Towards Standardized Prevention of Unsolicited Communications and Phishing Attacks

JaeSeung Song and Andreas Kunz

NEC Laboratories Europe

Received 3 April 2013; Accepted 14 May 2013

Abstract

The world of communication technology is changing fast and the means of communication are moving towards a packet switched transmission systems such as Voice over IP (VoIP). Formerly call identity spoofing of the displayed number in circuit switched (CS) networks was too difficult to perform so that people could be sure that when receiving a call on their mobile phone or at home, the displayed number is the one as it is supposed to be. Nowadays this is not the case anymore, voice communication from the internet with VoIP is cheap and spam calls can be easily realized without any costs, also it is getting easier to perform spoofed calls with wrong display name or number.

The mobile network operators have no mechanisms to tackle those threats, but standardization activities are already in place within the security group SA3 of 3GPP. This paper provides an overview of the current status of the standards activities and shows the most promising solutions that are proposed up to now. The proposed solutions detect unsolicited communications and spoofed calls by tracing back to the displayed number used in the attack.

Keywords: Spam, Unsolicited Communication, Voice Phishing, Call Id Spoofing.

Journal of ICT Standardization, Vol. 1, 109–122.
doi: 10.13052/jicts2245-800X .126

1 Introduction

Unsolicited communication (UC) is defined bulk voice communication in communication networks where the benefit is weighted in favor of the sender [1]. Due to its anonymous, low cost and easy-to-use applications, unsolicited communication has become a popular method used by attackers [23]. Although many solutions protecting unsolicited communication exist [11], the volume of spam emails and the amount of financial damages are increasing rapidly every year [24]. Protecting users from unsolicited communication is now an important topic among network operators and system vendors, because it enables to provide high-quality services to users and helps to reduce management costs. However, this requires collaborations between stakeholders such as customers, operators, system vendors and legitimate organizations. To tackle this problem, various standards organizations (SDOs) have started their studies in this area.

The remainder of this article is organized as follows. The next section gives background information about security threats in unsolicited communications. Section 3 provides various SDOs' latest standardization activities related to unsolicited communications together with a potential solution. In Section 4, we focus our attention specifically on voice spoofing attacks and describe latest standardization activities. We also present our prototype implementation. After that the paper finishes with conclusions in Section 5.

2 Security Threats in Unsolicited Communications

The introduction of low-cost communications to operators' networks, such as VoIP and IP Multimedia Sub-system (IMS) [17], imposes many security threats by unsolicited communications, as listed below. Compared to the traditional voice networks, e.g., Public Switched Telephone Networks (PSTN), network operators provide significantly low-cost VoIP based services such as SMS, email and voice call. The customers have been enjoying such services because they are very attractive from the cost aspect and provide various rich multimedia services. On the other hand, this makes VoIP an attractive carrier for delivering unsolicited communications by spammers or attackers.

There exist security mechanisms provided by such networks or services, however, customers are still suffering from several types of security threats, for instance, fraud, spam emails and voice phishing attacks. We describe several well-known security threats resulting from unsolicited communication as follows:

- Flooding attack [20]: The attacker can generate a large number of unsolicited messages and send them to victims such as terminals and network nodes.
- Spam-over-Internet-Telephony (SPIT) [21]: This attack is similar to E-mail spam. The attacker disturbs users or group of users through placing unsolicited calls. Since such unsolicited calls can be made using bots or other malicious software at any time (for instance at the midnight) with extremely low costs, many network operators are seeking a solution for protecting unsolicited communication in their VoIP networks.
- Private information leakage [22]: A victim may receive a spoofed call with a call ID that is known by the victim to be the one from his bank and the victim may provide private information or passwords about his bank account. Conversations and messages can easily be intercepted by attackers, e.g. in case he mobile operator uses the call ID for providing access to the voice mailbox, which lead the leakage of private information.

Although existing solutions provide a certain level of protections to customers, they often fail to detect such threats because legislation issues and frequent changes of threat patterns [25].

