SPEERMINT Working Group	S. Niccolini	
Internet-Draft	NEC	
Intended status: Informational	E. Chen	
Expires: May 4, 2009	NTT	
	J. Seedorf	
	NEC	
	H. Scholz	
	freenet	
	October 31, 2008	

TOC

SPEERMINT Security Threats and Suggested Countermeasures
draft-niccolini-speermint-voipthreats-05

Status of this Memo

Abstract

This memo presents the different security threats related to SPEERMINT classifying them into threats to the Location Function, to the Signaling Function and to the Media Function. The different instances of the threats are briefly introduced inside the classification. Finally the existing security solutions in SIP and RTP/RTCP are presented to describe the countermeasures currently available for such threats. The objective of this document is to identify and enumerate the SPEERMINT-specific threat vectors in order to specify security-related requirements. Once the requirements are identified, methods and solutions how to achieve such requirements can be selected.

Table of Contents

---

1. Introduction

TOC

With VoIP, the need for security is compounded because there is the need to protect both the control plane and the data plane. In a legacy telephone system, security is a more valid assumption. Intercepting conversations requires either physical access to telephone lines or to

compromise the Public Switched Telephone Network (PSTN) nodes or the office Private Branch eXchanges (PBXs). Only particularly security-sensitive organizations bother to encrypt voice traffic over traditional telephone lines. In contrast, the risk of sending unencrypted data across the Internet is more significant (e.g. DTMF tones corresponding to the credit card number). An additional security threat to Internet Telephony comes from the fact that the signaling devices may be addressed directly by attackers as they use the same underlying networking technology as the multimedia data; traditional telephone systems have the signaling network separated from the data network. This is an increased security threat since a hacker could attack the signaling network and its servers with increased damage potential (call hijacking, call drop, DoS attacks, etc.). Therefore there is the need of investigating the different security threats, to extract security-related requirements and to highlight the solutions how to protect from such threats.

---

2. Security Threats relevant to SPEERMINT

TOC

This section enumerates potential security threats relevant to SPEERMINT. A taxonomy of VoIP security threats is defined in [refs.voipsataxonomy] (Zar, J. and et al, “VOIPSA VoIP Security and Privacy Threat Taxonomy,” October 2005.). Such a taxonomy is really comprehensive and takes into account also non-VoIP-specific threats (e.g. loss of power, etc.). Threats relevant to the boundaries of layer-5 SIP networks are extracted from such a taxonomy and mapped to the classification relevant for the SPEERMINT architecture as defined in [refs.speermintarch] (Penno, R., Malas, D., Khan, S., and A. Uzelac, “SPEERMINT Peering Architecture,” August 2007.), moreover additional threats for the SPEERMINT architecture are listed and detailed under the same classification and according the CIA (Confidentiality, Integrity and Availability) triad:

*Look-Up Function (LUF);

*Location Routing Function (LRF);

*Signaling Function (SF);

*Media Function (MF).

2.1. Threats Relevant to the Look-Up Function (LUF)

TOC

If the LUF is hosted locally it is vulnerable to the same threats that affect database systems in general. If the SSP relies on a remote 3rd party to provide the LUF functionality both integrity and authenticity of the responses are at risk.

2.1.1. Threats to LUF Confidentiality

TOC

*SIP URIs and peering domains harvesting - an attacker can exploit this weakness if the underlying database has a weak authentication system, and then use the gained knowledge to launch other kind of attacks.

*3rd party information - a LUF providing information to multiple companies / third parties can attacked to obtain information about third party peering configurations and possible contracts.

2.1.2. Threats to LUF Integrity

TOC

The underlying database could be vulnerable to:

*Injection attack - an attacker could manipulate statements performed on the database by the end user.

2.1.3. Threats to LUF Availability

TOC

The underlying database could be vulnerable to:

*Denial of Service attacks - e.g. an attacker makes incomplete requests causing the server to create an idle state for each of them causing memory to be exhausted.

