Prevention of Unsolicited Communication in IMS Networks using Sender Scorecards

Andreas U. Schmidt, *Member, IEEE,* Andreas Leicher, Novalyst IT AG
Yogendra Shah, Inhyok Cha, Louis Guccione, InterDigital, Inc.

Abstract— **Unsolicited communication is a major issue in digital communications and hence for the networks enabling such communication. With the increasing use of IP Multimedia Subsystem (IMS) networks, protection of time-critical communication, e.g. Voice over IP, from unsolicited messages, becomes an important topic. 3GPP identified and developed various concepts to cope with unsolicited communication in IMS networks (UCI) in 3GPP TR 33.937. The Protection against UCI (PUCI) borrows concepts from traditional email SPAM filtering but needs to adapt to the nature of IMS communication being direct and time critical. In addition to the protection methods identified in TR 33.937 we present a concept which uses a secure and interoperable scorecard which is associated with the caller and the IMS communication. Depending on the outcome of the scorecard evaluation, the receiving domain can take appropriate actions such as denying or allowing a communication attempt. Scorecards are used to generate a standardized exchange format for sender and message related information. Based on 3GPP standards we present an IMS architecture with scorecard elements, including basic operating procedures for the prevention of UCI.**

Index Terms—**IMS, SPAM, SPIT, 3GPP.**

I. Introduction

Sender Scorecards are conceived as a method to enable different IP Multimedia Subsystem (IMS) domains and networks to exchange trustworthy information on sender identities and other relevant information, to allow discrimination between legitimate and unsolicited IMS communication. Such a scorecard is generated, transported, and evaluated collaboratively between different network domains. Scorecards are used to generate a standardized exchange format for sender and message related information.

In the form of SPAM, unsolicited communication (UC) makes up the bulk of email traffic. However, filtering methods protect users from SPAM by inspecting email before it reaches their inbox. For time-critical communication over the Internet, such as Voice-over-IP (VoIP), the situation is different, since each incoming communication requires a user action resulting in limiting the use of automatic filtering. The so-called SPIT (SPAM over Internet Telephony) therefore represents an emerging threat to users and networks, due to the high bandwidth consumption. Similar threats are valid for large-scale networks based on the IP Multimedia Subsystem (IMS), in the context of which it is termed Unsolicited Communication over IMS (UCI), and its prevention is called PUCI. PUCI has been considered in standardization bodies such as 3GPP TSG SA WG3 (security working group) in a technical report [1] which collects various countermeasures against UCI in the context of IMS system architectures. In [1] 3GPP two broad categories of UCI, namely SPAM over IMS (SPIM) and SPIT are considered. We build our concept on the countermeasures and architecture defined in [1].

The main difference between email spam and UCI is, that an email arrives at the email server before it is accessed by the user. This means, that structure and content of an email can be analyzed at the server before it arrives at the recipient and so email spam can be detected before it disturbs the recipient. As in VoIP and IMS communication scenarios delays of communication establishment are not wished, session establishment messages are forwarded immediately to the recipients. Besides this fact the content of a VoIP call is exchanged immediately after the session is established. In other words if the phone rings it is too late for SPIT prevention and the phone rings immediately after session initiation, while an email can be delayed and even, if it is not delayed, the recipient can decide if he wants to read the email immediately or not. In addition to these aspects another main difference between email spam and UCI is the fact, that the single email itself contains information, that can be used for spam detection. The header fields, for example, may contain information about sender, subject and content of the message. UCI in contradiction is technically indistinguishable from a legitimate communication attempt, as it is initiated and answered with the same set of protocol messages as any other IMS communication.

The following are the most widely used countermeasures against SPIT:

- **Active and passive device fingerprinting**, as presented in [2], try to identify a SPIT session attempt using knowledge about the type of User Agent (UA) initiating the call and by comparing header layout and order or the response behavior of a SIP UA with a typical UA.
- **White-, black- and greylists** developed for SPAM mitigation, find their counterparts as SPIT countermeasures [3], [4].
- In **reputation based mechanisms** [5], [6], reputation values are assigned to the identity of the caller and can be used across multiple sessions.
- By **Turing tests, computational puzzles, and CAPTCHAS** [7], [8], challenges are used to distinguish humans from machines. Legitimate callers will not be able to get an immediate connection, and the protection may be circumvented by using (an inexpensive) human

workforce.