The threats listed above usually harm user experience and cause annoyance for users. On the other hand, there exist other types of threats used for taking a monetary benefit from the user, which is called "voice phishing". Typically, attackers modify the caller ID, i.e., displayed telephone number, of incoming call and pretend themselves as a trustworthy person or legitimate organizations such as bank [20]. This caller ID spoofing can easily be made through various methods, for instance using a VoIP client or spoofing web sites. Since the damage caused by phishing attacks has been increasing steeply in the recent years [18], there is a strong need for protecting customers against voice phishing attacks.

3 Prevention of Unsolicited Communications

The growth of the bandwidth capacities in the networks due to the demand of more and more resource hungry applications and the highly competitive market situation of the network operators led to a significant decrease of the prices for data connectivity services. Now it became very cheap and easy for attackers to distribute unsolicited voice communication, since only a SIP-Server is needed with nearly no costs in distributing the messages to a huge amount of (randomly) selected recipients. There are several services

that can be realized with SIP such as multimedia video, voice, messaging, etc. standardized by the Internet Engineering Task Force (IETF). 3GPP then further reused the IETF work and created services for operators in the IP Multimedia Subsystem (IMS) [17], which can be used as well by fixed and mobile network operators. All those services can be misused for unsolicited communication.

3.1 Status of Standardization

Since unsolicited communication is becoming a more and more common issue for operators around the world [25], several standardization organizations already looked into the problem and tried to address it for selective services. [18] gives a short overview on the past standardization activities. IETF discussed several internet drafts about SPam over Internet Telephony (SPIT), but all of them expired and no RFC was created. There is no active work in IETF on this topic. ETSI TISPAN performed two studies [5, 6] on prevention of unsolicited communication in the Next Generation Network (NGN). The security group of ITU-T produced several recommendations ([12–16]), analyzing the different types of unsolicited multimedia communication. The recommendations on the overall aspects [15] proposes corresponding countermeasures, but only limited to authentication, authorization and security management. The technical strategies [12] and the overall framework [16] differentiate between store-and-forward and real-time communication for the type of the service. The technical strategies propose a hierarchical model with filtering strategies, feedback strategies [12], service strategies, equipment strategies and network strategies. The framework consists of anti-spam functions on sender, core and recipient side, which can perform several actions e.g., protocol analysis and filtering. GSMA focus with their recommendation on call ID spoofing and phishing attacks, which are the main frauds in the mobile networks, but with the introduction of IMS for voice and multimedia services also other unsolicited multimedia communication will increase. 3GPP is the only major standardization organization that is at the moment still trying to find a solution for the prevention of unsolicited communication and call spoofing attacks. Two studies were carried out for Prevention of Unsolicited Communication in IMS (PUCI) ([1, 2]) and a new study is actively discussed on the prevention of caller ID spoofing [19]. Even the two studies on PUCI did not lead to normative work up to now; nevertheless the findings of the work are worthwhile to be described further in more details.

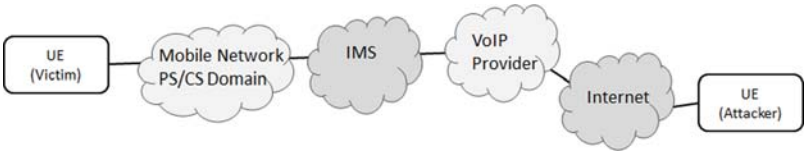

Figure 1 UC Source outside the operator network

3.2 Scenarios

3GPP analyzed in [1] the two basic scenarios of the threat of unsolicited communication (UC), i.e., the source of the UC is:

- Inside the mobile operator home network of the victim
- Outside the mobile operator home network, as shown in Figure 1

Depending on the location of the UC source, different network nodes are impacted in order to host the functionality to prevent that the UC is successfully established to the victim and to block the UC setup attempts. There are many accompanying threats e.g., like cost creation if the victim has supplementary services enabled like call forwarding, victim is roaming, phishing, equipment hijacking etc.