2.2. Threats Relevant to the Location Routing Function (LRF)

TOC

2.2.1. Threats to LRF Confidentiality

TOC

*URI harvesting - the attacker harvests URIs and IP addresses of the existing User Endpoints (UEs) by issuing a multitude of location requests. Direct intrusion against vulnerable UEs or telemarketing are possible attack scenarios that would use the gained knowledge.

*SIP device enumeration - the attacker discovers the IP address of each intermediate signaling device by looking at the Via and Record-Route headers of a SIP message. Targeting the discovered devices with subsequent attacks is a possible attack scenario.

2.2.2. Threats to LRF Integrity

TOC

An attacker may feed bogus information to the LRF if the routing data is not correctly validated. Dynamic call routing discovery and establishment, as in the scope of SPEERMINT, introduce opportunities for attacks such as the following.

*Man-in-the-Middle attack - the attacker has already or inserts an unauthorized node in the signaling path modifying the SED. The results is that the attacker is then able to read, insert and modify the multimedia communications.

*Incorrect destinations - the attacker redirect the calls to a incorrect destination with the purpose of establishing fraud communications like voice phishing or DoS attacks.

2.2.3. Threats to LRF Availability

TOC

The LRF can be object of DoS attacks. DoS attacks to the LRF can be carried out by sending a large number of queries to the LS or Session Manager, SM, with the result of preventing an originating SSP from looking up call routing data of any URI outside its administrative domain. As an alternative the attacker could target the DNS to disable resolution of SIP addresses.

2.3. Threats to the Signaling Function (SF)

TOC

Signaling function involves a great number of sensitive information. Through signaling function, user agents (UA) assert identities and VSP operators authorize billable resources. Correct and trusted operations of signaling function is essential for service providers. This section discusses potential security threats to the signaling function to detail the possible attack vectors.

TOC

2.3.1. Threats to SF Confidentiality

SF traffic is vulnerable to eavesdropping, in particular when the data is moved across multiple SSPs having different levels of security policies. Threats for the SF confidentiality are listed here:

- *call pattern analysis - the attacker tracks the call patterns of the users violating his/her privacy (e.g. revealing the social network of various users, the daily phone usage, etc.), also rival SSPs may infer information about the customer base of other SSPs in this way;

- *Password cracking - challenge-response authentication mechanism of SIP is not secure if the attacker is able to eavesdrop a sufficient number of SIP authentication messages exchanged between a SIP server and a SIP client.

2.3.2. Threats to SF Integrity

TOC

The integrity of the SF can be violated using SIP request spoofing, SIP reply spoofing and SIP message tampering.

2.3.2.1. SIP Request Spoofing

TOC

Most SIP request spoofing require first a SIP message eavesdropping but some of the them could be also performed by guessing or exploiting broken implementations. Threats in this category are:

> session teardown - the attacker uses CANCEL/BYE messages in order to tear down an existing call at SIP layer, it is needed that the attacker replicates the proper SIP header for the hijacking to be successful (To, From, Call-ID, CSeq);
>
> REGISTER spoofing - the attacker forges a REGISTER request and register a bogus contact information with the objective of hijacking incoming calls.
>
> Billing fraud - the same attack as in the case of the REGISTER spoofing may lead an attacker to be able to direct billing for calls to the victim UE and avoid paying for the phone calls;
>
> user ID spoofing - SSPs are responsible for asserting the legitimacy of user ID; if an SSP fails to achieve the level of identity assertion that the federation it belongs expects, it may create an entry point for attackers to conduct user ID spoofing attacks.