- The idea of **payments at risk** [9] is to raise costs for SPIT callers, especially for the typical high-volume call attempts, while keeping legitimate calls inexpensive.

Most methods for SPIT prevention in the literature such as in [10], [11], as well as the UCI countermeasures in [1], follow the paradigm of perimeter security, where the main defense is provided by the receiving domain. The Identification-Marking-Reaction (IMR) architecture [1] integrates multiple of such countermeasures in a ’holistic’ approach.

Applying perimeter security measures to SPIT/UCI has principal limitations, due to the lack of trust in any information coming from the sender domain (which can include non-IMS, non-trusted domains), sender UAs, or intermediate nodes [12], [13]. In particular, it was previously shown in [13], that the first line of defense of a receiving domain in common VoIP networks, the Session Broder Controller (SBC), can be bypassed by an attacker who carefully controls his call rate and cyclically rotates caller identities within a small set of (fake) IDs.

This led us to the idea of a PUCI method relying on inter-domain collaboration and information exchange based on Sender Scorecards (SSC). These PUCI SSC, transport trustworthy information that can be used in UCI classification and also supplement any other existing countermeasure such as those described earlier in this section. SSC is therefore an orthogonal concept to the traditional mitigation methods, and could in particular be combined with IMR, for instance.

Originally used as a performance measurement instrument, e.g. in the form of balanced scorecards [14], scorecards can also be used in SPIT prevention [15]. We further developed this concept, providing a framework to create, manage, and transport UCI score information between domains. Such information can be about sender trustworthiness such as identity and authentication strength, reputation or device security properties, as well as trust properties of intermediate nodes and networks, or message properties, e.g. protocol header information assessment.

In Section II, an architecture for inclusion of scorecard information in an IMS network is sketched. Section III shows basic SSC processing and call flows in a template fashion and proposes an expression format for SSCs. Section IV concludes the paper with an outlook to concrete realisation options.

II. Sender Scorecards in IMS Architecture

Our approach is to provide an umbrella scheme for heterogeneous sender information in PUCI Sender Scorecards, which are generated and managed by an intermediate architectural layer between the sender and receiver of the communication. Our scorecards provide reliable assurance of the properties of the sending user agent device, using a standardized approach to allow exchange of information between IMS and non-IMS domains.

A general scheme to transport sender identity and other information, relevant for UCI detection and prevention across different identifier domains, i.e. IMS and non-IMS networks must fulfill different requirements. It must provide reliable assurance on different properties of the sending user agent device for the receiving domain. However, the establishment, verification and certification of properties can be different between the IMS (and non-IMS) networks. By the use of a standardized scorecard approach, the receiving domain is able to verify received information from the sender domain and build its decision on whether to allow or disallow communication to the receiving UA in domain B.

TABLE I
Scorecard content example.

Category	Claim	Score	Atribute
Identification	Authenticated using username and password	3	Verified by V_0 at t_0
Identification	Can be resolved to a physical identity	9	Verified by V_1 at t_1
Device	Is certified by manufacturer	4	Verified by V_2 at t_2
Device	Has been integrity checked	8	Verified by V_i at t_i
Reputation	Reputation score in community X is *high*	6	Verified by V_n at t_n

Each scorecard contains multiple entries, each of them having a single category, a claim which defines the property in this category, a score, which is globally defined and comparable, and an attribute field which keeps track of the state of the claim. The scorecard allows the receiving network and UA to assess the level of SPIT/SPAM probability using a standardised format for information exchange.

Categories and scores must be comparable, e.g. by standardisation and agreements between domain operators. Different claims allow to assert properties on the sender and sending device. Examples are given in Table I. The verification of the claims and the attribute field, reflecting any changes to the state of a claim, play a central role in the concept of the scorecards. The approach is implementation independent in the sense that the structure is standardised, whereas actual claims and properties which can be asserted will vary depending on the network’s and device’s capabilities.

A. Scorecard Expression Format

Technically, several options for the implementation of the scorecards are possible; one example would be a XML scheme which provides the necessary portability across the different domains. The XML scheme could be embedded or complemented by SAML assertions. With the use of SAML assertions it could be possible to implement scorecards in which different claims are verified and signed by different entities. This allows for a heterogeneous approach, in which not one single entity has to verify all claims before issuing the scorecard, but can instead rely on assertions made by other claim verifiers.