All communication services available in IMS were considered as potential source of UC, therefore all solutions analyze the SIP signaling and treat the session accordingly.

3.3 Available Solutions and Analysis

There are two main solutions that can be applied effectively to fight UC in the network: one based on supplementary services and one based on identification, marking and reacting to the UC session (IMR).

3.3.1 UC Protection with Supplementary Service

Using supplementary services is from deployment perspective the easiest way to provide a limited protection against UC to the end customers. Supplementary services are usually hosted in the Telephony Application Server (TAS). Figure 2 shows a simple architecture where the attacker and the victim are located in the same IMS network:

The user devices, called User Equipment (UE) connect to the proxy server (Proxy Call Session Control Function, P-CSCF) in the IMS network. The P-CSCF itself connects to the Serving Call Session Control Function (S-CSCF), which provides originating and terminating services with the help of

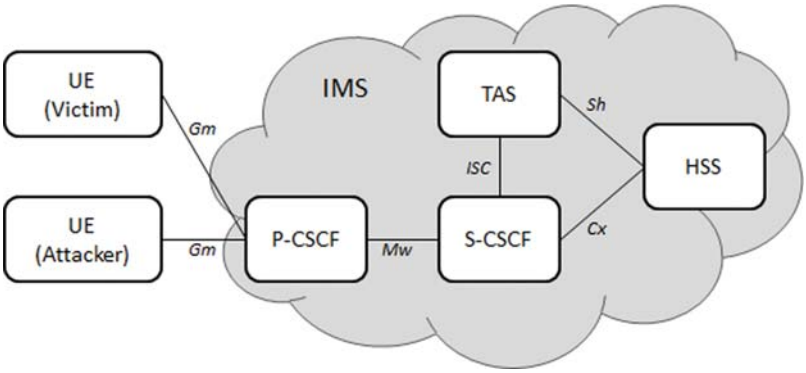

Figure 2 : Simple IMS Network Architecture

Application Servers (AS) based on the subscriber profile, downloaded from the Home Subscriber Server (HSS) at the time of registration. The IMS network itself is access agnostic and can provide multimedia services for fixed and mobile networks.

There are several supplementary services that are suitable for filtering incoming session requests:

- Incoming Call Barring with White List: the caller's ID is compared with the white list and the session setup is interrupted if the calling ID is not on the list
- Incoming Call Barring with Black List: the caller's ID is compared with the black list and the session setup is interrupted if the calling ID is on the list
- Anonymous Call Rejection: session setups without calling ID, i.e., restricted asserted public user ID, are rejected
- Closed User Groups: special trust network based on white list
- Call Diversion on Originating Identity: the callee can redirect the incoming session, e.g., to a mailbox
- Malicious Customer Identification: generates a trace of the last anonymous session to identify the source

All these supplementary services can be of course also combined, the disadvantage of such a solution is that the configuration is not updated in real time, e.g., customers configure their black and white lists based on their experience and normal call behaviour. If e.g., an attacker creates outside the network random public user ids for unsolicited communication, the black listing filtering would be not successful. Using white lists would prevent

this, but this has the drawback that the user can be called only by the very limited and comparable small group of people on the list. For this reason another solution is described in the next chapter, which overcomes those problems.

3.3.2 UC Protection with IMR

In order to be able to dynamically react on unsolicited communication attacks, those sessions need to be identified, marked for further processing and afterwards a decision is taken to react to the attack. This concept is called IMR (Identification, Marking, Reaction).

The incoming session request is then processed according to the three stages:

- Identification: the UC identification can be classified into three categories:
  - Non-intrusive tests: analysis of session signaling
  - Intrusive tests: caller test to identify UC attempt
  - Feedback by user: personal black list, react during call etc.
- Marking: The session gets marked with a UC score to rate the session.
- Reaction: based on the UC score different actions can be performed, e.g., blocking the session, redirection to mailbox, automatic update of filter lists etc.