2.3.2.2. SIP Reply Spoofing

TOC

Threats in this category are:

> Forged 200 Response - the attacker sends a forged CANCEL request to terminate a call in progress tricking the terminating UE to believe that the originating UE actually sent it, and successfully hijacks a call sending a forged 200 OK message to the originating UE communicating the address of the rogue UE under the attacker's control;
>
> Forged 302 Response - the attacker sends a forged "302 Moved Temporarily" reply instead of a 200 OK, this enables the attack to hijack the call and to redirect it to any destination UE of his choosing;
>
> Forged 404 Response - the attacker sends a forged "404 Not Found" reply instead of a 200 OK, this enables the attack to disrupt the call establishment;

2.3.2.3. SIP Message Tampering

TOC

This threat involves the alternation of important field values in a SIP message or in the SDP body. Examples of this threat could be the dropping or modification of handshake packets in order to avoid the establishment of a secure RTP session (SRTP). The same approach could be used to degrade the quality of media session by letting UE negotiate a poor quality codec.

2.3.3. Threats to SF Availability

TOC

*Flooding attack - a SBE is susceptible to message flooding attack that may come from interconnected SSPs;

*Session Black Holing - the attacker (assumed to be able to make Man-in-the-Middle attacks) intentionally drops essential packets, e.g. INVITEs, to prevent certain calls from being established;

*SIP Fuzzing attack - fuzzing tests and software can be used by attackers to discover and exploit vulnerabilities of a SIP entity, this attack may result in crashing SIP entity.

2.4. Threats to the Media Function (MF)

TOC

The Media function (MF) is responsible for the actual delivery of multimedia communication between the users and carries sensitive information. Through media function, UE can establish secure communications and monitor quality of conversations. Correct and trusted operations of MF is essential for privacy and service assurance issues. This section discusses potential security threats to the MF to detail the possible attack vectors.

2.4.1. Threats to MF Confidentiality

TOC

The MF is vulnerable to eavesdropping in which the attacker may reconstruct the voice conversation or sensitive information (e.g. PIN numbers from DTMF tones). SRTP and ZRTP are vulnerable to bid-down attacks, i.e. by selectively dropping key exchange protocol packets may result in the establishment of a non-secure communications.

2.4.2. Threats to MF Integrity

TOC

Both RTP and RTCP are vulnerable to integrity violation in many ways:

*Media Hijack - if an attacker can somehow detect an ongoing media session and eavesdrop a few RTP packets, he can start sending bogus RTP packets to one of the UEs involved using the same codec. As illustrated in Fig. 8, if the bogus RTP packets have consistently greater timestamps and sequence numbers (but within the acceptable range) than the legitimate RTP packets, the recipient UE may accept the bogus RTP packets and discard the legitimate ones.

*Media Session Teardown - the attacker sends bogus RTCP BYE messages to a target UE signaling to tear down the media communication, please note that RTCP messages are normally not authenticated.

*QoS degradation - the attacker sends wrong RTCP reports advertising more packet loss or more jitter than actually experimented resulting in the usage of a poor quality codec degrading the overall quality of the call experience.

TOC

2.4.3. Threats to MF Availability

*Malformed messages - the attacker tries to cause a crash or a reboot of the DBE/UE by sending RTP/RTCP malformed messages;

*Messages flooding - the attacker tries to exhaust the resources of the DBE/UE by sending many RTP/RTCP messages.

---

3. Security Requirements

TOC

The security requirements for SPEERMINT have been moved from an earlier version of this draft to the SPEERMINT requirements draft [I-D.ietf-speermint-requirements] (Mule, J., “SPEERMINT Requirements for SIP-based Session Peering,” October 2009.). These security requirements are the following [I-D.ietf-speermint-requirements] (Mule, J., “SPEERMINT Requirements for SIP-based Session Peering,” October 2009.):

*Requirement #15: The protocols used to query the Lookup and Location Routing Functions MUST support mutual authentication.

*Requirement #16: The protocols used to query the Lookup and Location Routing Functions MUST provide support for data confidentiality and integrity

*Requirement #17: The protocols used to enable session peering MUST NOT interfere with the exchanges of media security attributes in SDP. Media attribute lines that are not understood by SBEs MUST be ignored and passed along the signaling path untouched.

