)

Workstream “Technical Aspects”

White Paper

Security for IP Interconnections

(Release 1.0) May 2011

Executive Summary

To facilitate the transition to IP of international voice interconnections there is a requirement to ensure that connections are secured properly against security threats and fraud. This document aims to provide an introduction to security for carriers and service providers involved in international VoIP interconnections to help understand the environment, security challenges and appropriate responses.

In order to achieve this goal, this document covers the following:

- ✓ Security Trust Model
- ✓ Current security threats
- ✓ Specific information on threats to IP services
- ✓ Security mechanisms for threat mitigation
- ✓ Security mechanism deployment recommendations
- ✓ Policy recommendations

This document concentrates on security of VoIP interconnections and does not cover organizational IT and network security.

The trust model establishes zones to understand security requirements of devices:

- ✓ **Trusted Zone** – internal network elements solely under the control of the carrier or service provider
- ✓ **Trusted But Vulnerable Zone** – network elements that are placed at the Trusted Zone border that may have shared control
- ✓ **Un-trusted** Zone – network elements in the wider network that have unknown control and configuration

Threats discussed include DoS attacks, network intrusion and theft of service. The particular sensitivities of the service interfaces involved in VoIP interconnections are reviewed for:

- ✓ SIP/SIP-I interface
- ✓ RTP interface
- ✓ SIGTRAN interface
- ✓ ENUM interface
- ✓ Routing & Addressing Provisioning interface

Mechanisms are described and appropriate recommendations are given for the securing of the service interfaces in both:

- ✓ Private-oriented interconnection
- ✓ Public-oriented interconnection

Policy recommendations include the creation of a security code of conduct with an interconnection partner and appropriate processes to handle internal security and fraud.

Table of Contents

Figures:

Matrix:

1 Scope of the Document

The scope of this document is to discuss the security of VoIP interconnection used for the transport of international voice traffic and related services between carriers and service providers. This includes the security of VoIP signalling interfaces using the SIP or SIP-I protocols, VoIP audio path interfaces using the RTP protocol, messaging and signalling services using the SIGTRAN protocol, routing and addressing queries using the ENUM DNS protocol and routing/addressing provisioning interfaces.

This is consistent with the services discussed in the i3 Forum Technical Interconnection Model for International Voice Services [1].

This document is limited to security threats relevant to VoIP interconnections operating as carrier to carrier NNI and service provider to carrier NNI, and the impact on the service interfaces. The document takes into account the relevant literature for VoIP security.

This document does not discuss the requirements for general IT and network security within a carrier or service provider organization except where that is relevant to the security of VoIP interconnections.

This document does not discuss the requirements of local regulations related to network security and the use of the security mechanisms by carriers and service providers.

2 Objective of the Document

The objective of this white paper is to provide helpful practical information for carrier and service provider organizations to secure VoIP interconnections and associated component service interfaces.

The security threats commonly encountered on the Public Internet are described and discussed with reference to the component services of VoIP interconnections. Types of mechanisms for the protection of component service interfaces are discussed and recommendations given for minimum, recommended and optional configurations for applying these mechanisms. Information on security policies appropriate for VoIP interconnections are also given together with information on fraud.

3 Acronyms

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AS/WS	Application Server/Web Server
AUP	Acceptable Use Policy
B2BUA	Back-to-Back User Agent
BGP	Border Gateway Protocol
BSR	Base Station Router
BSS	Business Support System
CDR	Call Data Record
CERT	Computer Emergency Response Team
CHF	Call Handling Function
CLI	Call Line Identification
CPU	Central Processing Unit
Cseq	Command Sequence
DBE	Domain Border Elements
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DPI	Deep Packet Inspection
ENUM	Electronic Numering
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
GSM	Global System for Mobile communications
GSMA	GSM (Global System for Mobile) Association
HLR	Home Location Register
IBCF	Interconnection Border Controlling Function
IBGF	Interconnection Border Gateway Function
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IMS	IP Multimedia Subsystem
IPSec	Internet Protocol Security
ISP	Internet Service Provider
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MAC address	Media Access Control address
MAP	Mobile Application Part
MD5	Message-Digest
MG	Media Gateway
MITM	Man In The Middle
MPLS	Multi Protocol Label Switching
NAPT	Network Address & Port Translation
NAT	Network Address Translation
NE’s	Network Elements
NISCC	National Infrastructure Security Coordination Centre
NIST CSRC	National Institute of Standards and Technology Computer Security Resource
NNI	Network to Network Interface
NOC	Network Operations Center
NTP	Network Time Protocol
OS	Operating System
OSS	Operating Support System
P-CSCF	Proxy-Call Session Control Function
PSTN	Public Switched Telephone Network

RSA	Rivest, Shamir and Adleman (first publicly described source of the algorithm for public-key cryptography)
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SDP	Session Description Protocol
SGF	Signaling Gateway Function
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
SIP-I	SIP with encapsulated ISUP
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SRTP	Secure Real-time Transport Protocol
SS7	Signalling System 7
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network

4 References

[1] i3 Forum ”Technical Interconnection Model for International Voice Services”, Release 4.0, May 2011

[2] ITU-T Recommendation Y.2701 Security requirements for NGN phase 1

[3] ITU-T Recommendation Y.2704 Security mechanisms and procedures for NGN

[4] IETF RFC 3261 “SIP: Session Initiation Protocol”, June 2002

[5] GSM Association IR77 “Inter-Operator IP Backbone Security Requirements for Service Providers and Inter-operator IP backbone Providers“ Release 2.0 15 October 2007

[6] “Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks,” October 2008, ISBN: 978-3-540-89053-9; IPTComm July 2, 2008 published articles by Ormazabal and Schulzrinne, et al: “Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems,” and; “Large Scale SIP-aware Application Layer Firewall (see http://www.springerlink.com/content/b15676j0h4j77708/ and http://www.cs.columbia.edu/~hgs/papers/Yard06_Large.pdf)

[7] ATIS Document ATIS-1000026.2008 Session/Border Control Function Definition and Requirements, August 2008

[8] NISCC Vulnerability Advisory 004033/NISCC/IPSEC “Vulnerability Issues with IPSec Configurations”, May 2005

[9] IETF RFC 2663 “IP Network Address Translator (NAT) Terminology and Considerations”, August 1999

[10] IETF RFC 2401 “Security Architecture for the Internet Protocol”, November 1998

[11] IETF RFC 2246 “The TLS Protocol”, January 1999

[12] NIST (National Institute of Standards and Technology) “Advanced Encryption Standard (FIPS 197)” , November 2001

[13] IETF RFC 5853 “Requirements from Session Initiation Protocol (SIP) Session Border Controller (SBC) Deployments”, April 2010

[14] IETF RFC 3711 “Secure Real-time Transport Protocol (SRTP)”, March 2004

[15] IETF RFC 6189 “ZRTP: Media Path Key Agreement for Unicast Secure RTP”, April 2011

[16] IETF RFC 4033 “DNS Security Introduction and Requirements”, March 2005

[17] IETF RFC 4034 “Resource Records for the DNS Security Extensions”, March 2005

[18] IETF RFC 4035 “Protocol Modifications for the DNS Security Extensions”, March 2005

[19] IETF RFC 1321 “MD5 Message-Digest Algorithm”, April 1992

5 Security Trust Model

This section defines and describes the i3 Forum security trust model. This model is useful for understanding the general requirements for securing VoIP interconnections.

Within the trust model there are 3 security zones:

- **Trusted Zone**
- **Trusted But Vulnerable Zone**
- **Un-trusted Zone**

These zones are defined by the operational control of the carrier / service providers, by the location of the specific network element and their connectivity to other network elements. This model is consistent with the trust model described in ITU-T Y.2701 [2].

5.1 Trusted Zone

The Trusted Zone is a zone where a carrier / service provider's network elements and systems reside. Trusted zone elements and systems never communicate directly with external domains such as the networks of interconnected partners. The following are characteristics of network elements in the Trusted Zone:

- *Located in the carrier / service provider's domain*
- *Under the full and sole control of the carrier / service provider*
- *Communicate only with other Trusted Zone or Trusted But Vulnerable Zone elements.*

However, it should not be assumed that because an element is in the Trusted Zone it is secure, Trusted Zone elements should be protected by a combination of various methods. For example elements may be protected by physical security, system hardening, use of authenticated and encrypted signalling or a separated logical network for communication within the Trusted Zone and with network elements in the Trusted But Vulnerable Zone.

5.2 Trusted But Vulnerable Zone

The Trusted But Vulnerable Zone is a zone where network elements are operated by the carrier / service provider; but are not necessarily fully controlled by that carrier / service provider. The following are characteristics of network elements in the Trusted But Vulnerable Zone:

- *Located within or outside service provider locations*
- *May be under the control of partners, customers or the carrier / service provider*
- *Communicate with Trusted Zone or Un-trusted Zone elements*

The role of elements within the Trusted But Vulnerable Zone is to protect the elements in the Trusted Zone from the security attacks originated in the Un-trusted Zone. Elements within the Trusted But Vulnerable Zone that provide connectivity between the Trusted Zone and Un-trusted Zone, located within the carrier / service provider's domain, are referred to as Network Border Elements. For VoIP interconnections these are Border Function elements.

Elements within the Trusted But Vulnerable Zone should be protected by a combination of various methods, as with Trusted Zone elements.

5.3 Un-trusted Zone

The Un-trusted Zone is the zone which includes the network elements belonging to other carriers, service provider or end customers; all other elements not in the Trusted Zone or Trusted But Vulnerable Zone belong to the Un-trusted Zone. The following are characteristics of network elements in the Un-trusted Zone:

- *Located typically carrier / service provider locations*
- *May be under the control of anybody, including unknown entities*
- *Should communicate with the Trusted But Vulnerable Zone only*
- *Carrier / service provider does not control security policy or may only partially control it*

Elements within the Un-trusted Zone cannot be fully secured by the carrier / service provider.