B. Architecture for Scorecards

We introduce new architecture entities for the creation and processing of PUCI SSCs. We build on the existing IMS infrastructure by adding the needed entities in a modular way. Figure 1 gives an overview of the architecture, showing two different operator domains.

Scorecards are provided by a new entity, the scorecard issuer (SC-I), in each domain for the sending devices in this domain. Upon initiation of an IMS connection, the device requests a scorecard from the SC-I. The device authenticates towards the SC-I, which allows the SC-I to look up if it has previously issued a scorecard for this device. If the SC-I stored a scorecard for this device it may check if existing data needs to be updated. If no scorecard exists, the SC-I creates the SSC including all the property claims that the device and sending network can fulfil. Such properties can for example include the authentication strength, the level of identification, reputation, device integrity verification and previous call behaviour. The SC-I signs the statements such that the receiving network can verify the property claims. The SC-I is responsible for the verification of the claims, before adding them to the scorecard. The SC-I could be implemented in different ways, but the simplest form would verify all claims and sign them. Depending on the network architecture, even more complex schemes can be employed, e.g. by relying on claim assertions made by other (trusted) third parties, and only verifying a subset of the scorecard at the SC-I. The SC-I should then at least provide a timestamp and a signature on the final scorecard, allowing for a statement of freshness and authenticity. The creation and update process for scorecards is bound to the authentication of the sending device for the communication session. The scorecard will be uniquely identifiable and the SC-I which issued the card can always be identified. The SC-I then stores the new scorecard in the network or, if the device is able to securely store the card, send the card to the device. In either case, the scorecard is sent together with the session initialization message from sender A to a scorecard proxy (SC-P) in the receiving domain.

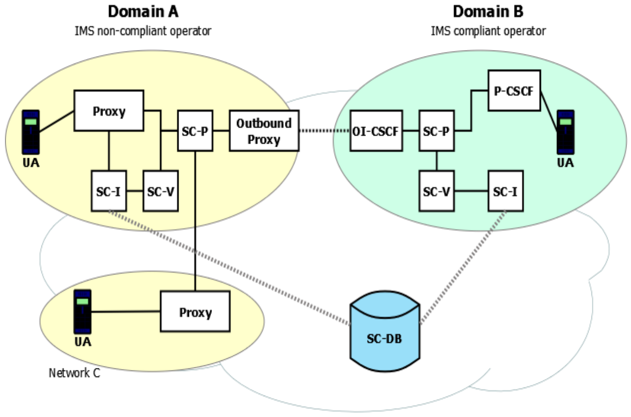

Fig. 1. Basic Scorecard Architecture

In the receiving domain, the first point of contact will be the SC-P which upon receipt of a communication attempt will first check if the receiver is indeed reachable in the receiving network domain. Then the SSC is forwarded to the scorecard verifier entity (SC-V). The main task of the SC-V is to validate the scores provided in the SSC.

The SC-V evaluates the scorecard, verifies the signature and timestamp applied to it and optionally also verifies the given claims. The result is again sent to the SC-P which can then decide to forward the call to the legitimate receiver or drop the communication. The decision can be based on different policies, e.g. allowing only communications where scorecards exhibit high scores. If the SC-P decides to allow communication, the connection can be established.

For the generation of scorecards, it must be possible to query a global database of reference scores for the different claims. The score represents the strength of the score in relation to other possible claims in the same category. For example if a user provides his full name and address to the operator and the operator verified this, e.g. by an out of the band process, this claim will get a higher score than a (disposable) email address, which itself might have a slightly higher score than a mere pseudonymous username. We will refer to this database as SC-DB. The SC-DB is queried by the SC-I when new scorecards have to be generated. The SC-I looks up the score for every claim and includes the value in the scorecard. If possible, the SC-I also verifies the claim, and if SC-I is successful in doing so, SC-I adds a statement on successful verification of the claim including a timestamp of occurred verification in the attribute field for the specific claim in the scorecard.

The information in the scorecard should be protected for integrity and for those claims which are privacy sensitive also for confidentiality using cryptographic means. The receiving party should not be able to see the privacy sensitive data, but it will be able to see the score, contributing to the overall score of the SSC. Advanced cryptographic methods, such as zero-knowledge proofs could be used to include such information in a privacy protecting manner.