The security requirements are currently being finalized and this creates a dependency for this draft. As soon as they will be mature and stable enough this section will provide a mapping of concrete solutions and protocols to meet them.

---

4. Suggested Countermeasures

TOC

This section describes implementer-specific countermeasures against the threats described in the previous section to supplement the security requirements described in [I-D.ietf-speermint-requirements] (Mule, J., “SPEERMINT Requirements for SIP-based Session Peering,” October 2009.). The following table provides a map of the relationships between threats and countermeasures. The suggested countermeasures are discussed in detail in the subsequent subsections.

Group	Threat	Suggested Countermeasure

LUF	Unauthorized access	database BCPs
	SQL injection	database BCPs
	DoS to LUF	database BCPs
LRF	URI harvesting	DNSSEC (DNSSEC)
	SIP equipment enumeration	DNSSEC, privacy protection (Cross-Domain Privacy Protection)
	MitM attack	DNSSEC
	Incorrect destinations	DNSSEC
	DoS to LRF	DNS replication (DNS Replication)
SF	Call pattern analysis	TLS
	Password cracking	TLS
	Session teardown	TLS, TCP (Use TCP instead of UDP to deliver SIP messages), digest authentication (Digest Authentication on all requests in peering agreements), ingress filtering (Ingress Filtering / Reverse-Path Filtering)
	REGISTER spoofing	digest authentication
	Billing fraud	digest authentication
	User ID spoofing	strong identity assertioan (Strong Identity Assertion)
	Forged 200 Response	TLS, TCP, ingress filtering
	Forged 302 Response	TLS, TCP, ingress filtering
	Forged 404 Response	TLS, TCP, ingress filtering
	Flooding attack	reliable border element pooling (Reliable Border Element Pooling), rate limit (Rate limit)
	Session black holing	DNSSEC
	SIP fuzzing attack	border element hardening (Border Element Hardening)
MF	Eavesdropping	SRTP (SRTP)
	Media hijack	SRTP
	Media session teardown	SRTCP (SRTCP)
		SRTCP

	QoS degradation	
	Malformed messages	border element hardening
	Message flooding	rate limit

4.1. Database Security

TOC

Adequate security measures must be applied to the LUF to prevent it from being a target of attacks often seen on common database systems. Common security Best Current Practices (BCPs) for database systems include the use of strong passwords to prevent unauthorized access, parameterized statements to prevent SQL injections and server replication to prevent any database from being a single point of failure. [refs.dbsec] (Gertz, M. and S. Jajodia, “Handbook of Database Security,” .) is one of many existing literatures that describe BCPs in this area.

4.2. DNSSEC

TOC

If DNS is used by the LRF, it is recommended to deploy the recent version of Domain Name System Security Extensions (informally called "DNSSEC-bis") defined by [RFC4033] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.)[RFC4034] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Resource Records for the DNS Security Extensions,” March 2005.)[RFC4035] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “Protocol Modifications for the DNS Security Extensions,” March 2005.) to enhance the security of DNS data using strong cryptography. DNSSEC provides authentication to defend against URI harvesting, SIP equipment enumeration, as well as integrity checking to defend against MitM attacks, session blackholing and other attacks that lead traffic to incorrect destinations.

4.3. DNS Replication

TOC

DNS replication is a very important countermeasure to mitigate DoS attacks on LRF. Simultaneously bringing down multiple DNS servers that support LRF is much more challenging than attacking a sole DNS server (single point of failure).

4.4. Cross-Domain Privacy Protection

TOC

Stripping Via and Record-Route headers, replacing the Contact header, and even changing Call-IDs are the mechanisms described in [RFC3323] (Peterson, J., “A Privacy Mechanism for the Session Initiation Protocol (SIP),” November 2002.) to protect SIP privacy. This practice allows an SSP to hide its SIP network topology, prevents intermediate signaling equipment from becoming the target of DoS attacks, as well as protects the privacy of UEs according to their preferences. This practice is effective in preventing SIP equipment enumeration that exploits LRF.