5.4 Interconnection Trust Model

Figure 1 shows the zones within the trust model applied to an interconnection between two service providers or carriers:

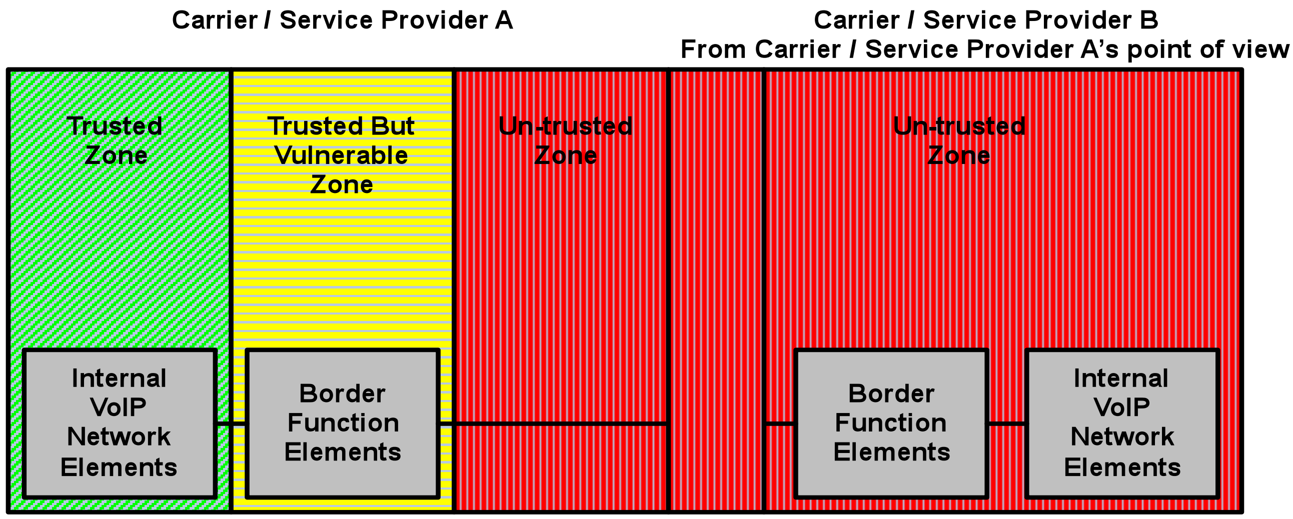
Carrier / Service Provider A
Carrier / Service Provider B
From Carrier / Service Provider A's point of view
Trusted Zone
Trusted But Vulnerable Zone
Un-trusted Zone
Un-trusted Zone
Internal VoIP Network Elements
Border Function Elements
Border Function Elements
Internal VoIP Network Elements

Figure 1: Interconnection Trust Model

The carrier within this model would see the interconnecting carrier or service provider as being within the Un-trusted Zone and equipment used to communicate with the interconnecting carrier or service provider would be in the Trusted But Vulnerable Zone; this is true regardless of whether the interconnection is Public or Private.

In the i3 Forum Technical Interconnection Model for International Voice Services [1] document the general reference architecture is discussed in section 5. The security model can be linked to the reference architecture as follows, with reference to figures 1 and 2 in section 5:

- Call Handling Functions (CHF), Media Gateway and OSS/BSS Systems etc. are in the Trusted Zone.
- Border Functions (IBCF and IBGF) and SIGTRAN SGF are in the Trusted But Vulnerable Zone
- Other carrier or service provider systems are in the Un-trusted Zone.

6 Security Threats

This section discusses some of the threats that may be seen by carriers and service providers using VoIP interconnections:

- DoS/DDoS Attack
- Protocol Vulnerabilities
- Address/Identity Spoofing
- Theft of Service
- Rogue Media
- Session Hijacking
- Network Intrusion
- Internal Network Security

6.1 DoS/DDoS Attack

- Definition

Denial of Service (DoS) attacks aim to make unavailable, or degrade the performance of, network connectivity or services. A Distributed Denial of Service (DDoS) is a type DoS attack which originates from many sources to make it more difficult to mitigate and protect against. This section will use DoS attack to refer to both DoS and DDoS attacks and primarily discusses DoS attacks against signalling and media interfaces present in VoIP interconnections.

There are two classes of DoS attacks:

- General DoS Attacks
- Targeted DoS Attacks

- General DoS Attacks

General DoS Attacks aim to overwhelm network elements and cause the maximum amount of disruption. Methods include message amplification and targeted triggering of resource-intensive tasks i.e. an attacker may flood a Border Function system with fake SIP INVITE messages [4] which will consume large amounts of system resources. Attackers may also attempt to exhaust the capacity of network links to the target elements to prevent access.

- Targeted DoS Attacks

Targeted DoS attacks aim to block access for a particular interconnection or group of interconnections. Methods include launching repeated unsuccessful authorization attempts using the target's identity to trigger activation of network protection mechanisms, such as account lockouts and fraud prevention systems.

Both types of DoS attacks may be combined with Address Spoofing techniques to increase effectiveness; Address Spoofing is discussed in section 6.3.

- Discussion

DoS attacks continue to be a problem on the Public Internet and it is common for attackers to use networks of infected hosts i.e. 'zombie hosts' or 'bot-nets' to create large volume attacks. These attacks can overwhelm load balanced cluster systems and network links when they get very large; attacks have been seen on the Public Internet at the 50Gbps level. Such large scale attacks are very difficult to protect against.

However, attacks against VoIP infrastructure, such as Border Function systems, often require only small amounts of signalling traffic. E.g. a 2Mbps SIP INVITE attack, which can be generated by a single user, could be at a rate of 300 messages per second which may overwhelm unprotected Border Function systems. The effectiveness of attacks may be further increased by targeting exception handling with the target system e.g. by causing authorization failures which are often not optimized which can reduce further the amount of traffic required to disable the system. Attacks may also be handled correctly by Border Function systems, but cause further problems inside the network e.g. in MG systems or SS7 network elements. It is important therefore to be able to protect against attacks of small and medium sizes.

DoS attacks are most likely to occur when Border Function or MG systems are connected to the Public Internet with unsecured network connections. With private interconnections the risk is reduced, but not eliminated, as DoS traffic may originate inside a partner network or can be leaked through routing if BGP network advertisements are provisioned incorrectly. Further, if public and private interconnection systems are shared, e.g. when using a shared VLAN trunk, a DoS attack affecting public interconnections could cause outages for private interconnections.

Mitigation measures include load balancing/clustering to provide sufficient system scale to absorb attacks, the implementation of detection system to analyse attacks, cleaning systems that can use the results of analysis to remove attack traffic and coordination with upstream security teams to remove attacks before they reach targeted network elements.

6.2 Protocol Vulnerabilities

- Definition

Protocol vulnerability threats use intentionally crafted messages to disable a service/system or gain access to a system. This is often associated with the production of malformed messages but may include the generation of messages that have correct syntax but are out of sequence with other messages, which may cause system errors, e.g. by making a software finite state machine confused.

Protocol vulnerabilities can be categorized into the following types:

- Protocol Implementation Vulnerabilities
- Protocol Design and Specification Vulnerabilities
- Architectural Vulnerabilities.

- Protocol Implementation Vulnerabilities

These are normally product specific and include, but are not limited to: default or poor configuration settings; buffer overflows and inadequate or non-existent security controls in the product. Implementation vulnerabilities are “short-term” vulnerabilities since the mitigation strategy is usually provided by the respective vendor within a short time in the form of a patch or workaround. This is normally shorter than the time it takes to address a design or architectural vulnerability, which may involve several organizations including standard bodies and commercial entities.

- Protocol Design and Specification Vulnerabilities

These are weaknesses related to a protocol’s design including: security controls, such as integrity, authentication or confidentiality; message properties, such as headers or values and message flows. Vulnerabilities of this type are discovered by long term usage and may take a long time and be very difficult to mitigate.

- Architectural Vulnerabilities

These consist of weaknesses where the architectural design and placement of network elements and their intercommunications can allow an attacker to launch attacks. These are also discovered over long term usage and difficult to mitigate.

- Discussion

All protocols and associated implementations can be subject protocol vulnerabilities including: SIP/SIP-I, SIGTRAN, RTP/RTCP, IPSec and ENUM DNS. The more commonly used a protocol or implementation the more vulnerabilities that have been discovered and the more likely it is that mitigation for those vulnerabilities exists.

Attempts to exploit vulnerabilities typically enter the network via Public Internet interfaces and may be enhanced by Address Spoofing techniques to defeat security mechanisms such as ACLs. However, they may also originate from public or private partner interconnects due to differences in implementations that allow one implementation to pass unnoticed a malicious packet to a target implementation, because of this sources may be difficult to identify.

6.3 Address/Identity Spoofing

- Definition

Spoofing is where an attacker uses the forged identity of another system or network element to gain unauthorized access or bypass other security mechanisms. In an IP network this identity is typically an IP address or MAC address however, there may be other forms of identity in use, such as dialled number prefixes or reverse DNS records.