C. Use of Assertion Providers

One variant is to use different assertion providers, especially if the SC-I cannot by itself verify all claims. The SC-I tries to verify all yet unverified claims, e.g. by using indicators to responsible verification information providers which are either included in the claims or can be retrieved from the SC-DB. Therefore the SC-I can query different assertion information providers. The referred information providers could for example be an AAA server for additional identity information, device integrity verification servers for device integrity checks, reputation systems, gathering user reputation and behavior history, etc.. These entities provide assertions on the presented claims and are therefore referred to as Assertion Providers (SC-AP). SC-APs can be situated outside of the domains and can be queried by the SC-Is. A sample of this concept, using distributed databases is shown in Figure 2.

The SC-I must at least include a notice in the attribute field of the claim, that it retrieved the necessary information from SC-AP, because it cannot be assumed that the receiving domain’s SC-V is able to verify this assertion from SC-AP.

While the general concept uses a central, global database, it could be possible to use different, domain specific SC-DBs for every category. This allows each domain to judge on the score differently and independently. For example one domain could give a higher score for two-factor authenticated identities than another domain. In this case, the scores will have to include an indicator to the SC-DB they have been derived from, allowing the receiving SC-V to apply weighting functions to the score.

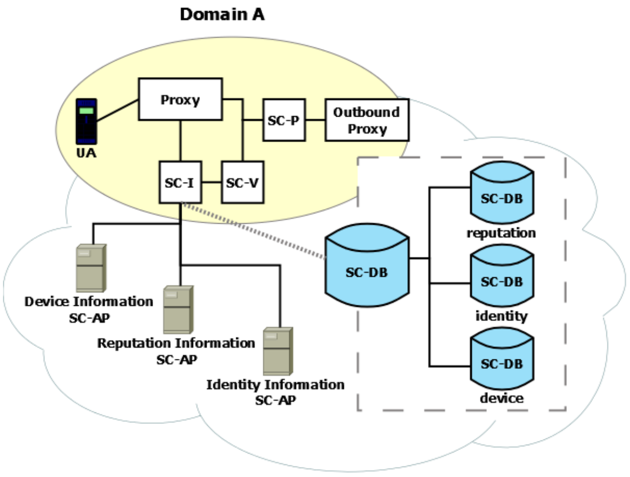

Fig. 2. Scorecard Architecture with Distributed Databases

III. Scorecard Processing

The verification of the scorecard takes place in the SC-V of the receiving network. Since different domains could use different types of claims, the claims are categorized and their score can be looked up by the receiving SC-V using different, independent, global SC-DB, allowing the SC-V to get the scores for individual claims based on the scores stored in the databases. The scorecard verifier SC-V is not necessarily involved in the verification of individual claims, such as the evaluation of device integrity measurements or authentication credentials. All claim validation related tasks are performed in the sending network by the respective SC-I upon creation of the scorecard. The SC-V is intended to check if the scorecard is valid, i.e. the SC-V first verifies the freshness using the timestamp and authenticity by verifying the signature. The SC-V further checks if the included claims are compliant to domain/user specific rules, e.g. users might set up rules indicating that they only want to receive messages from devices with an identification score above a treshold value. In addition to that, the SC-V could also be able to verify the trustworthiness of the issuing SC-I in the sender domain, e.g. based on technical means, such as platform integrity verification, or based on other available data such as existing business relationships with the operator of the sender domain or the reputation and behaviour of the sender domain.

The calculation of the final score could follow different rules and could even be domain-specific. The calculation method must be standardized and indicated on the scorecard. Different options include the use of the lowest score as the total score for a scorecard, category-based calculations, where a score is calculated for each category or a weighted calculation using different weights for claim types or categories.

The receiving network may also keep network scores for all sending networks. The network scores express the level of trustworthiness the receiver has in the sending domain's SC-I. The individual caller or calling device's scorecard from a sending network with an existing network score will be weighted by the network score. Every domain can have individual and non-uniform weighting mechanisms for all other networks. A new sending network, which is not known by the receiver, should start with a network score which is below the lowest network score known to the receiver. Network score can be increased by different mechanisms, such as reputation, agreements between domain operators or certifications of domains.

A. *Device Binding of Scorecards*

Instead of issuing a new scorecard for every communication attempt being made, the SC-I issues a scorecard which is re-usable. Such a scorecard requires additional protection in the sense that it cannot be used by another device, such that redistribution to another device is impossible or at least useless when the SSC cannot be used with another device. Furthermore, the scorecard should then include at least one timestamp to state freshness of the claims and their verification. One option would be to encrypt the scorecard (or parts of it) with a secret which is only known to the sending device.

