Have I Met You Before? Using Cross-Media Relations to Reduce SPIT

Kumiko Ono
Columbia University
New York, USA
kumiko@cs.columbia.edu

Henning Schulzrinne
Columbia University
New York, USA
hgs@cs.columbia.edu

ABSTRACT

Most legitimate calls are from persons or organizations with strong social ties such as friends. Some legitimate calls, however, are from those with weak social ties such as a restaurant the callee booked a table on-line. Since a callee's contact list usually contains only the addresses of persons or organizations with strong social ties, filtering out unsolicited calls using the contact list is prone to false positives. To reduce these false positives, we first analyzed call logs and identified that legitimate calls are initiated from persons or organizations with weak social ties through transactions over the web or email exchanges. This paper proposes two approaches to label incoming calls by using cross-media relations to the previous contact mechanisms which initiate the calls. One approach is that potential callers offer the callee their contact addresses which might be used in future correspondence. Another is that a callee provides potential callers with weakly-secret information that the callers should use in future correspondence in order to identify them as someone the callee has contacted before through other means. Depending on the previous contact mechanisms, the callers use either customized contact addresses or message identifiers. The latter approach enables a callee to label incoming calls even without caller identifiers. Reducing false positives during filtering using our proposed approaches will contribute to the reduction in SPIT (SPam over Internet Telephony).

Keywords

Unsolicited calls, SPIT prevention, Cross-media relations, Email, WWW, web, VoIP, SIP

1. INTRODUCTION

Unsolicited calls usually originate from unknown persons or organizations, whom the callee has not been informed of their contact addresses nor met before. Since an IP-based infrastructure is more vulnerable to unsolicited calls, as described in [1], people have recently been experiencing more SPIT calls. Most legitimate calls, by contrast, have caller identifiers (IDs) that the callee has seen before. Some legitimate calls, however, have unknown caller IDs. Examples of these legitimate calls include confirmations of reservations or deliveries, and recorded notifications of school closing on a snowy day. These legitimate calls are often labeled as unsolicited calls at a typical SPIT filtering system illustrated in Figure 1 since their caller IDs are not found on the callee's white list. This is called as the "introduction problem." Due to this introduction problem, some systems forward these calls to a voice mail box, rather than reject them.

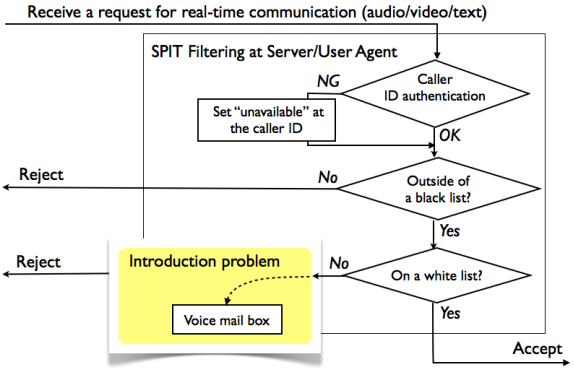

Figure 1: Existing SPIT Filter

Generally, the callee's white list or accept-list contains the same addresses with his contact list or address book, which is populated by contact addresses of people with strong ties in his social network [2] such as family members and friends. For business use, the accept-list usually links to a directory service located on an LDAP (Lightweight Directory Access Protocol) [3] server. For either use, however, the accept-list does not usually include the addresses of persons or organizations with weak ties [2] such as friends of a friend in an SNS (Social Network Service) over the web. On the other hand, a black list or reject-list contains the contact addresses of undesired callers or links to a reputation server that gathers IDs of well-known malicious callers.

Using a white list or a black list to label incoming calls requires caller ID authentication. For a VoIP (Voice over IP) call using the SIP (Session Initiation Protocol) [4], the SIP Identity header [5] enables a callee to authenticate the caller ID. However, some legitimate calls are sent with "unavailable" caller IDs, because the authentication of the caller IDs

fails, as illustrated in Figure 1. For example, most international calls or calls through a VoIP - PSTN (Public Switched Telephone Network) gateway have no authenticated caller ID. These anonymous calls limit the effectiveness of labeling incoming calls based on the caller ID.