Figure 3 shows the simplified IMS architecture with attacker and victim in the same network and with IMR functionality in the Application Server (AS) and in the S-CSCF. The AS could also interact with a content inspection function in order to test the incoming session, e.g., by playing an announcement at the Media Resource Function (MRF) to press certain keys and then to analyze the DTMF answer from the caller. If the caller would be an attacker who does random calls in order to play e.g., commercials then it cannot answer the test and would be classified as UC.

The S-CSCF could also do some simple testing, e.g., analyzing the session setup rate from a specific source and then mark the sessions accordingly.

All tested sessions are marked with the UC score, the result of the tests. There may be only one test, but there could be also different tests in sequence and the UC score would be updated accordingly. If the UC score is transmitted between operators, then it would be beneficial also to agree for the UC score in the Service Level Agreements (SLA) on the range and the threshold, i.e., the UC score from when onwards an operator considers a session to be UC.

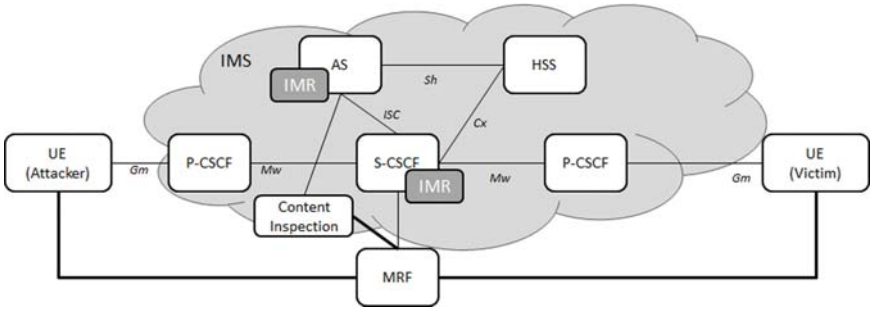

Figure 3 : Simplified IMR Architecture

Incoming session requests that got already tested and marked in the originating network can then be mapped to the UC score used in the intermediate or terminating network. The terminating operator can then decide how to react on the session request.

3.4 Proposed Solution

Operators should start and take countermeasures to the increasing problem of UC attacks in the networks. Starting with a basic solution with Supplementary Services that provides some elemental protection of the subscribers, it is recommended to use an IMR system to test incoming and outgoing session requests. Only with an IMR solution it is possible to identify also more sophisticated UC session requests and to react dynamically to them. Additionally the IMR system is learning and can dynamically update filter lists according to the tests.

4 Prevention of Voice Phishing Attacks

Voice phishing called vishing is a scam usually carried out by unsolicited communication in particular using voice call to obtain sensitive information from users, such as login credentials or information to be used for identity theft. The main objective of the attacker is usually to gain monetary benefits from victims. In this section we provide an overview of latest standard activities of the two major SDOs (i.e., 3GPP and TISPAN) together with potential solutions to prevent voice phishing attacks. We also introduce a prototype implementation to show the feasibility of the proposed solution in Section 4.3.

4.1 Use Cases and Attack Scenarios

So far most work that has been done in 3GPP regarding spoofed call detection and prevention is about analyzing various use cases. PUCI TR [1] addresses two popular use cases which are often used by attackers for phishing. There exist various scenarios achieving these use cases. In this section we introduce these use cases together with some popular phishing attack scenarios.

Use cases: A main purpose of phishing attacks is for financial gain of the attacker. The attacker usually tries to get sensitive information from users such as bank account information and login credentials.

The first use case is about the *leakage of personal bank account information*. Similar to email phishing scams, the attacker approaches users using phone calls pretending to be from the bank or the government organization. The attacker then asks victims to disclose their bank account information or transfer money. Sometimes the attacker even tries a prior call where no information is required in order to convince victims that the call is from a legitimate bank. The user is then easily fooled by receiving a subsequent call, which refers to the initial call.