The device should present reliable evidence of its capabilities that it can store the scorecard securely and that the key used for encryption and decryption is protected by the device. The use of existing and standardised security technologies and device profiles enables interoperability of heterogeneous networks, where multiple devices from different vendors with varying hardware (and software) capabilities interact.

The device can then decrypt the scorecard when initiating a communication session and present the scorecard to the receiving domain's SC-P. Such a scheme of re-usable scorecards reduces network traffic and computational efforts for the SC-I but increases the requirements on the device side.

B. *Re-use of Scorecards*

If the scorecard contains sufficiently strong, verified, identity information, and satisfies the conditions of device binding as detailed above, the scorecard provides high assurance about the identity and properties of the party initiating communication. It then has all the information of a credential as is commonly used in Identity Management (IdM) systems. In fact, the scorecard is enriched by other information which would be called claims in IdM. It may therefore be natural for the SC-Ps in sending and receiving network to consider and use such Id-enabled scorecards in lieu of access credentials.

A primary use case could be the re-use of scorecards toward various receiving networks. For this, one receiving network's SC-P could be singled out as an identity provider for card-bound identitites, for instance after first receipt and positive assessment of a particular scorecard. The SC-P would announce his identity provider (IdP) role for this particular card in a central directory so that other receiving networks called by that user could look up this directory. There, the SC-P of the currently called network could select one card IdP SC-P, for instance the one with freshest assessment information on the scorecard's claims (meaning that the directory entries bear time-stamps) to vouch for the identity and integrity of that caller and obtain an identity assertion. This would avoid locally verifying the claims of that scorecard. The resulting mechanism has some similarity to common IdM schemes such as OpenID, on the highest conceptual level. One precondition to that is that a sending network can keep a store of old, but re-usable scorecards.

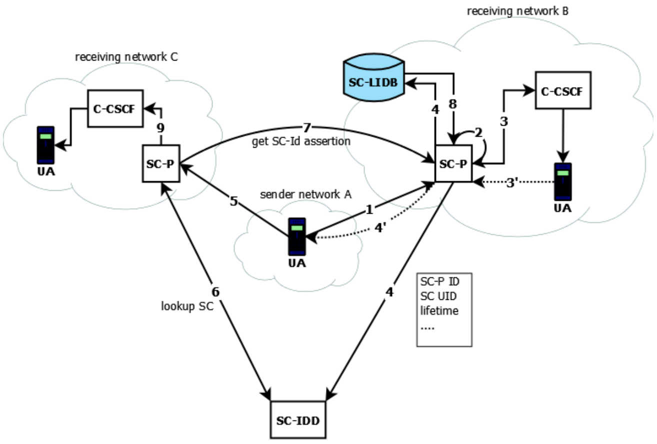

Fig. 3. Protocol Flow for Scorecard based Architecture

Figure 3 shows a possible call flow, highlighting the general functionality. Security elements may need to be added, in particular replay and integrity protection, where necessary. Table II details the protocol steps, where proxies and gateways are omitted for simplicity.

Depending on the availability of network elements, some additional steps may amend the call flow. In a modified step 3', the receiving UA notifies SC-P A that the call was not UC. SC-P A will then create the scorecard IdP binding. In step 4', SC-P B notifies SC-P of sender network A of the lifetime of the IdP commitment made, allowing the sender network to judge when to issue a new SSC or re-use the old one.

C. *Scorecard Categories*

In general it is useful to provide different categories for the claims in the scorecards. As stated in previous sections, there could be independent SC-DBs for every claim category. The contents of the SC-DBs and the categories must be standardized for interoperability between different domains. The scorecard concept can easily be extended to include additional categories or sub-categories to existing categories.

Identity Scoring includes all information on the sender identity. Several fields can be used in the ID category and as examples would include information on the identity authentication scheme (e.g. username/password, biometrics, two-factor authentication). It can also include information on the assurance level, e.g. that an identity can be resolved to a physical address. Additional inclusion of identity properties, like name, country, company, etc. could be desired for some cases, however, for privacy reasons this information should be protected, using well-known methods, such as zero-knowledge proofs to verify the claims. Some fields might include authentication credentials or references to them. One example could be the inclusion of a signed challenge, if public key crypto authentication is used. Technically, the use of extensible resource identifiers (XRI) allows to create a structured scheme with tags, which are interoperable across domains, and additionally could allow a persistent link to a possibly moving resource.

