

SIP Security and the IMS Core



Simply Better Connected

SIP SECURITY AND THE IMS CORE

Much has been written about the security of SIP-based networks and security of Voice over IP in general, but ultimately good security is a complete architecture, not a single product or protocol. The advent of Fixed/Mobile Convergence and IMS has created some widely accepted standards and has equally highlighted architectural differences in the converging networks. Whilst the overall objective of providing a flexible, secure network and secure services is common, the implementation details differ from network to network.

Even within the standards themselves there is sometimes an assumption of trust which may not in reality exist. For example, the IMS definition within TISpan assumes that the signalling elements are able to handle excessive signalling rates and badly formed signalling messages. In reality these elements are designed to process sessions, handling attacks at the same time may not be the best use of the equipment. In a data-centric network we would expect to see servers ringed by Firewalls and Intrusion Detection and Prevention systems, so why would we build a media-centric network any other way?

Fixed/Mobile Differences

The networks that support mobile services have developed their own security and authentication mechanisms that reside primarily in the radio access part of the network. This means that when 3GPP developed their IMS specification there was no need to be overly concerned with those issues. The IMS can assume that the subscriber that is registering has already been authenticated and that the only thing to deal with now is the policies that apply to the caller. In the case of a fixed line service there is no guarantee that the user will be authenticated against a USIM (Universal Subscriber Information Module), thus authentication must rely on other, potentially less secure techniques.

This ability to connect almost any hardware or software device opens the door to other potential problems in the fixed line network – that of device malfunction and malicious attack. The mobile radio access network is a far more controlled environment, with each device having a security association

with the network, meaning that any abuse can be tracked back to a particular device. Another consideration is that there is currently a marked difference in the bandwidth available in fixed and mobile networks, thus the fixed line network offers a potentially larger pipe to deliver disruptive traffic. Fixed line networks will support a large population of PC based soft-clients, these require minimal testing and therefore the potential for the presence of badly behaved device is much greater, it also means that a familiar environment is available for creating malicious software.

ETSI's TISpan architecture takes the 3GPP IMS definition and expands it to include additional elements that help to address some of these concerns. The most noticeable difference is that the 3GPP definition deals only with the signalling path whilst the TISpan definition includes elements that manage the media path, the BGFs – Border Gateway Functions. There is also a formalised Border Control Function between interconnected networks – the IBCF.

The 3GPP IMS security architecture is based around IPsec, which works well in the 3G environment which does not have NAT devices. Most NAT devices translate port numbers as well as IP addresses, which due to the way IPsec encodes the packets means that NAT devices will prevent end-to-end use of IPsec.

However, in TISpan with client devices typically being connected through broadband access networks NAT devices are virtually guaranteed. Thus, TISpan encryption and authentication must take another route. RFC3261 specifies TLS as the secure transport mechanism for use with SIP, and this was considered by TISpan, however, the selected encryption method is UDP encapsulation of IPsec. This eliminates the problems encountered when using IPsec across NAT devices. IPsec, NAT traversal and TISpan's selection of UDP encapsulated IPsec are examined in the White Paper "[IPsec in VoIP Networks](#)".

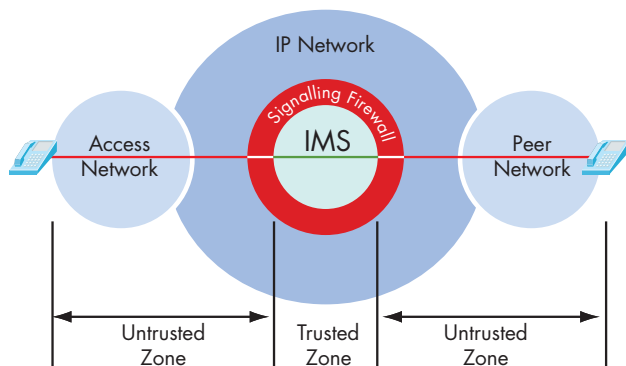
IMS as the Heart of the Network

The role of an IMS core is to enable service providers to roll out new services rapidly and deliver them to any device over any network. It is the glue that sits between the service layer and the network layer. Whilst these elements can be expected

to provide some level of resilience to attacks, pragmatic service providers are looking to create a protected zone in which these highly valuable assets can be located.