Secondly, identity theft is introduced as another popular voice phishing use case. The attacker aims to get personal information from a victim, and the information is then used to obtain credit in the name of the victim. One popular example, for instance, is to call a user and saying the user has won a prize. The user is asked to provide certain sensitive personal information to collect the prize.

Attack scenarios: The attacker uses various methods to trick users to make them believe a call is from a legitimate company or organization. Figure 4 shows four common voice spoofing scenarios, and they are described in the following:

1. **IMS Application Server**: Within IMS, application servers acting as a back-to-back user agent (B2BUA) can be deployed by 3rd party service provider. Such application servers can easily change the identities of the incoming SIP request and initiates a new one with faked ID towards the victim.
2. **Private Branch eXchange (PBX)**: In a typical telecommunications system, a Primary Rate Interface (PRI) is used to establish a connection between a PBX and a local network. Such PRI trunks are generally trusted by the network operator, and any caller ID through these trunks are delivered to the user without verifications.

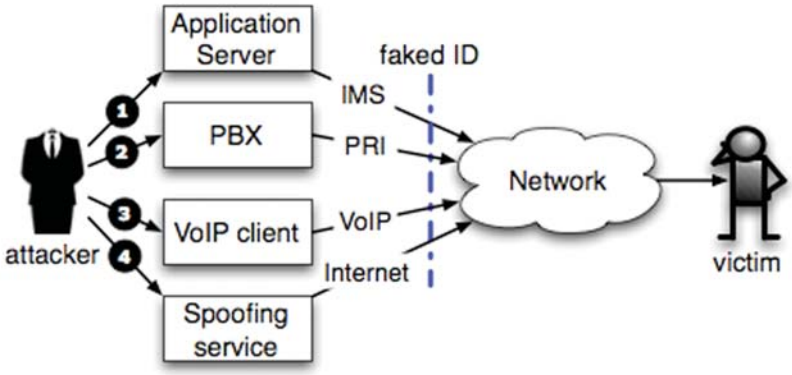

Figure 4 Common voice spoofing scenarios

3. **VoIP client**: Using VoIP clients is the easiest way to generate spoofed calls. There exist many VoIP clients that allow the attacker to attach a spoofed caller ID to the destination field of the data packet. For instance, in the SIP protocol [8], caller ID is provided by the "From" header of a SIP message in requests.
4. **Caller ID Spoofing service**: There are many online web sites providing a caller ID spoofing service. The attacker can easily subscribe such service and modify the caller ID. In this case, the faked caller ID is displayed on the victim's UE to a legitimate entity such as bank and policy station.

4.2 Available Solutions and Analysis

There exist many different proposed solutions to protect users from voice phishing attacks. They can be roughly categorized into three types: (1) *voice analysis*, (2) *blacklist* & *whitelist* and (3) *runtime ID checks*. Each technology is described in the followings.

Voice analysis: Several solutions recently proposed introduce a mechanism analyzing an incoming voice call to find a pattern that can distinguish spoofed calls from normal calls. PinDr0p [7] assists users to guess the source and the path taken by a call through analyzing network specific characteristics such as packet loss, noise profiles and applied voice codecs. It is possible to use an algorithm based on Gaussian mixture model. Chang et al. [9] use the fact that the human voice can be used for detection of deception. For instance, the voice of a liar usually has a larger pitch lag value than the normal voice.

Chang et al. first extract coding parameters followed by selecting relevant feature vectors to detect voice phishing.

Although such algorithms can easily be implemented in the user's terminal, the main problem is that analyzing codecs and characteristics of the call can require significant processing power. In addition, these voice analysis methods would be unable to cope with all different kinds of phishing attacks.