The inclusion of **Trusted Sender Identities** into the score-card approach is a natural extension to the identity information. 3GPP already identified strong authentication as one key element of PUCI in [1]. Hence, it makes sense to also include the strength of the authentication, as well as additional information on the authentication process in a scorecard. Such additional information covers aspects of the device and security features which are used in the authentication procedure. For example an UICC based authentication for mobile devices, performed by the network operator might have an increased level of trust over a SIP digest authentication using a username and password combination which is more prone to phishing and theft. Another authentication mechanism, discussed in 3GPP aims to provide interworking of the GBA protocol and the web-based OpenID protocol [16] to allow for a more secure authentication, which leverages the use of established, MNO based authentication to a general web-based authentication scheme, building on existing security in mobile devices.

Another flavour of trusted sender identities can be established when the UA uses HW-based security anchors allowing to assure UA integrity, such that the UA can be expected to behave in the expected manner and is for example not infected with malware, etc. Binding the identification to the assessment of the trustworthiness of the UA is then a key element in establishing trusted identities, relying on the strength of authentication and additional device integrity. By the inclusion of trusted sender identities in a scorecard, the card will have a higher score and additionally can include references to verifiable trustworthy information. This enables SC-V to perform an independent trust-assessment on specific claims.

TABLE II
TYPICAL CALL FLOW.

1) The UA in the sending network A calls the UA in the receiving network. A scorecard is sent to SC-P B.
2) SC-P B assesses the scorecard and upon positive result...
3) forwards the call to the target UA via the Call Session Control Function (CSCF).
4) SC-P B stores the scorecard and assessment result in a local scorecard Identity Database SC-LIDB. It also publishes its association as IdP to this particular SC in a public directory SC-IDD. The data sent to the SC-IDD contains (a) the ID of SC-P B, (b) unique ID of the scorecard, (c) a lifetime for this IdP association and (d) other data such as integrity/replay protection or metadata.
5) At another time, the same sender UA in network A wants to call a UA in another network C. It sends the same scorecard to SC-P C (without knowing the lifetime of that scorecard, the sending network may still follow a policy of re-use scorecard until failure and only generate a new scorecard when the receiving networks rejects the scorecard as being too old).
6) SC-P C looks for a SC-IdP association in SC-IDD.
7) SC-P C requests and obtains a scorecard identity assertion from SC-P B, for which...
8) SC-P B queries his SC-LIDB.
9) The call is forwarded to the target UA.

Device Scores are used to characterize devices, by different features such as vendor, device type, such as handset, laptop, software version, device certification, etc.

It is further possible to introduce **Reputation-Based Scoring** into the scorecard, which allows establishing a certain score based on a reputation or network of reputations, similar to social-networks or webs of trust. Additionally, the scorecard could also include information on the **behavior of the caller**. Such information cannot be retrieved by the SC-I prior to call initiation and can only be collected by user feedback mechanisms. Such data in the scorecard will always be based on historic averaged or long-term data, which must be kept by the SC-I or in a database to which the SC-I has access.

IV. Conclusion

In this paper a basic scheme and numerous variants on the use of sender scorecards was presented. Typical scorecard content, including critical user and device identification categories were also provided. In presenting the basic architecture for the scorecards, key infrastructure elements were introduced: 1) a scorecard issuer (SC-I) which provides a signature, timestamp and queries assertion information providers; 2) a scorecard proxy (SC-P) which verifies the presence of the receiving device in the receiving domain and makes the final decision on the call; and 3) scorecard verifier (SC-V) which verifies the signature and identity claims of the SSC.

The presented concept of SSC can be implemented in addition to the measures for PUCI described in [1]. If a user or domain operator defines target scores for individual claims or claim categories it is possible to implement an automatic score based access control. This could be used to populate blacklists, e.g. by automatically putting all communication attempts with low scores on a blacklist. Another option would be to solve the introduction problem of whitelists by defining minimal scores. If the minimal scores are reached, the communication can be established. In the case of a 'high-score but still UC' the user would then put the caller on the blacklist.

We show that the impact on communications overhead can be reduced by allowing the re-use of SSCs by binding SSCs to devices. While this requires the devices to provide a minimum set of security relevant features, such as cryptographic capabilities and secure storage, this allows us to reduce the traffic. The SSCs are created by the SC-I and then sent to the device, stored securely and cryptographically bound to the device identity such that they cannot be used with another device. This allows re-use of the SSCs without having to create a new SSC for every communication attempt.