So we are in effect talking about creating a DMZ for the signalling through the use of 'signalling firewalls'. The job of the signalling firewall is to protect the core elements from accidental overload, malicious attack, malformed signalling messages and irrelevant protocols.

Protect the core with signalling firewalls



Providing protection for the core requires more than a conventional firewall, it requires a firewall that can understand SIP signalling. This requires a resilient hardware based solution capable of rejecting any unwanted traffic whilst admitting legitimate traffic at a rate which can be supported by the core elements. Not a trivial task - lets look at the requirements one by one.

Requirement 1: Must stand up under attack

A basic requirement of any signalling firewall is that it must remain operational under all attack conditions. Before we get carried away with all of the exotic and innovative application layer attacks, the basics must be in place. The TCP SYN flood, for example, is one of the oldest attacks around and probably one of the most common exploits used to cause resource starvation in vulnerable targets. The IMS core may not need to even respond to any TCP traffic if the SIP signalling is carrier using UDP, thus TCP traffic can be rejected at the perimeter of the IMS. Similarly logic exploits like the Ping of death, should simply be blocked by the firewall at the IMS perimeter. A minimum requirement for the signalling firewall is that it should stand up to vulnerability tests such as ISIC - IP Stack Integrity Checker and Nessus.

SIP signalling traffic must also be viewed with considerable suspicion, malformed SIP messages should be discarded and not passed through to the IMS core elements. Resistance to this type of attack can be determined by testing against suites such as the IETF SIP Torture test developed through the SIPIT Events or the PROTOS Test-Suite, developed by the University of Oulu.

Requirement 2: Must prevent propagation of attacks

This is the logical extension of the first requirement. The signalling firewall must identify and discard malicious traffic in order to protect the core. Many protocols can simply be discarded, as described in Requirement 1 above, as they have no relevance to the SIP proxies. Thus the IMS elements are effectively protected from both transport and application layer attacks.

Requirement 3: Must preserve an operational service through pacing

Now that the basics are in place we must turn our attention to the applications themselves. The rate of SIP signalling can be the cause of problems for the Softswitch and not just through malicious intent, for example, following the hurricanes in Florida when the power was restored, this caused all the IP phones to register at the same time. This resulted in the service failing due to the rate of registrations. In these situations the core elements must be protected by pacing both registrations and call attempts. The signalling firewall should deliver the registrations and call invitations to the Softswitch at a rate that it can sustain.

Requirement 4: Must preserve network anonymity through topology hiding

Topology hiding features prominently in most service providers' requirements. As the SIP signalling passes through various servers on route to its destination, the SIP messages acquire information about where the message came from and what devices it passed through. Since global networks are made up of a mesh of service provider networks this information gets passed from network to network. It is therefore important to strip all this information from the signalling prior to it being passed from one network to another. This prevents internal network addresses and client address details from being propagated. This benefits the service provider by effectively shielding both network and subscriber from prying eyes.

Requirement 5: Must preserve service quality and protect revenue through media policing

This requirement is present to counter some of the innovative ploys to steal services. When SIP establishes a call it uses a server to locate and communicate with the destination, once the addresses of the source and destination have been exchanged there is no reason why the two parties cannot communicate directly – without the intervention of the server. Thus, a party can request a voice call which, once established can be renegotiated as a video call without the knowledge of the SIP servers from which the billing may be derived. The service provider is unaware of the additional bandwidth being used. This results in loss of revenue and potential degradation of service quality for other users.

To prevent this service theft it is necessary to link the media path with the signalling path. This is carried out by session border controllers, or in the case of a TISpan IMS, by a combination of the P-CSCF and A-BGF managing the signalling and media respectively. The signalling and media elements exchange information to ensure that the media remains within the requested limits, any deviation from the requested bandwidth can be blocked.

A key benefit of this process is to preserve the Quality of Service of calls, particularly within the access networks, by preventing over-booking of the network resources.