In the next section, we analyze how legitimate calls from people with weak ties are initiated. We then propose two mechanisms to label incoming calls by using cross-media relations between calls and the previous contacts. Our first mechanism is that potential callers offer the callee their contact addresses which might be used in future correspondence. If the callee agrees, these contact addresses are added to his white list. We describe this mechanism further in Section 3.1. Our second mechanism is that a callee provides potential callers with weakly-secret information that the callers should use in future correspondence in order to identify them as someone the callee has contacted before through other means. Depending on the previous contact mechanisms, the callers use either customized contact addresses or message identifiers, as outlined in Section 3.2. Section 4 describes a use case integrated with an SNS, and Section 5 describes implementation details to achieve these mechanisms. Finally, Section 6 concludes the paper with the effects of our proposed mechanisms.

2. LEGITIMATE CALLS FROM WEAK TIES

Our quick survey gives a rough sense of how often people are experiencing unsolicited calls, how well-maintained contact lists are effective in labeling legitimate calls, and how legitimate calls from weak ties are initiated. In this survey, we gathered call records of 246 calls from eight cell phones and 136 calls from four landline phones from our colleagues at our lab. We also asked the participants about their relationship to legitimate callers whose IDs were not found on their contact lists.

First, Figure 2 indicates a significant difference in the proportions of unsolicited calls between cell and landline phones. Whereas only six percent of the incoming calls on cell phones are unsolicited calls, 52 percent of those on landline phones are unsolicited. We suspect that this difference is caused by the FTC (Federal Trade Commission) regulations that prohibit telemarketing calls to cell phones [6], as well as the higher usage cost on cell phones than on landline phones. Even though we can reduce unsolicited telemarketing calls using the national "Do Not Call Registry" service, the effect is unfortunately limited. The jurisdiction is only for domestic telemarketers, not for international ones nor for calls over IP infrastructure. Thus, we need a technical mechanism to help a callee decide whether to accept incoming calls.

Second, another difference in Figure 2 is found in the proportions of legitimate calls with known caller IDs. A larger proportion, 78 percent, of the calls to cell phones carries known caller IDs, which are found on the contact list, than 18 percent to landline phones. Since people usually maintain their contact lists on cell phones better than landlines, the result shows how well-maintained contact lists are useful to label incoming calls.

Third, Figure 2 also indicates that 17 or 29 percent of the incoming calls are legitimate, but with unknown or unavailable caller IDs. By asking the participants, we found that all these legitimate calls with unknown caller IDs were initiated from transactions over the web or email exchanges. For example, they are confirmation calls from the restaurants which the callee made on-line reservation, or notification calls of flight changes from the airline on which the callee booked flights. On the other hand, the legitimate calls with no caller IDs were international calls or calls through VoIP-PSTN gateways from people with strong ties. There were no unsolicited calls from legitimate callers whom the callee has had no prior contact with. Even if we had larger number of the data set, most legitimate calls from people with weak ties would still have the previous contacts with the callees. This suggests that we need a new mechanism to label incoming calls beyond using caller IDs, and the solution could be use a piece of information related to the previous contacts.

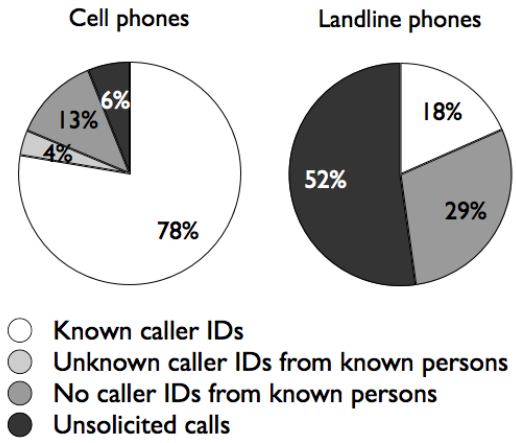

Figure 2: Incoming Calls: Cell Phones vs. Landline Phones

From these three indications, therefore, we set our goal to enhance a SPIT filtering system covering calls from people with weak ties. we approach it to use caller IDs and other information related to the previous contacts between the callee and the caller.

3. USING CROSS-MEDIA RELATIONS

Legitimate calls from persons or organizations with weak ties, as analyzed in Section 2, are usually initiated from the previous contacts between the callee and caller through transactions over the web or email exchanges. Focusing on these previous contacts, we propose that both parties exchange an additional information which should be used in future correspondence as an indication that the callee has contacted before. We call this piece of information a "cross-media relation." Our approach is to expand filter conditions for incoming calls by using the cross-media relations as illustrated in Figure 3, which is also applicable to other real-time communication requests. We distinguish two types of the cross-media relations: contact addresses offered by potential callers and weakly-secret information provided by a callee. The following outlines the mechanisms using each type of the cross-media relations and shows our proposed filtering system.