4.5. Digest Authentication on all requests in peering agreements

TOC

Digest authentication [RFC2617] (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, “HTTP Authentication: Basic and Digest Access Authentication,” June 1999.) is commonly used to challenge REGISTER and INVITE requests in order to prevent REGISTER spoofing and billing fraud. However, it is recommended to apply digest authentication to all SIP requests in peering agreements, especially BYE and CANCEL requests, to prevent session teardown as well.

4.6. Use TCP instead of UDP to deliver SIP messages

TOC

SIP clients need to stay connected with the server on a persistent basis (differently from HTTP clients). Scalability requirements are therefore much more stringent for a SIP server than for a web server. This leads to the choice of UDP as protocol used between SSPs to carry SIP messages (especially for providers with a large user community). New improvements in the Linux kernel [refs.tcp-scalability] (Shemyak, K., “Scalability of TCP Servers, Handling Persistent Connections,” .) show a big increase of the scalability of TCP in handling large number of persistent (but idle) connections. Therefore SSP operators still using UDP for their SIP network should consider switching to TCP. This would significantly increase the difficulty of performing session teardown and forging responses (200, 302, 404 etc). Since look-up and SED data should be exchanged securely (see security requirements), it is further recommended to not only use TCP but TLS for messages exchanged between SSPs.

TOC

4.7. Ingress Filtering / Reverse-Path Filtering

Ingress filtering, i.e., blocking all traffic coming from a host that has a source address different than the addresses that have been assigned to that host (see [RFC2827] (Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," May 2000.)) can effectively prevent UEs from sending packets with a spoofed source IP address. This can be achieved by reverse-path filtering, i.e., only accepting ingress traffic if responses would take the same path. This practice is effective in preventing session teardown and forged SIP replies (200, 302, 404 etc), if the recipient correctly verifies the source IP address for the authenticity of each incoming SIP message.

4.8. Strong Identity Assertion

TOC

"Caller ID spoofing" can be achieved thanks to the weak identity assertion on the From URI of an INVITE request. In a single SSP domain, strong identity assertion can be easily achieved by authenticating each INVITE request. However, in the context of SPEERMINT, only the originating SSP is able to verify the identity directly. In order to overcome this problem there are currently only two major approaches: transitive trust and cryptographic signature. The transitive trust approach builds a chain of trust among different SSP domains. One example of this approach is a combined mechanism specified in [RFC3324] (Watson, M., "Short Term Requirements for Network Asserted Identity," November 2002.) and [RFC3325] (Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.). Using this approach in a transit peering network scenario, the terminating SSP must establish a trust relationship with all SSP domains on the path, which can be seen as an underlying weakness. The use of cryptographic signatures is an alternative approach. "SIP Authenticated Identity Body (AIB)" is specified in [RFC3893] (Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," September 2004.). [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.) introduces two new header fields IDENTITY and IDENTITY-INFO that allow a SIP server in the originating SSP to digitally sign an INVITE request after authenticating the sending UE. The terminating SSP can verify if the INVITE request is signed by a trusted SSP domain. Although this approach does not require the terminating SSP to establish a trust relationship with all transit SSPs on the path, a PKI infrastructure is assumed to be in place.

TOC

4.9. Reliable Border Element Pooling

It is advisable to implement reliable pooling on border elements. An architecture and protocols for the management of server pools supporting mission-critical applications are addressed in the RSERPOOL WG. Using this mechanism (see [RFC3237] (Tuexen, M., Xie, Q., Stewart, R., Shore, M., Ong, L., Loughney, J., and M. Stillman, “Requirements for Reliable Server Pooling,” January 2002.) for requirements), a UE can effectively increase its capacity in handling flooding attacks.