An integration with the IMR approach is also possible, where the receiving network SC-P gathers different information on the communication itself (e.g. user feedback, statistical data, etc.) and generates an SSC in the receiving domain together with a sender fingerprint, e.g. based on system characteristics or network address. If communication without an associated SSC occurs, the SC-P can use these SSCs to associate them with the communication attempt. Depending on the level of integration, it could be possible to integrate SSCs on a lower level protocol, such that routers on the way from sender to receiver can evaluate the scores and possibly drop the communication even before it reaches the receiving domain in the case of UCI.

V. References

[1] 3GPP TR 33.937 v9.2.0 "Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)," available at http://3gpp.org/ftp/Specs./html-info/33937.htm. June 2010.

[2] H. Yany, K. Sripanidkulchaiz, H. Zhangy, Z. Shaez and D. Saha, "Incorporating Active Fingerprinting into SPIT Prevention Systems," in Proc. VSW'06. ACM, 2006 .

[3] M. Hansen, M. Hansen, J. Müller, T. Rohwer, C. Tolkmit and H. Waack, Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT, in Proc. 3rd Annual VoIP Security Workshop, Berlin, Germany. ACM, 2006.

[4] S. Dritsas, J. Mallios, M. Theoharidou, G. F. Marias, and D. Gritzalis, "Threat analysis of the session initiation protocol regarding spam," in Proc. IEEE Intl. Conf. Performance, Computing, and Communications Conference, 2007. IPCCC 2007., 2007, pp. 426 – 433.

[5] M. Stiemerling S. Niccolini, S. Tartarelli, "Requirements and methods for SPIT identification using feedbacks in SIP," Internet-Draft, 2007. [Online]. Available: http://tools.ietf.org/html/draft-niccolini-sipping-feedback-spit-03

[6] F. Wang, Y. Mo, B. Huang, "P2P-AVS: P2P Based Cooperative VoIP Spam Filtering," in Proc. IEEE WCNC 2007.

[7] C. Jennings, "Computational Puzzles for SPAM Reduction in SIP," Internet-Draft, 2008. [Online]. Available: http://tools.ietf.org/html/draft-jennings-sip-hashcash-06

[8] H. Tschofenig, E. Leppanen, S. Niccolini, M. Arumaithurai, "Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) based Robot Challenges for SIP," Internet-draft, 2008. [Online]. Available: http://tools.ietf.org/html/draft-tschofenig-sipping-captcha-01

[9] J. Rosenberg and C. Jennings, "The Session Initiation Protocol (SIP) and Spam," RFC 5039 (Informational), Internet Engineering Task Force, Jan. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5039.txt

[10] M. Nassar, R. State, O. Festor, Intrusion detection mechanisms for VoIP. In Third annual VoIP security workshop (VSW'06). [Online]. Available: http://arxiv.org/abs/cs.NI/0610109 applications, 2007.

[11] M. Nassar, S. Niccolini, R. State, and T. Ewald, "Holistic voip intrusion detection and prevention system," in IPTComm '07: Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications. New York, NY, USA: ACM, 2007, pp. 1–9.

[12] A. U. Schmidt, N. Kuntze, and R. E. Khayari, "Spam over internet telephony and how to deal with it," in Proceedings of the 7th annual Conference Information Security South Africa, H. S. Venter, J. H. P. Eloff, L. Labuschagne, and M. M. Eloff, Eds. Information Security South Africa (ISSA), 2008.

[13] A. U. Schmidt, N. Kuntze, and R. E. Khayari, "Evaluating measures and countermeasures for spam over internet telephony," in ISSE 2008 Securing Electronic Business Processes, N. Pohlmann, H. Reimer, and W. Schneider, Eds. Wiesbaden: Vieweg + Teubner, 2008, pp. 329–340.

[14] Robert S. Kaplan and David P. Norton, "The Balanced Scorecard - Measures that Drive Performance." Harvard Business Review, 1992, January-February, pp. 71-79.

[15] D. Wing, S. Niccolini, M. Stiemerling, H. Tschofenig, "Spam Score for SIP," Internet-Draft, 2008. [Online]. Available: http://tools.ietf.org/html/draft-wing-sipping-spam-score-02

[16] 3GPP TR 33.924 v9.2.0 "Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking," document is available at http://ftp.3gpp.org/specs/html-info/33924.htm. June 2010.