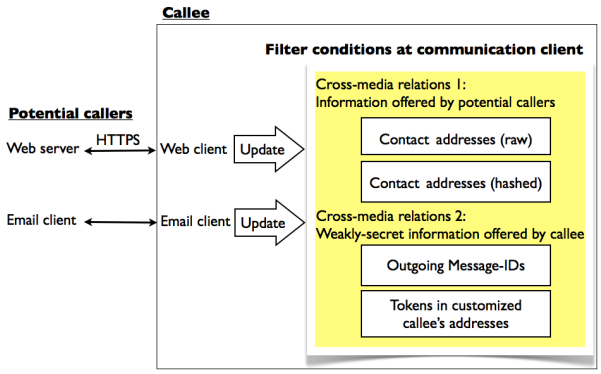

Figure 3: Overview of Proposed Mechanisms

3.1 Contact Addresses of Potential Callers

In general, the more contact addresses we can obtain from potential callers, the more incoming calls we can label, since a typical filter system uses the caller IDs as shown in Figure 1. Thus, persons or organizations that a callee contacts through the web transactions or emails offer their contact addresses which they might use in future correspondence with the callee.

Depending on the contact mechanism, callers use a different method to convey their contact addresses. In a web transaction, i.e., HTTP transaction shown in Figure 4, the contact address is conveyed in a new HTTP header, Correspondence-URIs [7] or an HTML META tag, HTTP-EQUIV [8] in the response from the potential caller, e.g., `book.airline.com`. In an email exchange shown in Figure 5, the contact address is contained in a vCard [9] attached to an email message sent from the potential caller. After the callee receives the contact addresses of potential callers, he adds them to his white list only if he agrees.

The format of the contact address is either raw or hashed. Hashed contact addresses are suitable if the potential caller prefers concealing his routable address for privacy or operating reasons. For example, in an SNS, when a subscriber prefers not publishing his routable contact address, he can instead publish his hashed contact address for the limited purpose of filtering calls.

The mechanism to use this type of cross-media relations is appropriate in a case where the previous contact was one-to-one correspondence between the callee and the potential caller There are, however, several cases where we cannot apply this mechanism. In these cases, the callee should deliver weakly-secret information to potential callers.

3.2 Weakly-Secret Information

We propose another type of the cross-media relations: weakly-secret information provided by a callee. Potential callers should use this information in future correspondence to be identified as someone with whom the callee has contacted before through other means. This mechanism is useful in the following cases. One is where the previous contact was one-to-many correspondence between the callee and the potential callers, such as joining an association, the callee is unwilling to receive many contact addresses of the potential

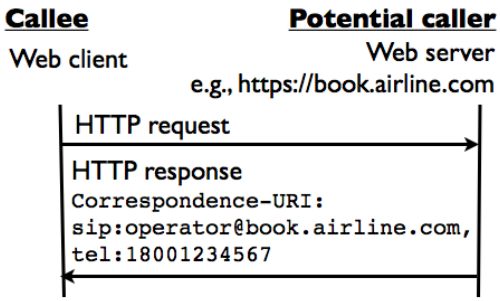

Figure 4: HTTP Message Exchanges where a Potential Caller Delivers His Contact Addresses

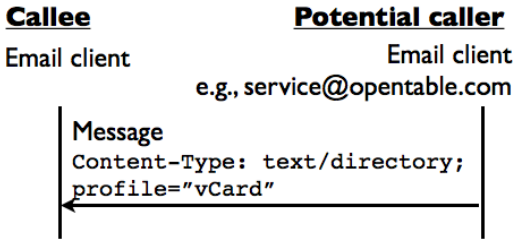

Figure 5: Email Message Exchanges where a Potential Caller Delivers His Contact Addresses

callers. Another case is where potential callers might use a different or no authenticated caller ID, due to the type of communication medium or service such as two stage dialing.

Depending on the communication medium of the previous contact, a callee provides potential callers with either customized contact address or message identifier. The customized contact address contains a random component or a token. This mechanism works when a callee fills out contact information on a web site, as shown in Figure 6, or in a vCard attached to an email message. The random component or token can be automatically generated in correspondence to the URL (Uniform Resource Locator) [10], or manually specified. In the examples in Figure 6, a token, `coms4001`, in SIP-URI is set between the user name and the domain name preceded with +, in the same way as the email addressing practice called as "sub-addressing" [11]. For TEL-URI [12], a token, `0012`, follows the E.164 number like an extension. To convey this information in a later call, the caller just needs to set the destination address to the customized contact address.