4.10. Rate limit

TOC

Flooding attacks on SF and MF can also be mitigated by limiting the rate of incoming traffic through policing or queuing. In this way legitimate clients can be denied of the service since their traffic may be discarded. Rate limiting can also be applied on a per-source-IP basis under the assumption that the source IP of each attack packet is not spoofed dynamically and will all the limitations related to NAT and mobility issues. It may be preferable to limit the number of concurrent 'sessions', i.e., ongoing calls instead of the messaging associated with it (since session use more resources on backend-systems). When calculating rate limits all entities along the session path should be taken into account. SIP entities on the receiving end of a call may be the limiting factor (e.g., the number of ISDN channels on PSTN gateways) rather than the ingress limiting device.

4.11. Border Element Hardening

TOC

To prevent fuzzing attacks on SPEERMINT border elements these implementations should be security hardened. For instance, fuzz testing is a common black box testing technique used in software engineering. Also, security vulnerability tests can be carried out preventively to assure a UE/SBE/DBE can handle unexpected data correctly without crashing. [RFC4475] (Sparks, R., Hawrylyshen, A., Johnston, A., Rosenberg, J., and H. Schulzrinne, “Session Initiation Protocol (SIP) Torture Test Messages,” May 2006.) and [refs.protos] (Wieser, C., “SIP Robustness Testing for Large-Scale Use,” .) are examples of torture test cases specific for SIP devices and freely available security testing tools, respectively. These type of tests needs to be carried out before product release and in addition throughout the product life cycle.

TOC

4.12. SRTP

Secure Real-time Transport Protocol (SRTP) adds security features to plain RTP by mainly providing encryption using AES to prevent eavesdropping. It also uses HMAC-SHA1 and index keeping to enable message authentication/integrity and replay protection required to prevent media hijack attacks.

4.13. SRTCP

TOC

Secure RTCP (SRTCP) provides the same security-related features to RTCP as SRTP does for RTP. SRTCP is described in [RFC3711] (Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” March 2004.) as optional. In order to prevent media session teardown, it is recommended to turn this feature on.

---

5. Current Deployment of Countermeasures

TOC

At the time of writing this document not all suggested countermeasures are widely deployed. In particular, the following measures to prevent attacks suggested in section Section 4 (Suggested Countermeasures) have not seen wide deployment:

- *DNSSEC
- *Digest authentication on all requests in peering agreements

Nevertheless, these protocols and solutions can provide effective means for preventing some of the attacks with respect to the SPEERMINT architecture described in this document. It is envisioned that these countermeasures will be more widely deployed in the future. Therefore, these mechanisms are listed in this document even though they are not widely deployed today.

---

6. Conclusions

TOC

This memo presented the different SPEERMINT security threats classified in groups related to the LUF, LRF, SF and MF respectively. The multiple instances of the threats are presented with a brief explanation. Afterwards the suggested countermeasures for SPEERMINT were outlined together with possible mitigation of the existing threats by means of them.

---

7. Security Considerations

TOC

This memo is entirely focused on the security threats for SPEERMINT.

---

8. Acknowledgements

TOC

This memo takes inspiration from VOIPSA VoIP Security and Privacy Threat Taxonomy. The authors would like to thank VOIPSA for having produced such a comprehensive taxonomy which is the starting point of this draft. The authors would also like to thank Cullen Jennings for the useful slides presented at the VoIP Management and Security workshop in Vancouver. Further, the authors thank Hendrik Scholz for providing extensive and very helpful comments to this draft.