- Example: High Volume Spoofing

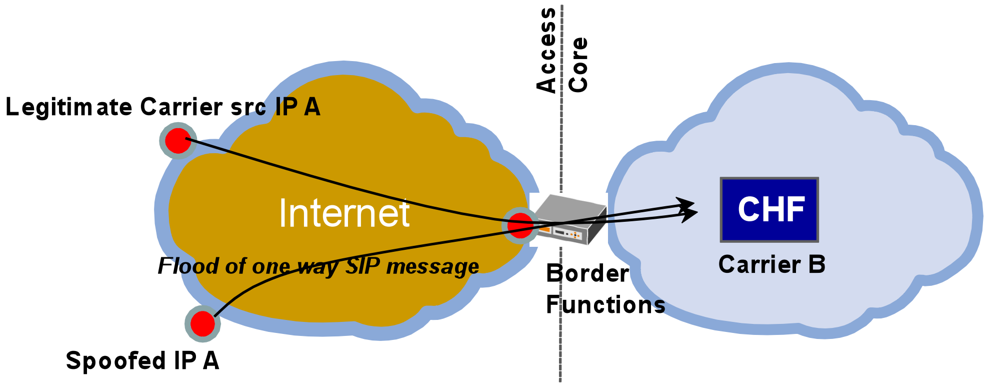

Figure 2: High Volume Identity Spoofing

In this case the attacker uses the source IP address of Carrier A to bypass Carrier B's ACL security between the Un-trusted Zone and the Trusted But Vulnerable Zone and sends a high volume of valid SIP messages. Calls cannot be established as messages will not be sent back to the Spoofed IP address; however the high volume of SIP messages can overload the Border Function system of Carrier B or cause Carrier A to be rate limited. This could be a targeted DoS attack to disrupt the interconnection between Carrier A and Carrier B or a general DoS attack against Carrier B's services.

- Example: Low volume spoofing

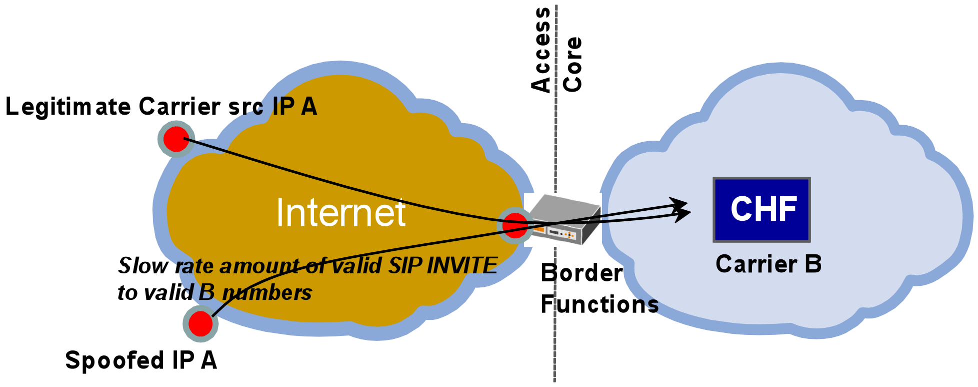

Figure 3: Low Volume Identity Spoofing

In this example the attacker sends a low volume of SIP messages from the spoofed address of Carrier A which will not overload the Border Functions of Carrier B or trigger any rate limiting of Carrier A's traffic. Note: the called number can be randomly distributed in a valid range, so effectively causing the called numbers to 'ring' and therefore reserving resource for short period of time. In this case capacity downstream within the network will be tied up from the incoming call attempts causing issues for Carrier B. This may be difficult to detect.

- Example: CLI Spoofing

In this case the CLI is being spoofed, which is the practice of the falsifying the number and/or name of the calling party. CLI spoofing is used by attackers to hide their identity and to commit fraud. This may be used by interconnecting parties to avoid charges based on identifying the location of the caller or may be used by individual users to bypass authentication schemes e.g. credit card companies may use authentication of caller ID to activate newly issued cards. In the traditional PSTN this was difficult to achieve due to the design of the networks that prevented manipulation of the Caller ID. However, with VoIP services the CLI can be easily manipulated.

- Discussion

Spoofing attacks are often used in combination with other threats to help defeat security mechanisms and gain unauthorized access e.g. network intrusion threats may involve the use of spoofing to defeat ACL security.

Spoofing attacks can affect carriers / service providers that provide services over the Public Internet or private interconnections. Particularly vulnerable, but extremely common, are architectures that only use one parameter to provide identity for security such as the use of only the IP address for authentication. Attacks involving spoofing can often be defeated by the use of protocols that provide strong identity authentication such as IPSec or TLS. However, these security protocols are currently not used widely with VoIP interconnections.

6.4 Theft of Service

- Definition

Theft of service is when an end user, partner carrier / service provider or other organization fraudulently obtains service without paying for it e.g. this may be where a 3rd party breaks the authentication scheme being used and manages to send traffic without being identified correctly and is therefore not billed for the traffic.

- Example: Wholesale prefix theft

Common methods currently used to secure the exchange of VoIP traffic between carriers / service providers are vulnerable to attack. E.g. in one incident attackers targeted a legitimate voice wholesaler engaged in the buying and selling of traffic; the attackers used a brute force scheme to find the prefixes, which were between 3 and 9 digits in length, used to identify the originating carrier / service provider by the target carrier. The prefixes were passed over the Public Internet without encryption and the target carrier checked the prefix to identify if the traffic came from a known partner or customer. If the prefix was valid the target carrier permitted the traffic to continue into their network without further security checks. The attackers then used the prefixes of other entities to send traffic through the target network without being billed, the bill for the traffic being sent to the carriers or service providers who the prefixes belonged to.

- Discussion

A complicating factor in tracing theft of service in the VoIP environment is the lack of fixed locations from which traffic originates. In the PSTN network, incidents could be more easily traced back to fixed points of interconnections, originating trunks, or subscriber lines e.g. if a user was to call from a phone and provide fraudulent billing information there was a location which was useful to investigate from. In VoIP traffic can be readily moved from one ISP to another and can take advantage of multiple routes through the Internet by the use of relaying and proxying. When fraud has been committed the target carrier / service provider can often only conclude that fraud has happened; in many cases carriers / service providers lack the means to detect and shutdown fraudulent VoIP activity.

Theft of service can also originate from partner carriers and service providers that may themselves have inadequate security and so can occur on private interconnections as well as the Public Internet.

VoIP carriers and service providers need to have the ability to build a comprehensive view of what is happening in their networks. By having a network-wide, end-to-end view service providers can detect fraud and abuse, correlate events, take action, and successfully perform forensic analysis.

6.5 Rogue Media

- Definition

Rogue media is when RTP traffic is received that is not associated with an active call / session. In relation to SIP this would be where an RTP flow occurs before a corresponding SIP session has been established, or RTP flow continues after a SIP session has ended.

- Example

An example rogue media attack would be to send a small amount of traffic to a large range of RTP ports available on a particular Border Function IP address, perhaps from a spoofed IP address bypassing ACL security that is in place. This traffic will cause distortion of audio or video of RTP sessions on that Border Function.

- Discussion

Rogue media can be used to disrupt calls due to unauthorized use of UDP ports in RTP, acting as a DoS attack and degrading audio quality. Depending on implementation it can also affect the billing of calls by interfering with call duration calculation and can be used as a potential attack vector for protocol vulnerabilities or session hijacking.

Rogue media is mostly likely to occur on elements with Public Internet interfaces which allow RTP packets to be received from external sources.

6.6 Session Hijacking

- Definition

Session Hijacking or Man-in-the-middle (MITM) attacks are where the attacker inserts himself in the communication path between two network elements or networks. To the first element the attacker appears like the second element and to the second element the attacker appears like the first element. The attacker can act transparently, simply relaying messages between the first element and the second element. If confidentiality protection is not used the attacker can eavesdrop on the communication. If integrity protection is not used the attacker can manipulate the messages. The attacker will also have the opportunity to compromise the authentication exchange, since this will be performed prior to confidentiality and integrity protections being in use.

Eavesdropping can also exist outside of Session Hijacking scenario; this will be discussed in more detail in the next release of the whitepaper.

- Example

Session Hijacking can be implemented by corrupting the routing tables or address resolution caches of service provider / carrier systems on either side. This can then be used to hijack calls either for the purposes of eavesdropping or for theft of service. The attacker can also cause issues with audio or video quality by changing values in RTP protocol packet headers such as the sequence number.

- Discussion

MITM attacks are sophisticated attacks that can be used to disrupt interconnections between carriers or service providers in a DoS attack and can also be used to commit fraud or perform network intrusion.

Session Hijacking / MITM can also be an effective attack in situations where confidentiality protection is used, but integrity protection is lacking. In May 2005 NISCC issued a vulnerability advisory [8] for IPSec when making use of the Encapsulating Security Payload (ESP) configuration using tunnel mode with confidentiality only or with integrity protection provided by a higher layer protocol. In this case by making careful modifications to select portions of the outer packet payload, controlled changes to the header of the inner packet payload could be achieved. When processed by the security gateway, the inner packet may be redirected or incorporated as part of ICMP messages in clear text, making the content of the communication potentially available to the attacker. This is not an implementation bug; it is an undesirable interaction compliant with the protocol rules. A possible work around is to only use IPSec with both confidentiality and integrity protection.

6.7 Network Intrusion

- Definition

Network Intrusion, or unauthorized access, can refer to a number of different attacks where the goal is to gain access to some resource inside the network. It is a general security problem for all types of entities that present Public Internet interfaces or interconnect with other networks.

- Discussion

Attackers can exploit many possible entrance points for network intrusion e.g. the service provider / carrier interconnection itself, intranet or extranet tools used by employees and partners or management networks used by software or hardware vendors. Once an attacker has gained access into a service provider Trusted Zone the attacker can then compromise more systems / networks, including internal organization systems, or engage in theft of service. This can result in VoIP fraud and the smuggling of unauthorized traffic through carrier / service provider networks due to the inability of the carrier / service provider to adequately monitor and detect intrusion through interconnection. In addition, the interconnection of VoIP networks with the PSTN may introduce new risks that the PSTN is not equipped to handle. This may result in new types of PSTN attacks, exploitation, and other negative consequences.

Protecting the network at various levels can help to prevent unauthorized access. At the network layer the use of Border Function systems can provider additional protection, but hackers are getting smarter all the time and this may not be sufficient. Using access control at the network and application level with appropriate authentication and authorization can also minimize the risks of unauthorized access.

6.8 Internal Security Issues

- Definition

Internal security issues refer to unauthorized or improper use of network resources attempted by users within the carrier / service provider organization. Internal security incidents can also involve external parties who are working with an internal user to compromise network security. Internal users may not always be deliberately be acting in unauthorized manner, the changes can be inadvertent and in error.