Blacklist & whitelist: The use of a blacklist (or a whitelist) [10] which can detect previously known phishing (or legitimate) caller IDs can reduce the traffic usage by filtering phishing attacks at the earliest possible stage; that is, before forwarding them to the callee. Surely, it would be difficult to maintain the latest blacklists (or whitelists) either on mobile phones or on the database deployed in network entities. There also exist several legal issues that need to be considered by network operators when rejecting incoming calls from certain user accounts. For example, there will always be countries where it is legal to send SPIT.

Runtime ID checks: When spoofed calls are delivered to end users, they usually do not have enough information to judge that the caller ID is spoofed. On the other hand, the first entry point to the operator network has a lot more information. This first entity can be used to initiate a verification process of the originating party caller ID to check whether there is an ongoing call to the request caller ID. Although this requires an enhancement to an interworking gateway (i.e., the entry point of the operator network), such method provide several advantages over others, including no impact on call setup time and performance.

4.3 Proposed System Implementation

Since VoIP is a real-time communication, we believe that a method checking the caller ID at runtime is a promising solution to detect phishing attacks while avoiding many drawbacks. Since different players, such as the mobile network operator, entities that want to be trusted (banks, governments, etc.) and customers, are involved in providing the protection of voice phishing attacks, standards are required to define information exchange procedures. This section describes a system that we developed and implemented to provide runtime caller ID verification.

We introduce a system that detects possible voice phishing attacks through checking the display name of an incoming call at runtime. First, the system uses the fact that the display number is faked in a spoofed call and subject for the verification. Second, the system performs the verification process at

runtime either initiated by user on-demand or as a supplementary service. A method used in the system traces back through the incoming call routes to the entity that operates the actual caller ID in order to detect spoofed calls.

Figure 5 shows a simplified architecture together with the caller ID verification procedure. To know a caller is using a faked caller ID, the callee initiates the caller ID verification process by asking the interworking GW (Ingress Entity) to check (1, 2). When the GW is asked by the user (3), it formulates a verification request message with the display number and forwards the message to the actual organization that owns the display number (4). The organization then checks its registered subscribers whether any of them are using the faked display number (5). The verification results are then reported to help the user decides the call is spoofed (6).

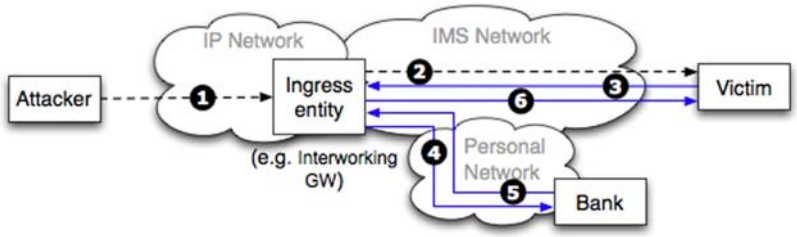

Figure 5 A potential high level architecture

5 Conclusions

This paper has provided an overview of standardization activities associated with preventing unsolicited communications. Unsolicited communications, such as spam emails and voice phishing attacks, are becoming a serious problem for both users and network systems. Therefore, studies and specifications in various SDOs have gained broad industry attention and support. Most SDOs, such as 3GPP, ITU-T, TISPAN, etc., have completed their study on the analysis of unsolicited communications and are now considering to start normative work to standardize a solution for protecting unsolicited communication attacks.

After introducing several existing solutions, we proposed potential frameworks in Sections 3.4 and 4.4 to mitigate the threats from both unsolicited communications and call spoofing attacks, respectively. We show that these solutions easily can be introduced to the existing network architectures while having minimal impact to the current network architecture and network design.

As a future work, we intend to integrate two proposed systems into a generic UC protection system in order to reduce complexities and maintenance cost. For instance, through combining the proposed systems in Sections 3.4 and 4.4, we can manage a single unified blacklist/whitelist for all UC calls.