The Survivable Core

With all of the above requirements satisfied we have helped to create a survivable core. Through a combination of firewalling, signal pacing and traffic management, the valuable assets that make up the IMS core can get on with doing their job: providing any service to any device over any network.

Is the signalling firewall a logical component or a physical device? The answer is actually both. There are several functions within the 3GPP and TISpan IMS definitions that can be considered to be border devices. The P-CSCF is the first point of contact for registration and routing of new calls and is therefore a suitable device in which to implement the signalling firewall. The I-CSCF provides topology hiding for the interconnect point. Within TISpan, the BCF and BGF functions define signalling and media borders. All these functions may be extended to include the requirements defined above as part of a fully integrated solution. Equally, it is

possible to treat the whole IMS as a target and implement the signalling and media protection externally.

What next? SPIT – Detection and Deflection

SPAM over Internet Telephony, or SPIT as it so colourfully known, is being touted as the next e-plague to descend upon us. This is the voice equivalent of email SPAM, i.e. machine driven mass dialling to subscribers to deliver junk voice mail. So how can we deal with this? The answer may lie in a two layered defence of detection and deflection. Many of the best SPAM filters around today are in fact great learning machines, they constantly learn what is SPAM and what is not, they build black lists of known sources and can achieve high rates of successful blocking. However, SPAM is non-real-time, in order to apply this technology to SPIT the detection engine must employ pattern recognition on calls to determine a potential source, this can be carried out non-intrusively in near-real-time, the results written to a policy database which is accessed by the signalling firewall which deflects or blocks the signalling and prevents the call from being established.

Conclusion

IMS offers the potential to deliver a great range of innovative services to a range of different networks. In doing so it offers an attractive target for disruption. The IMS core must be protected through the use of an effective security architecture either intrinsically as part of the perimeter of the IMS e.g. a hardened P-CSCF acting as a signalling firewall, or extrinsically by using signalling firewalls to create a DMZ for the core elements.

Newport Networks 1460 provides the carrier class hardware platform required for these duties, either as a P-CSCF itself, or as a signalling firewall protecting a third party P-CSCF. The 1460 can also offer separated signalling and media elements capable of offering full topology hiding and media policing.

Guaranteeing continuity of service is an imperative for service providers deploying IMS cores. The survivable core also forms the cornerstone of delivering reliable Emergency Call Handling and key worker prioritisation – this is discussed in more detail in Newport Networks Emergency Call Handling White Paper. ■



Glossary

A-BGF	Access Border Gateway Function
BCF	Border Control Function
BGF	Border Gateway Function
I-BCF	Interconnect Border Control Function
I-BGF	Interconnect Border Gateway Function
I-CSCF	Interrogating-Call Session Control Function
IMS	IP Multimedia Subsystem
IPsec	IP Security Protocol
NAPT	Network Port and Address Translation
NAT	Network Address Translation
P-CSCF	Proxy-Call Session Control Function
SIP	Session Initiation Protocol
SPIT	SPAM over Internet Telephony
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
UDP	User Datagram Protocol
USIM	Universal Subscriber Information Module

Other White Papers

You may find the following White Papers of interest:

- IPsec in VoIP Networks
- SIP, Security and Session Controllers
- Lawful Interception Overview

These and other papers can be found at:

<http://www.newport-networks.com/whitepapers>



The Newport Networks' logo is a registered trademark of Newport Networks Ltd. MediaProxy™ and SignallingProxy™ are trademarks of Newport Networks Ltd. ©2006 Newport Networks Limited. All rights reserved. Whilst every effort has been made to ensure that the information included in this publication is accurate at the time of going to press, Newport Networks Ltd assumes no responsibility for the accuracy of the information. Newport Networks Ltd reserves the right to change their specifications at any time without prior notice. Some features described in this document may be planned for future releases and may not be available in the current product. Newport Networks Ltd reserves the right to modify its product development schedule without notice and does not guarantee that any feature or product mentioned in this document will be produced or produced in the form described.

91-0088-01-0001-A