The most common examples are presented below, for further examples please see Appendix A – Internal Security Examples -.

- Example: Incorrect Source Address

To create a typical VoIP interconnection each IP belonging to Customer A needs to be explicitly configured in the border function of Carrier B. However, it is also possible for an internal user to add into the configuration addresses that do not belong to Customer A.

Traffic coming from the additional IP address, “X” will be considered as valid by the border function and terminated through the network, and be billed under Customer A’s account. This is shown in Figure 4 below.

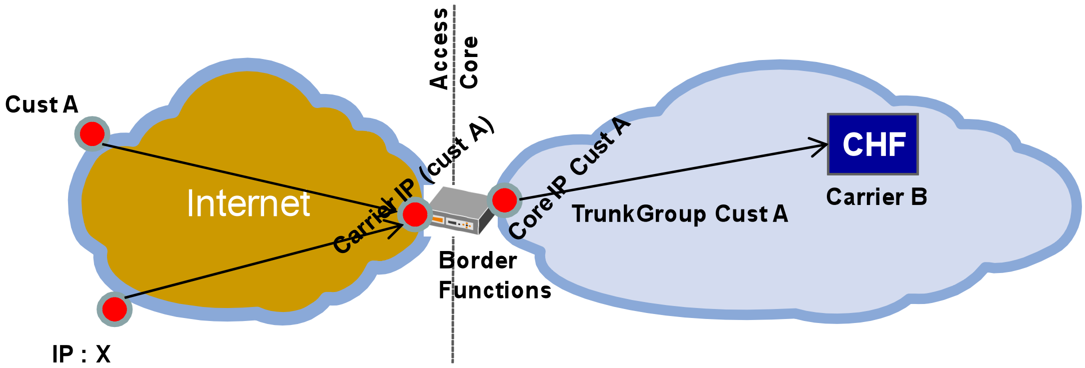

Figure 4: Incorrect Source Address

This will cause theft of service and fraud, which the carrier will only have limited ability to resolve.

I3 Forum members have reported that 3rd parties have attempted to get additional IP addresses configured in carrier Border Functions in this way. One example seen is to bypass the normal provisioning processes, contacting the NOC to report a technical problem; the Carrier NOC unwittingly causing a security incident.

- Example: Border Function Traffic Mixing

In this example two interconnects are configured: one to Customer A and another to Customer B, with both A and Bs addresses configured in the border functions. However, all or a portion of the traffic from Customer B traffic, such as for particular destinations or during particular time periods, is presented to the onward network as coming from Customer A. Figure 5 below shows this situation.

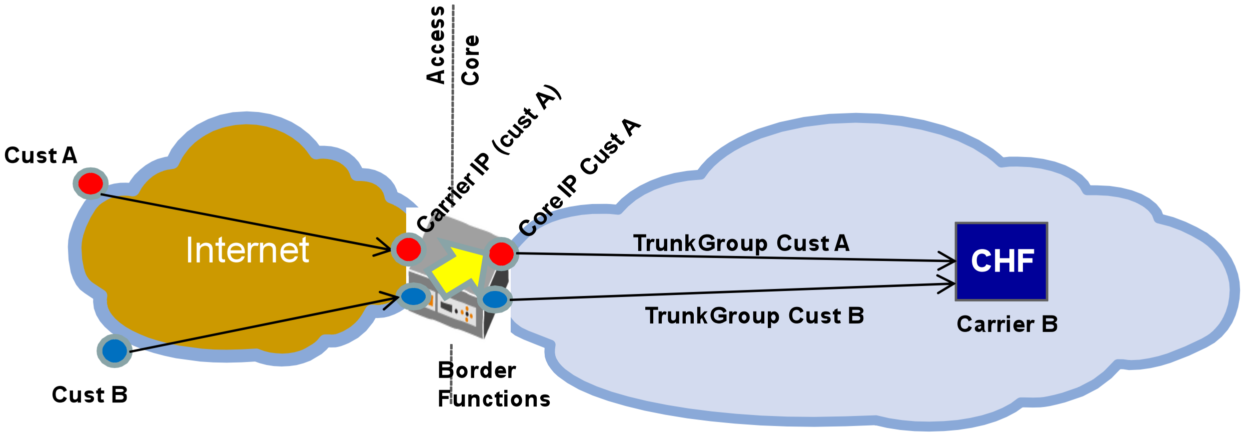

Figure 5: Border Function Traffic Mixing.

In this scenario, Customer B is defrauding Customer A and the carrier.

This scenario takes advantage of the existence of routing functions that are sometimes available in external Border Functions: the Border Function can be seen as a small standalone VoIP to VoIP switch, with its own local routing table, totally independent of the CHF of Carrier B. In this situation it is relatively easy to "mix" traffic towards the CHF and make traffic from Customer B appear as actually coming from Customer A.

- Discussion

Fraud or billing disputes are the main problems associated with the compromise of security by users within the organization and may occur over both Public Internet and private interconnections.

Internal issues can be mitigated by implementing logging and auditing of Border Function CDRs, logs and configuration and by having strong internal processes related to Border Function provisioning. For example to deal with the problem of incorrect source addresses a process can be setup to automatically perform Border Function system configuration audit against an "official" IP address list. Similarly to deal with the problem of Border Function traffic mixing CDRs can be compared between the Border Function system and the CHF.

7 Review of Service Security

This section discusses the security issues and types of attack that may occur for each of the different interconnection services discussed in the i3 Forum Technical Interconnection Model for International Voice Services document [1]:

- Voice Services
- SIGTRAN Services
- Routing & Addressing Query Services
- Routing & Addressing Database Provisioning Services

Mechanisms and recommendations to mitigate the issues discussed in section 7 are provided in sections 8 and 9.

7.1 Voice Services

Voice interconnection services are subject to all of the threats discussed in section 6, sometimes combined together in new ways to cause problems for the carrier / service provider network.

There are two particular problems that Voice interconnection services are particularly susceptible to: large scale theft of service / fraud and the impact of relatively low level DoS attack traffic.

7.1.1 Theft Of Service & Fraud

Voice networks bill by the minute or second and have a relatively high cost of termination which creates an environment in which large amounts of fraudulent money can be generated by attackers quickly and without consequences to themselves. This increases the temptation to work on new theft of service attacks with which to defraud carriers and other service providers. These attacks have already been very successful, as discussed in section 6.4. The resulting financial impact can be very large and the attack is often too quick to spot easily before it becomes significant. Further, it is often possible by discovering a small amount of information from inside a carrier network, e.g. from an employee, to bypass the simple security schemes which are often employed to counter these issues. Some of the numerous ways to do this are discussed in section 6.8. Carriers / service providers should protect themselves from fraud by configuring security mitigation mechanisms in combination with each other and carefully analyzing system architectures to prevent exploitation.

7.1.2 DoS Attacks

Voice interconnection equipment is often poorly prepared to deal with the large volume of requests generated by even a low level DoS attack from a small number of hosts, especially if that attack is properly targeted. This is due to the complexity of Voice routing and accounting mechanisms, which are implemented in software layers rather than hardware. Also, in some cases the equipment is older and was designed for SS7 signalling interconnection or connection to a limited and controlled VoIP domain. Therefore, interconnection equipment has a limited ability to absorb large request volumes especially if the traffic is accompanied by protocol vulnerabilities or the deliberate causing of exception conditions within the software. As a result voice infrastructure must be protected by mechanisms that can provide methods for controlling traffic and protecting critical Voice infrastructure. DoS attacks have great potential to generate significant financial losses for the carrier / service provider in the event of a prolonged attack.

7.2 SIGTRAN Services

Networks using SIGTRAN and SS7 protocols for the delivery of signalling or messaging services have not yet seen significant security incidents related to the underlying protocols used for the interconnection. This is probably due to the use of SIGTRAN only inside the carrier / service provider network or over a private network connection between two partners. The relatively obscurity of SS7 protocols may also be a factor in the lack of incidents. However, it should not be taken that this guarantees that SIGTRAN interconnection relationships could not be disrupted by MITM or DoS attacks. In addition, the financial risk could be significant if the SIGTRAN infrastructure is not properly secured.

There is also the risk of the SIGTRAN / SS7 network and elements being overwhelmed by relatively small numbers of requests which may originate in connected IP networks. Like Voice routing systems, of which SIGTRAN and SS7 networks may be a part, SIGTRAN and SS7 involves complicated processing in software layers often on legacy equipment with limited CPU resources or interconnection bandwidth. These may represent weak spots within a carrier / service provider network that can be exploited to disrupt or damage services.

7.3 Routing & Addressing Query Services

Routing and addressing query services can be provided using a variety access protocols: ENUM/DNS, SIP and SS7 INAP or MAP protocol over SIGTRAN. The security issues surrounding query services are therefore related to the security issues of the query protocol used. This section will discuss only the ENUM/DNS query protocol.

All query services regardless of protocol may be subject to theft of service depending on the commercial model chosen for the service. If query services are provided in a similar way to HLR access provided on GSM mobile networks where queries are non chargeable, but calls and messages that are terminated from the results of successful queries are, then a situation may develop where large numbers of queries are completed without actually traffic being offered to the service provider or carrier for termination. E.g. networks can be exploited for the harvesting of number portability data. Due to this it will be important to make sure that interfaces are secured against unauthorized access and provide accounting so that usage can be checked for abuse.

7.3.1 ENUM/DNS

ENUM/DNS security issues are the same as those of general DNS services on the Public Internet. DNS services are prone to DoS attacks, particularly those involving address spoofing techniques and protocol vulnerabilities. These attacks have not yet been seen on ENUM/DNS deployments largely due to the relative immaturity of the ENUM infrastructure which is not yet a widely deployed critical piece of carrier / service provider networks. However, attacks against DNS, perhaps using existing DNS attack scripts and programs, may quickly be applied against ENUM systems.