---

9. Informative References

TOC

[refs.voipsataxonomy]	Zar, J. and et al, “VOIPSA VoIP Security and Privacy Threat Taxonomy,” October 2005.
[refs.speermintarch]	Penno, R., Malas, D., Khan, S., and A. Uzelac, “SPEERMINT Peering Architecture,” draft-ietf-speermint-architecture-04.txt (work in progress), August 2007.
[RFC3263]	Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” RFC 3263, June 2002 (TXT).
[refs.zrtp]	Zimmermann, P., Johnston, A., and J. Callas, “ZRTP: Extensions to RTP for Diffie-Hellman Key Agreement for SRTP,” draft-zimmermann-avt-zrtp-04.txt (work in progress), July 2007.
[refs.tlsbis]	Dierks, T. and E. Rescorla, “The TLS Protocol Version 1.2,” draft-ietf-tls-rfc4346-bis-09.txt (work in progress), February 2008.
[RFC3711]	Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” RFC 3711, March 2004 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” RFC 4474, August 2006 (TXT).
[I-D.ietf-speermint-terminology]	Malas, D. and D. Meyer, “SPEERMINT Terminology,” draft-ietf-speermint-terminology-17 (work in progress), November 2008 (TXT).

[I-D.ietf-speermint-requirements]	Mule, J., "SPEERMINT Requirements for SIP-based Session Peering," draft-ietf-speermint-requirements-09 (work in progress), October 2009 (TXT).
[refs.dbsec]	Gertz, M. and S. Jajodia, "Handbook of Database Security."
[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, March 2005 (TXT).
[RFC4034]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions," RFC 4034, March 2005 (TXT).
[RFC4035]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions," RFC 4035, March 2005 (TXT).
[RFC3323]	Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)," RFC 3323, November 2002 (TXT).
[RFC2617]	Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," RFC 2617, June 1999 (TXT, HTML, XML).
[refs.tcp-scalability]	Shemyak, K., "Scalability of TCP Servers, Handling Persistent Connections."
[RFC2827]	Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," BCP 38, RFC 2827, May 2000 (TXT).
[RFC3324]	Watson, M., "Short Term Requirements for Network Asserted Identity," RFC 3324, November 2002 (TXT).
[RFC3325]	Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," RFC 3325, November 2002 (TXT).
[RFC3893]	Peterson, J., "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format," RFC 3893, September 2004 (TXT).
[RFC3237]	Tuexen, M., Xie, Q., Stewart, R., Shore, M., Ong, L., Loughney, J., and M. Stillman, "Requirements for Reliable Server Pooling," RFC 3237, January 2002 (TXT).
[refs.protos]	Wieser, C., "SIP Robustness Testing for Large-Scale Use."
[RFC4475]	Sparks, R., Hawrylyshen, A., Johnston, A., Rosenberg, J., and H. Schulzrinne, "Session

	Initiation Protocol (SIP) Torture Test Messages," RFC 4475, May 2006 (TXT).

Authors' Addresses

TOC

	Saverio Niccolini
	NEC Laboratories Europe, NEC Europe Ltd.
	Kurfuersten-Anlage 36
	Heidelberg 69115
	Germany
Phone:	+49 (0) 6221 4342 118
Email:	niccolini@nw.neclab.eu
URI:	http://www.nw.neclab.eu
	Eric Chen
	Information Sharing Platform Laboratories, NTT
	3-9-11 Midori-cho
	Musashino, Tokyo 180-8585
	Japan
Email:	eric.chen@lab.ntt.co.jp
URI:	http://www.ntt.co.jp/index_e.html
	Jan Seedorf
	NEC Laboratories Europe, NEC Europe Ltd.
	Kurfuersten-Anlage 36
	Heidelberg 69115
	Germany
Phone:	+49 (0) 6221 4342 221
Email:	seedorf@nw.neclab.eu
URI:	http://www.nw.neclab.eu
	Hendrik Scholz
	freenet Cityline GmbH
	Am Germaniahafen 1-7
	Kiel 24143
	Germany
Phone:	+49 (0) 431 9020 552
Email:	hendrik.scholz@freenet.ag
URI:	http://freenet.ag

Full Copyright Statement

TOC

Intellectual Property