References

[1] 3GPP TR 33.937 "Study of mechanisms for Protection against Unsolicited Communication for IMS (PUCI)"
[2] 3GPP TR 33.838 "Study on Protection against Unsolicited Communication for IMS (PUCI)"
[3] 3GPP S3-121245 "Security study on spoofed call detection and prevention;(Release 12)"
[4] 3GPP TS 24.416 "TISPAN; PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol specification"
[5] ETSI TR 187 015 Ver. 3.1.1, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Prevention of Unsolicited Communication in the NGN"
[6] TR 187 009 Ver. 2.1.1 "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN"
[7] Balasubramaniyan, V.A., Poonawalla, A., Ahamad, M., Hunter, M.T., Traynor, P.: Pindr0p: using single-ended audio features to determine call provenance. In: Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, pp. 109-120. ACM, New York, NY, USA (2010).
[8] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard) (2002). URL http://www.ietf.org/rfc/rfc3261.txt
[9] Chang, J.H., Lee, K.H.: Voice phishing detection technique based on minimum classification error method incorporating codec parameters. Signal Processing, IET 4(5), 502-509 (Oct.)
[10] Kolan, P., Dantu, R.: Socio-technical defense against voice spamming. ACM Tranactions on Autonomous and Adaptive Systems (TAAS). 2(1) (2007)
[11] Schmidt, A., Leicher, A., Shah, Y., Cha, I., Guccione, L.: Sender scorecards for the pre vention of unsolicited communication. In: Collaborative Security Technologies (CoSec), 2010 IEEE 2nd Workshop on, pp. 1-6 (2010)
[12] X.1231 Technical strategies for countering spam
[13] X.1242 Short message service (SMS) spam filtering system based on user-specified rules
[14] X.1243 Interactive gateway system for countering spam
[15] X.1244 Overall aspects of countering spam in IP-based multimedia applications
[16] X.1245 Framework for countering spam in IP-based multimedia applications
[17] 3GPP TS 23.228 "IP Multimedia Subsystem (IMS); Stage 2"
[18] Nico d'Heureuse, Jan Seedorf, Saverio Niccolini, Thilo Ewald: Protecting SIP-based Networks and Services from Unwanted Communications. IEEE "GLOBECOM" 2008

[19] 3GPP TR 33.8de "Security study on spoofed call detection and prevention; (Release 12)", S3-130242
[20] Keromytis, A.: A survey of voice over ip security research. In: A. Prakash, I. Sen Gupta(eds.) Information Systems Security, Lecture Notes in Computer Science, vol. 5905, pp. 1 – 17. Springer Berlin Heidelberg (2009)
[21] Quittek, J., Niccolini, S., Tartarelli, S., Schlegel, R.: On spam over internet telephony (SPIT) prevention. Communications Magazine, IEEE 46(8), 80 – 86 (2008)
[22] Neumann, T., Tillwick, H., Olivier, M.: Information leakage in ubiquitous voice-over-ip communications. In Trust and Privacy in Digital Business, Lecture Notes in Computer Science, vol. 4083, pp. 233-242. (2006)
[23] Nassar, M., Niccolini, S., State, R., Ewald, T.: Holistic voip intrusion detection and prevention system. In Proceedings of the 1^{st} international conference on Principles, systems and applications of IP telecommunications, IPTComm '07, pp. 1-9 (2007)
[24] J.Rosenberg and C. Jennings, "The Session Initiation Protocol (SIP) and Spam" IETF RFC 5039, jan. (2008)
[25] Frost, N.: VoIP: VoIP threats – getting louder. Netw. Secur. 2006 (3), 16-18 (2006)

Biography

JaeSeung Song is currently working as a senior researcher and oneM2M standardization engineer at NEC Europe Ltd, Heidelberg, Germany.Previously, he worked for LG Electronics as a senior research engineerfrom 2002 to 2008. He received a PhD at Imperial College London in theDepartment of Computing, United Kingdom andBS and MS degrees fromSogang University.

Andreas Kunz received his diploma degree and his Ph.D. in Electrical Engineering from the University of Siegen, Germany. He is working for NEC Laboratories Europe with focus on 3GPP standardization, mainly in the system architecture working group.