7.4 Routing & Addressing Database Provisioning Services

Provisioning interfaces for routing and addressing databases have the potentially to be delivered across a very wide variety of implementation protocols, the exact discussion of which is beyond the scope of this white paper. A provisioning service may be implemented across a SOAP web service interface or across a file based interface such as FTP. However, in general issues are related to network intrusion, session hijacking and theft of service.

The provisioning interface must be secured against being a mechanism for intrusion into the network i.e. if it is possible to replace or change E.164 record entries in the routing and addressing database this may be used to gain access further into the network.

Similarly, the provisioning database must again be secured to prevent session hijacking from being carried out on a subscriber or against the carrier / service provider. For example, a possible session hijacking could be the replacement of an E.164 record and then a redirection of RTP traffic to allow the insertion of the attacker into the media path, allowing the attacker to listen in to or alter audio or video data.

Theft of service scenarios may involve session hijacking to cause calls to be identified incorrectly to the carrier network or the theft of actual data such as number portability or subscriber data.

8 Security Mechanisms

This section discusses the various mechanisms available for protection of the services utilized for VoIP interconnection. These mechanisms can be used with either Private or Public VoIP interconnections. The following mechanisms are discussed:

- Topology Hiding
- Encryption
- Authentication
- Access Control Lists
- Reverse Path Filters
- Traffic policing
- Application Level Relaying
- Deep Packet Inspection
- SRTP
- DNSSEC
- Media Filtering
- Firewalls
- Intrusion Detection Systems
- Device Hardening
- Logging and Auditing
- Security Information & Code Updates

Each mechanism will be defined, implementation will be discussed and issues related to deployment discussed.

8.1 Topology Hiding

- Definition

Topology hiding is the function which allows the hiding of network element addresses from third parties as well as obscuring the architectural layout of those elements; this is undertaken to hide the elements within the Trusted Zone.

- Implementation

Hiding IP addresses can be implemented by the NAT/NAPT mechanism [9], which is applied at the IP level and involves the translation of addresses and ports from their original values. NAT/NAPT also requires changing the addresses and ports carried within signaling messages at the application layer to ensure that signaling protocols function correctly. NAT/NAPT is applied at the Border Function within the Trusted But Vulnerable Zone for both signaling traffic and media traffic; NAT/NAPT makes only Trusted But Vulnerable Zone network elements visible to the external interconnection partner.

- Discussion

Topology hiding using NAT/NAPT makes it hard to discover infrastructure within the Trusted Zone to target to further an attack. Also it is often not possible to send packets directly to devices behind the NAT/NAPT layer as networks may not be reachable due to the use of private addresses or not being in BGP. NAT/NAPT translations require to be explicitly configured and so can also provide a protection against inadvertent configuration of unsecured network services. Correctly configured NAT/NAPT has no impact on functionality and is transparent to the interconnecting parties. Topology hiding in VoIP interconnections is normally implemented in the Border Function functional blocks.

8.2 Encryption

- Definition

Encryption is the encoding of data to prevent the contents from being decoded by an unauthorized party; encryption is typically used across the Un-trusted Zone from the Trusted But Vulnerable Zone.

- Implementation

There are two main methods used for encrypting information in relation to interconnections: IPSec as specified in [10] and TLS (Transport Layer Security) as specified in [11].

IPSec provides for encryption at the network layer between two devices by forming a tunnel and encrypts IP traffic that uses the tunnel; the devices can be router systems, VPN devices or Border Function systems. The IPSec protocol also provider authentication. IPSec can be used with AES encryption [12] or other ciphers.

The TLS protocol is available to encrypt specific application protocols and does not encrypt the lower layers; for the SIP protocol is provides both authentication and encryption. It is also available for ENUM DNS and other protocols. TLS is implemented by Border Function systems or other application layer aware network elements.

- Discussion

Both the IPSec and TLS protocols provide for authentication and encryption to protect against MITM type attacks and the packet capture of sensitive data. However the use of IPSec or TLS as encryption protocols requires significant computational resources. For SIP/TLS the processing is in the Border Function system, the implementation may be software based and processing resources are shared with routing or other high level functions. IPSec encryption is often performed by another device or is provided by dedicated hardware resources within the Border Function, because of this IPSec may scale better and be easier to implement.

Use of encryption will make troubleshooting more difficult by limiting the use of external network probe systems.

8.3 Authentication

- Definition

Authentication is identification of the connecting party to assure that party's identity; authentication is used to identify elements within Un-trusted Zone from the Trusted But Vulnerable Zone.

- Implementation

There are several mechanisms available for authenticating VoIP interconnections: the use of encryption/authentication protocols such as IPSec or TLS (see section 8.2), the use of information within signaling messages such as prefix attached to the dialed number or a password or the identification of the source IP address of the incoming SIP messages.

- Discussion

Authentication using IPSec and TLS provides strong authentication. IP addresses, prefixes and passwords do not provide a level of security when used independently as they provide only weak authentication; they can be used to enhance overall security with other mechanisms. However, the deployment of such schemes is common for VoIP interconnections.

Note: A further authentication scheme can be performed at the IP/TCP layer by means of MD5 authentication protocol between the e-BGP neighbors routers involved in the interconnection.

8.4 Access Control Lists

- Definition

Access Control Lists are filters applied to packets which allow only matching traffic to be forwarded. Filtering can use source and destination IP address and other TCP/IP parameters such as protocol or ports. ACLs can be employed at all zone boundaries in the trust model e.g. from the Un-trusted Zone to the Trusted But Vulnerable Zone and also within each zone.

- Implementation

ACLs are applied on ingress and egress to the network to prevent unwanted traffic being forwarded from either malicious sources or from improperly configured equipment. ACLs should be designed to pass only traffic from allowed services; all other traffic should be blocked. For example, ACLs should be used to block unwanted ICMP messages that are not necessary for network function such as ICMP redirect messages (type 5). A future version of this document will give more detailed information on the construction of an appropriate filtering policy.

- Discussion

ACLs are a common mechanism for network security. ACLs are used to defeat attacks that target already blocked services or easy to identify attacks e.g. an attack from a limited set of source IP addresses. ACLs are less effective against attacks that exceed the size of network links or Public Internet uplink capacity.

It is important when using ACLs to understand the implementation within the filtering device; implementations can be entirely in software or can have hardware processing to improve performance. Hardware processing is usually orders of magnitude faster than software implementations; this means that devices with hardware processing are more suitable as ACL filtering points. Software implementations can be overwhelmed by traffic volume and can become a target for attacks. Hardware implementations may have limits on ACL length or complexity and fallback to software processing when these limits are exceeded. Routers or firewalls will usually have hardware assistance, hosts and other devices, including some Border Function systems, will have software based implementations. It is important to ensure that the filtering performance available is sufficient to process traffic equal to the maximum packet per second rate at the minimum packet size for active network interfaces. Because of this it is recommended to use ACLs that have hardware implementations to prevent exhaustion of CPU resources.

8.5 Reverse Path Filters

- Definition

Reverse Path Filters are a type of dynamic ACL that filters incoming traffic to ensure the traffic received is limited to that received from IP addresses that are sent via that interface. This mechanism can be used at zone borders within the trust model to prevent attacks that involve address spoofing i.e. those that involve pretending to be an internal IP address or an IP address of a partner to exploit a security loophole.

- Implementation

Reverse path filters work by only allowing traffic through an interface if the source address of the traffic matches a routing table entry that directs traffic to that source address through the interface; it requires symmetric routing and therefore should not be used where asymmetric routing is required. It is often deployed on a firewall or router that is close to the end device where the IP flow is terminating, for example the Border Function system.

- Discussion

Reverse path filters are a type of ACL, please see section 8.4.

8.6 Traffic Policing

- Definition

Traffic policing controls the rate of incoming or outgoing packets/requests; it can be used for security reasons or to enforce a business agreement. Traffic policing would typically be employed in the Trusted But Vulnerable Zone to limit the traffic towards the Trusted zone where the CHF typically resides.

- Implementation

Traffic policing can be performed by routers, firewalls, DPI systems or Border Function equipment. Traffic that is within the configured rate is called ‘conforming’ and forwarded and traffic that is in excess of the rate is called ‘nonconforming’ and discarded; there may also be burst parameters allowing traffic that exceeds the conforming rate to be forwarded temporarily. Limits can apply at the packet level, controlling the number of packets allowed from a particular source, or at the application level, controlling the number of requests from a particular source. Some network elements, such as Border Function systems, may be application aware and able to send back protocol specific responses to nonconforming traffic to facilitate better interworking, such as SIP 503 messages.

- Discussion

Traffic policing can be used to protect the Border Function systems or downstream infrastructure from DoS attacks, from incorrectly configured partner equipment and from 'mass call' events when traffic levels are too high.

As with ACLs, implementation of traffic policing can be in software or hardware assisted; routers, firewalls, load balancing devices and DPI devices will have hardware assistance, Border Function systems and soft switch equipment will normally implement policing in software, though may have hardware implementations of packet rate limits. The implementation is important as the policing may become a target for attackers to cause disruption.

Another consideration is whether the application of the rate limit can be specified for individual traffic sources and groups of traffic sources. While a global limit may be useful for protection of the platform and downstream components it offers less flexibility during an incident.

8.7 Application Level Relaying

- Definition

Application Level Relaying is performed by terminating a particular application request session on one side of the relaying device and then relaying the request/session to another network element, this is performed at Layer 7 by the Application Level Relay which implements a Layer 4-7 state machine. In the case of SIP the call itself is logically terminated on one side of the Application Level Relay and relayed by reinitiating the call to the downstream element such as the CHF or softswitch. The Relay therefore decodes, interprets and re-encodes any SIP message. The Application Level Relay typically performs this function from the Un-trusted Zone to the Trusted Zone, the Relay itself being in the Trusted But Vulnerable Zone.

- Implementation

For SIP/SIP-I calls or sessions a Back-to-Back User Agent (B2BUA) is the logical function that provides Application Level Relaying. This is implemented by inserting the B2BUA into the communication path between the source and the destination device and communicating on behalf of the destination device with the source before re-originating the request to the destination device. The Border Functions system will normally provide a B2BUA [13]

- Discussion

Application Level Relaying is useful for preventing protocol vulnerabilities from reaching the CHF or downstream network and to allow signalling manipulation that may be required by the CHF or downstream network. It is essential part of security for VoIP interconnections.

8.8 Deep Packet Inspection

- Definition

DPI devices provide the ability to look into the payload that is carried by the packet and use the contents to perform filtering or rate control; this means that the device is able to look at the information carried in the application layers, even though the device may not be actively participating at the application layer. DPI devices are distinct from application level relaying as they do not contain application implementations but provide the ability to decode the application. DPI devices are useful to protect borders between zones in the trust model, most commonly from the Un-trusted Zone to Trusted But Vulnerable Zone.

- Implementation

DPI devices are used for the separation of traffic of malicious intent from legitimate traffic that should be processed by the network; this can be done in situations where simple ACL or traffic policing are not sufficient to perform the task due to forged IP addresses or TCP/UDP ports or header information that varies in a randomized manner. Some DPI devices have the ability to create new attack signatures based on baseline traffic analysis. Traffic is sampled during periods of normal network operation and a normal baseline profile is constructed for the network. The device can then monitor the network and shut off traffic sources that are outside the normal baseline or control the injection of traffic into the network.

- Discussion

DPI is useful for dealing with protocol vulnerabilities and exploit attacks which are identified by protocol state etiquette or specific byte or text string patterns within incoming traffic. Some DPI implementations may use only IP layer information for statistical analysis which is not sufficient alone to detect and mitigate layer 7 attacks. For example, a flood of invites with the same transaction ID can not be detected at layer 3. Please see Appendix B – Deep Packet Inspection (DPI) Layer 5-7 Countermeasures - for more information on DPI in the application layer.

8.9 Secure RTP (SRTP)

- Definition

The SRTP protocol encrypts RTP media packets and provides authentication and integrity for those packets; it is described in RFC 3711 [14]. It would be used to communicate with Un-trusted Zone elements to protect from Rogue Media and Session Hijacking type attacks.

- Implementation

SRTP can be implemented by either the Border Function or MG systems and requires agreement as to the encryption standard to be used. It also requires master keys to be exchanged between SRTP endpoints either manually or using the ZRTP [15] protocol.

- Discussion

SRTP requires extra resources to perform the encryption on the Border Function or MG system. This can lower the concurrent call performance and may require additional resources. Some Border Function and MG system vendors offer hardware assisted encryption for the SRTP to increase performance. SRTP is not commonly deployed in VoIP interconnections at this time.

8.10 DNS Security (DNSSEC)

- Definition

DNSSEC [16][17][18] provides an additional layer of security for DNS clients by digital signing DNS query responses so that the client implementation knows that the DNS response has been received from the expected source. In particular it provides protection against MITM attacks on DNS. DNSSEC does not provide encryption of DNS query requests or responses and does not provide authentication of the querying network element.

- Implementation

DNSSEC is implemented by the ENUM/DNS server digitally signing the query responses using several possible algorithms such as RSA/MD5 [19], the signature itself is then contained in new resource record type in the DNS query response.

- Discussion

DNSSEC requires extra resources to digitally sign the query responses on the ENUM server; this may lower performance and require additional resources. In addition the benefits of DNSSEC are less critical in a typical ENUM environment where there are often no caching or recursive lookup mechanisms being used.

8.11 Media Filtering

- Definition

Media filtering, also termed 'Pinholing', is a dynamic ACL technique for filtering RTP protocol packets. It can be employed at zone boundaries in the trust model e.g. from the Un-trusted Zone to the Trusted But Vulnerable Zone.

- Implementation

Normally deployed in addition to static ACLs, media filtering is accomplished by looking at the signalling messages during call setup and then allowing RTP traffic associated with the call through the ACL. This is done by detecting the RTP source and destination IP addresses/ports. Once the call has finished the filter entry is removed preventing additional traffic from entering the network. Media Filtering can be applied by a firewall or router device or can be performed by Border Function devices directly.

- Discussion

This technique is useful for protecting media from rogue media attacks as well as preventing DoS attacks that may exploit RTP UDP packets.

8.12 Firewalls

- Definition

Firewalls are general security devices that have a variety of features: topology hiding, encryption, ACLs, DPI, application level relaying etc. Firewalls can be employed at all zone boundaries in the trust model e.g. from the Un-trusted Zone to the Trusted But Vulnerable Zone.

- Implementation

There is large diversity in the way firewalls can be implemented and used. The simplest usage is to provide basic packet filtering at Layers 3 through 5, however implementations may also perform application level relaying and packet inspection. In VoIP networks these functions may often be provided by the Border Functions system rather than a dedicated firewall device.

- Discussion

Firewalls are devices with wide applicability, however there are often issues with the deployment of application level relaying due to firewalls requiring to be capable of handling the full protocol specification required for the service. While this is often the case for enterprise networks, service providers and carriers have specialist requirements for VoIP interconnection that firewalls may not provide, such as support for specific SIP headers or the SIP-I protocol. Therefore in VoIP interconnections the application level relaying function is normally provided by the Border Function system B2BUA as discussed in section 8.7.

8.13 Intrusion Detection Systems

- Definition

IDS are devices or software applications that aim to detect unauthorized access to network resources primarily for the purpose of stopping network intrusion attacks. IDS can be employed at the major zone boundaries in the trust model e.g. from the Un-trusted Zone to the Trusted But Vulnerable Zone.

- Implementation

There are two common types of IDS: host based systems that analyze log files and system files and network based systems that monitor network traffic by packet capture. Both systems may be combined to provide a better picture of network security incidents. When an attack is detected the IDS can be configured to inform network operators or can automatically respond by creating dynamic ACL entries or configuring other devices to respond to the event.

- Discussion

IDS can also be used to detect other forms of attack as well as intrusions. IDS capabilities are also a feature of DPI equipment and can be found in products together.

8.14 Device Hardening

- Definition

Device hardening is set of techniques to ensure elements are less vulnerable to security exploits which may result in a network intrusion or make DoS attacks easier to accomplish; these techniques seek reduce the attack footprint of the systems. Device hardening is applicable to all network elements in the trust model.

- Implementation

The are several different techniques, for example one technique in device hardening is to turn off unused network services to prevent them being open to access by unauthorized parties; these services might be unused protocol interfaces e.g. H323 on a Border Function system that is only configured for SIP or management interfaces, such as web management. Devices can often arrive preconfigured for access by default to such interfaces, requiring explicit configuration to disable them. Another hardening technique seeks to limit the tasks running on system as a highly privileged user e.g. on UNIX systems, limiting the processes required to provide accessible services to a user other than the 'root' user wherever possible. Hardening is usually applied to general computing resources involved in service delivery, but the techniques can also be applied to specialist elements such Border Function systems or routers.

- Discussion

These techniques are primarily useful against network intrusion but can also help prevent DoS attacks.

8.15 Logging and auditing

- Definition

Logging and the auditing of the logs is a basic security practice. Logging and auditing processes are applicable to all network elements in the trust model.

- Implementation

The UNIX syslog protocol is the most commonly used logging mechanism available, though there are also proprietary logs generated by some products. Syslog or other data produced should be stored in a central logging system to allow searching and auditing. It is important to make sure that all devices in the network have synchronized clocks to ensure that log information can be correlated. Auditing of log information can be performed using the central logging system and there are many log auditing products available, these can be tied to monitoring tools to alert operators of potential problems and incidents.

Generation of useful network log information and diagnostics may also be performed by implementing packet capture and monitoring devices to the network using switch mirror ports or dedicated network taps.

- Discussion

It is important to be able to log network events and traffic flows to build a complete picture of the current operating state of the network. This becomes essential important during security incidents. It is also important to audit log information to identify incidents as early as possible to allow corrective action.

8.16 Security Information and Code Updates

- Definition

Using security alert information and applying code updates are basic security practices. Security information and code updating processes are applicable to all network elements in the trust model.

- Implementation

There are many sources of security information provided by equipment vendors and external organizations such as the CERT organizations or NIST CSRC. Organizations can use the information to plan immediate responses and plan software updates to correct security problems. It is common practice to monitor information sources and then mitigate vulnerabilities by using ACLs or other tools; in the longer term software updates are performed.

- Discussion

This approach works well to limit the impact of security problems, however the disadvantage is the amount of time it takes to receive information and then act on it. In addition some types of attack are not related to software vulnerabilities e.g. DoS attacks designed to overwhelm network links or router equipment upstream of the target.

8.17 Threat Mitigation by Mechanism Matrix

The matrix below maps the available mitigation mechanisms to the security threats discussed in Section 6. The matrix is not intended to convey the appropriateness or effectiveness of the mitigation mechanism and should not be used for design purposes. Each mechanism's applicability to a given threat is broad and non specific, a future version of this document will classify and provide more information on effectiveness against particular threats.

Mechanism/Threat Mitigated	**DoS/DDoS Attack**	**Protocol Vulnerabi-lities**	**Address/ Identity Spoofing**	**Theft of Service**	**Rogue Media**	**Session Hijacking**	**Network Intrusion**	**Internal Network Security**
Topology Hiding	X		X				X	X
Encryption			X	X	X	X	X	X
Authentication			X	X	X	X	X	X
Access Control Lists	X	X	X	X	X		X	X
Reverse Path Filters	X		X			X	X	
Traffic Policing	X			X				X
Application Level Relaying	X	X						
Deep Packet Inspection	X	X	X	X	X	X	X	X
SRTP			X		X			
DNSSEC			X	X		X		
Media Filtering			X		X			
Firewalls	X	X	X	X	X	X	X	X
Intrusion Detection Systems	X		X	X		X	X	X
Device Hardening		X		X		X	X	X
Logging and Auditing	X	X	X	X	X	X	X	X
Security Information & Code Updates	X	X	X	X		X	X	X

Matrix 1: Threat Mitigation by Mechanism Matrix

9 Implementation Recommendations

This section defines the security recommendations for parties involved in international VoIP interconnections. It defines general recommendations for security as well as policy that should be used internally and externally. The matrixes provide implementation recommendations on specific mechanisms that should be used to protect the service interfaces.

9.1 Transport Configurations

Transport network configurations may be either:

- Private-oriented interconnections using direct private links or VPN service from a transport network.
- Public-oriented interconnections using the IPv4 or IPv6 Public Internet.

Please see the i3 Forum Technical Interconnection Model for International Voice Services [1] for further information. The recommendations are split into sections for private or public interconnections separately.

However, by using private interconnections between trusted partner networks, security is greatly enhanced for all the services and the i3 Forum recommends the use of private interconnection wherever possible. The use of private interconnections between networks does not eliminate all security concerns as is shown in the trust model defined in section 5 as the carrier has limited ability to control partner networks. Therefore carriers may find it desirable to implement the security mechanisms available when working with private interconnections as well as when using the Public Internet for interconnection.

9.2 Use of Border Functions

The i3 Forum recommends the use of dedicated Border Function systems to provide security for VoIP interconnections [1]. Network elements that can perform the Border Function role are also called ‘Session Border Controller’ (SBC) systems [13]. The Border Function systems typically provide multiple security mechanisms including application level relaying of traffic, which allows verification of protocol contents. Border Function systems are not listed in the matrixes below in section 9.5 & 9.6, the matrix 2 – External Service Interfaces - and matrix 3 – Routing & Addressing Provisioning containing the logical component mechanisms provided by Border Function systems.

9.3 General Security Recommendations

Carriers should take seriously the requirement to have an in-depth approach to security for VoIP interconnections and help other carriers and service provider organizations to establish a comprehensive approach to security. The approach should be based on the understanding of the trust model discussed in section 5 of this document and establishment of appropriate security policies and procedures within the organization. Use should be made of the matrixes presented below to enhance security of the carrier and service provider networks.

9.4 Internal Policy Recommendations

Specification of a complete internal security policy is beyond the scope of this document but the following are recommended elements of for an internal security policy and organization that are relevant for VoIP interconnections:

9.4.1 Operations/Security Partitioning

Operations and engineering staff involved in provisioning and operating the network should not be allowed access to the security logging and auditing systems used by the network. This is to prevent cases where internal employees can alter records to disguise their own actions if they intend to make unauthorized changes to network systems.

9.4.2 Fraud Management

Carriers should have fraud management processes setup to deal with the potential of fraud by external or internal parties. This should include mechanisms to identify fraud occurring on the network, by the use of traffic management and monitoring tools, as well as the process for disconnecting interconnections that may involve the origination of fraudulent traffic. Further information regarding the processes and tools available to combat fraud is being produced by the i3 Forum Fraud Workstream.

9.4.3 Vendor/3rd Party Support Access

Vendor or 3rd party support access to the network should be restricted to the Trusted But Vulnerable Zone with only limited access into Trusted Zone networks and systems to prevent potential security incidents from vendor or 3rd party networks.

9.5 Interconnection Security Policy Recommendations

When establishing interconnection agreements with other carrier and service provider organizations security should be emphasized and an appropriate document created. This should be considered for inclusion in the bilateral agreement between the parties when implementing a new interconnection, including when migrating to a VoIP interconnection from TDM. Carriers may also find it helpful to refer to the GSMA document IR.77 [5] when interconnecting with mobile operators.

The policy should include sections on the following areas:

9.5.1 Minimum Required Security

This section defines which mechanisms and configuration should be deployed by the carrier and the interconnecting party so that each party has an understanding of the security level that will be deployed. This would consist of a list of mechanism that are listed in section 9.6.1 and 9.6.2 from either the Basic or Recommended section and an architectural diagram or description which specifies the configuration in use for the interconnection i.e. Private-oriented or Public-oriented as discussed in the section 6 of the i3F Technical Interconnect Model [1].

9.5.2 Acceptable Use Policy

This section defines what constitutes the acceptable use policy of the interconnection between the two parties:

- Allowed types of traffic on the interconnection.
- Acceptable rate of signaling or volume of sessions allowed.
- Prohibited behavior:
    - Attempts to scan, probe or look for vulnerabilities for the purposes of unauthorized access.
    - Attempts to overload the system with the intent of causing outages, service degradation or causing complaints by other parties
    - Forging of packets.
    - Attempts to circumvent billing mechanisms.
- Prohibition of illegal or unethical use of the interconnection or data exchange on the interconnection.
- Attempt to defraud any party including downstream parties of the carrier.
- Interconnection suspension terms in the event of a security incident.

Items within this policy may be covered by other documents between operators, such as a standalone AUP, and may be unnecessary in every case.

9.5.3 Security & Fraud Procedures

This section should identify the procedures to use if a security or fraud incident is in progress or has occurred. It should cover the appropriate parties to contact on the carrier side and on the interconnecting party side and the escalation procedures that will be used to respond to the incident, as well as each party’s responsibilities. It should also include the procedures for suspension or termination of the interconnection in the event of a serious security or fraud incident or recurrence.

9.6 Recommendation Matrixes

There are three levels specified in the following sections:

- Basic – the basic security mechanisms that reflect the minimum generally accepted industry practices for securing these services
- Recommended – in addition to basic, mechanisms consistent with the implementation documents of the i3 Forum
- Optional – in addition to recommended, other mechanisms that can be used to further enhance security for the specified service

9.6.1 Recommendations for External Service Interfaces

This matrix specifies which mechanisms should be deployed for external service interfaces related for VoIP interconnections, for the three security levels: basic, recommended and optional.

Configuration	**Basic**	**i3F Recommended** *(additional to Basic)*	**i3F Optional** *(additional to Recommended)*
		SIP/SIP-I interface	
Private Interconnection	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Authentication** **Application Level Relaying** **Topology Hiding** **Traffic policing**	i3F Recommended + Encryption Deep Packet Inspection Intrusion Detection Systems
Public Interconnection	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Authentication** **Application Level Relaying** **Encryption** **Topology Hiding** **Traffic policing**	i3F Recommended + Deep Packet Inspection Intrusion Detection Systems
		SIGTRAN Interface	
Private Interconnection	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Authentication** **Topology Hiding** **Traffic policing**	i3F Recommended + Encryption Deep Packet Inspection Intrusion Detection Systems
Public Interconnection	Access Control List Reverse Path Filters Authentication Device Hardening Logging and Auditing Security Information and Code Updates Traffic policing	**Basic +** **Encryption** **Topology Hiding**	i3F Recommended + Deep Packet Inspection Intrusion Detection Systems

RTP Interface			
Private Interconnection	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Authentication** **Media Filtering** **Topology Hiding**	i3F Recommended + Encryption SRTP Traffic policing Deep Packet Inspection Intrusion Detection Systems
Public Interconnection	Access Control List Reverse Path Filters Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Authentication** **Media Filtering** **Topology Hiding**	i3F Recommended + Encryption SRTP Traffic policing Deep Packet Inspection Intrusion Detection Systems
Routing & Addressing Query Interface			
Private Interconnection	Access Control List Reverse Path Filters Authentication Device Hardening Logging and Auditing Security Information and Code Updates	**Same as Basic**	i3F Recommended + Encryption DNSSEC Traffic policing Deep Packet Inspection Intrusion Detection Systems
Public Interconnection	Access Control List Reverse Path Filters Authentication Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Encryption** **Traffic policing**	i3F Recommended + DNSSEC Deep Packet Inspection Intrusion Detection Systems

Matrix 2: Recommendations for External Service Interfaces

9.6.2 Recommendations for Routing & Addressing Provisioning and Other Interfaces

This matrix specifies what type of mechanisms should be deployed for the external database provisioning interface and other interfaces, for the three security levels: basic, recommended and optional.

Configuration	**Basic**	**i3F Recommends** *(additional to Basic)*	**i3F Optional** *(additional to Recommended)*
Routing & Addressing Database Provisioning	Access Control List Reverse Path Filters Authentication Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Encryption** **Firewalls**	i3F Recommends + Deep Packet Inspection Intrusion Detection Systems
Other	Access Control List Reverse Path Filters Authentication Device Hardening Logging and Auditing Security Information and Code Updates	**Basic +** **Encryption** **Firewalls**	i3F Recommended + Deep Packet Inspection Intrusion Detection Systems

Matrix 3: Recommendations for Routing & Addressing Provisioning and Other Interfaces

10 Security Best Practices & Processes

There are many sources of information regarding best practices for use in general network and computer security. This section lists relevant literature that can be further consulted for more information on specifically VoIP security; this includes information on security in VoIP access networks and enterprise networks as well as interconnection security between service providers and carriers.

10.1 Applicable Standards and Literature

- GSMA Document IR.77 Inter-Operator IP Backbone Security Requirements For Service Providers and Inter-operator IP backbone Providers [5]
- ITU-T Recommendation Y.2704 Security mechanisms and procedures for NGN [3]
- ITU-T Recommendation Y.2701 Security requirements for NGN phase 1 [2]
- ATIS Document ATIS-1000026.2008 Session/Border Control Function Definition and Requirements [7]
- The i3 Forum Documentation e.g.
    - i3 Forum Technical Interconnection Model for International Voice Services.
    - i3 Forum Migration Interconnection Form
    - i3 Forum Working Stream Fraud documents

  Go to www.i3forum.org for further documents

Annex A – Example of Security Code of Interconnection

This Code describes the network security requirements to be satisfied by both Parties for a Service Agreement, including the interconnection specification for the offered Services between both Parties. The Parties should describe a mutually agreed security policy, the details of which should be specified in a separate i3 Forum Migration Interconnection Form which describes the technical details for the security of the interconnection.

General Security Requirements

- Interconnection model: the Parties will be interconnected as specified in sections 5, 6 & 8 of the i3 Forum Technical Interconnection Model for International Voice Services.
- Security requirements: the details of the security requirements should be as listed in the attached i3 Forum Migration Interconnection Form.
- Protocols and codec: the requested mandatory and optional codes of this interconnection agreement are specified in the i3 Forum Migration Interconnection Form.
- Fraud: Both Parties have a fraud management process in place and appropriate fraud contacts listed in the i3 Forum Migration Interconnection Form.

Requirement Parameters

- Each Party should have defined security policies that cover the following items:
  - Statement of compliance.
  - Internal and external security policies.
  - Confidentiality guideline.
  - Information management structure.
  - Data integrity.
  - Audited network security organisation.
  - Fraud management and procedures.
  - Security requirements for system vendors.
  - Security requirements for 3rd party support.

- Each Party should have network security documentation that cover the following items:
  - IT system
  - Web applications & services (if required)
  - Network routers and switches
  - Databases access
  - Provisioning/CRM access

- Each Party should only enable required services on network equipment.

- Each Party should make all reasonable effort that:
  - IP Addresses used for the interconnection are confidential
  - Only specified IP Addresses are used
  - Addition or deletion of IP Addresses used is notified by providing adequate written notice

- Security Auditing is in place to prevent against fraud such as address spoofing; as per the requirements for the interconnection specified in the i3 Forum Migration Interconnection Form.

- Each Party should ensure that authentication and access control lists for the network are defined as specified in the i3 Forum Whitepaper Security for IP Interconnection.

- The i3 Forum Migration Interconnection Form includes additional items, such as encryption, if required.

Appendix A – Internal Security Examples

This Appendix complements section 6.8, with some more examples.

App-A1 Example: Allowing an anonymous source

Each time a new partner interconnection is configured in a network, the remote IP addresses of the partner needs to be configured in the border function and security mechanisms. The IP address of the border function is also communicated to the partner as the address they need to use to send traffic to.

Because of this, the border function system is normally configured to only accept traffic from a set of predefined IP addresses, belonging to known partner equipment. However, if this check is not enabled correctly, the border function system will allow any traffic to enter the network. This can be seen in Figure 6 below.

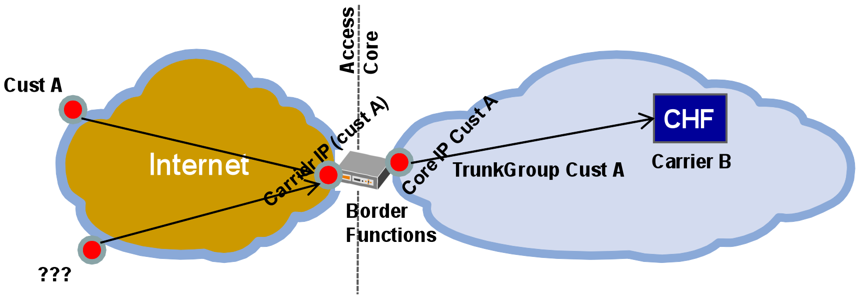

Figure 6: Allow anonymous source address

The consequence of the incorrect configuration is that anyone finding this weak point in the carrier's network will be able to place call without being identified and billed correctly. Such vulnerabilities in a network can be found in a few hours or days by automatically scanning networks. An attacker can use this to launch DoS attacks targeted at the relationship between customer A and the carrier, launch general DoS attacks on the carrier or perform theft of service.

A counter measure that can be deployed is to perform an automatic configuration audit of the Border Function system.

App-A2 Example: Border Function Tromboning

In this scenario two interconnects are configured: one to supplier A and another to Customer B, with both A and Bs addresses configured in the border functions. However, all or a portion of the traffic from Customer B traffic, such as traffic for particular destinations or time periods, instead of being sent to the carrier for termination is sent to Supplier A. Figure 7 shows this situation.

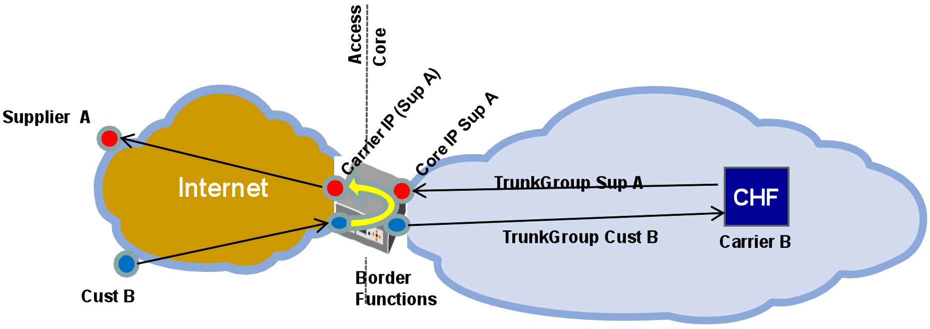

Figure 7: Border function tromboning

In this case Customer B will not be billed by the carrier or supplier A, but Supplier A will bill the carrier for customer B's traffic, Customer B is defrauding Supplier A and the carrier.
This scenario takes advantage of the existence of routing functions that are available in some Border Function implementations. The Border Function system may act as a standalone IP to IP switch, with its own local routing table, depending on configuration it may relatively easy to "mix" traffic towards the Supplier A and make traffic from Customer B appear as originating directly from the carrier.

App-A3 Example: Removal of Traffic Constraints

This scenario occurs when a customer is only allowed to use a limited number of concurrent sessions, for example, when limiting traffic due to credit risk. This limit can be configured in the Border Function system or on another device such as a soft switch further inside the network.

Removal of a configured limit can very quickly open a large amount of capacity to a fraudulent customer, which is only limited by the Border Function system, and downstream network capacity and licensing. The extra capacity only has to be active for a short period of time to generate significant theft of service and cause significant financial issues which the carrier cannot easily resolve.

Appendix B – Deep Packet Inspection (DPI) Layer 5 – 7 Countermeasures

Application Layer 5 – 7 deep packet inspection (DPI) methods that can help protecting from the impact of the manipulation of SIP protocol and RTP protocol by the use of: Filtering of Signalling, Origin Authentication, Media Pin-Holing, and a method to ensure Protocol Robustness, are described in this Appendix B and complete section 8.8 – Deep Packet Inspection.

App-B1 Filtering of Signalling (aka Method-Proofing)

- Definition:

Protects against the manipulation of SIP protocol via signalling flooding by detecting excess invites, responses and violation of "state machine" in signalling.

- Implementation:

A possible method is to check the source IP Address and Transaction ID using Branch Parameter and Cseq for comparison. [5] The ability to detect botnet organized attacks (aka Distributed DoS attacks) where hundreds-of-thousands and even millions of origins send only one packet requires DPI to detect a single malicious packet.

- Discussion:

The device and/or its management platform determine a value for a "reasonable" maximum number of repeated SIP methods/per transaction ID that may occur in a particular service environment. This value would be configured as the settable threshold for the device in that environment. Some solutions only aggregate this information on the interface or sub-interface level, and can't deal with aggregation at the "per end-point" level. If a "state-aware" Border Function is being used, the incremental effort to perform "per-end point" rate limiting should be considered.

App-B2 Spoof-Proofing (Origin Authentication)

- Definition:

It helps to avoid unnecessary performance draining calculations required by a Border Function for digest authentication by identifying and terminating second-attempts. Attackers with no intension of valid service overwhelm the Border Function by asking it to calculate hash, a very long procedure, in response to a provided 407 nonce.

- Implementation:

Use of a table algorithm employing "bit pattern search and matching" can accomplish "look ups" in a single CPU cycle to identify and terminate second attempts. Coupled with a hardware solution to successfully accomplish the tasks by "off-loading" the Border Function from this performance draining function is recommended [6].

- Discussion:

The capability to thwart "Spoofing" at SIP level (when using Digest Authentication) without degradation in performance is necessary to prevent the flood of Spoofed messages which can be accomplished by offloading the Digest Authentication mechanism from Border Function by using a hardware solution.

App-B3 Media Pin Holing

- Definition:

Helps to protect against SIP DoS Attacks by opening and closing Media Ports based upon SIP Signalling, blocking all other media. The Media Port is opened dynamically based upon Layer 7 application layer gateway.

- Implementation:

Existing methodologies introduce delay since info taken from SDP needs to be compared with tables using an approach that is very time consuming. Pinholes are opened and closed and incomplete table scans (due to time consuming processes) can leave pinholes open indefinitely during high processing events where some instructions are dropped. Use of a table algorithm employing "bit pattern search and matching" can accomplish "look ups" in a single CPU cycle [6]. This method is scalable, filtering at wireline speed, avoiding the creation of a bottleneck.

- Discussion:

“Carrier class” speed and scalability may be characterized by the capability for Media Pinholes to be opened within less than 60 ms and close within no more than 300 ms. Metrics and test results for opening and closing of pin holes should be shared securely among partner carriers to ensure they are closed within specified tolerances, and to make sure no pin holes remain open unknown to the carrier, thus creating a possible security problem.

App-B4 Protocol Fuzz-Proofing (Protocol Robustness)

- Definition:

Measure a device’s susceptibility to Fuzzing by testing a device’s software reaction to hundreds of thousands of “fuzzed” versions of the SIP protocol to determine a device’s robustness, preventing the impact upon the system by a single malformed packet.

- Implementation:

Use a commercially available Fuzz Generator to pre-test equipment prior to installation into a production environment. Various Fuzz Generator vendor solutions are available for carrier consideration. (For example, see Codenomicon at http://www.codenomicon.com/ or Mu Dynamics at http://www.mudynamics.com/)

- Discussion:

This approach is necessary given it is technologically impractical to sniff all possible header variations known to be malformed packets in live “real time” traffic.