Specifically in email exchanges, as shown in Figure 7, a potential caller first sends a message asking a real-time communication to the callee. Only if the callee accepts the request, he will respond to it by email telling his contact address. As a result, the message identifier of the response email, which is set in the Message-ID [13] header, can be used as weakly-secret information to prove the acceptance from the callee. Thus, the message identifiers of outbound emails or SIP calls can be included by the potential caller in a later call, even if he uses a different caller ID or type of communication medium.

To convey the message identifier in a SIP call, the caller

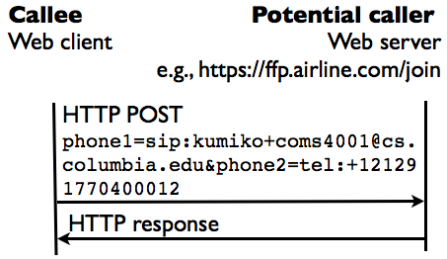

Figure 6: HTTP Message Exchanges where a Callee Delivers Weakly-Secret Information

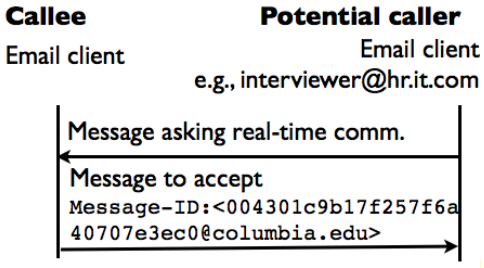

Figure 7: Email Message Exchanges where a Callee Delivers Weakly-Secret Information

should set its value of a SIP header extension, either Refer-To [14] or References [15]. Unfortunately, however, we need to modify the applicable SIP methods for the Refer-to header or define a new parameter of the References header. This is because the Refer-To header can contain any URI, but cannot appear except in a REFER method. On the other hand, although the References header can appear in an INVITE method, this header limits the parameter to call identifiers. Since the specification of the References header is still under discussion, we assume that the References header is used for this purpose.

For message exchange security, we should use an appropriate security mechanism for each communication protocol. That is, in web transactions, we use secure HTTP (HTTPS) [16] mechanism for message confidentiality, its integrity, and the authentication of the web server. For email security, we use TLS (Transport Layer Security) [17] for all the hops from a client to the other. We also leverage anti-spam email mechanisms when receiving emails.

3.3 Proposed Filtering Process

Figure 8 depicts a new filtering process for incoming calls, modifying and adding conditionals using the cross-media relations. If the caller ID of the incoming call is not found on a black list, then the process looks up on a white list. The white list contains contact addresses either in the raw or hashed format. In addition, especially for business use, the white list links to a remote server which securely maintains the list of contact addresses of all members in an organization and gives binary responses to query whether or not a contact address is found on the list.

If the caller ID of the incoming call is not found on the white list, the new filtering process tests on two new conditionals.

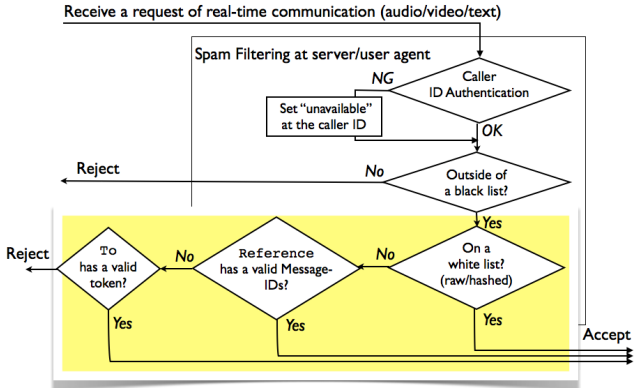

Figure 8: SPIT Filter Using Cross-Media Relations

The first one is whether it contains a valid Message-ID value in the References header. The second is whether it contains a valid token in the destination address, i.e., in the To header. The validity can be determined by looking up on the filter conditions of message identifiers and tokens. If the test succeeds on either conditional, the call request can be accepted.

4. A USE CASE: INTEGRATION WITH AN SNS

We describe how we can apply our proposed mechanisms in an SNS, since an SNS is the most popular and effective service for subscribers to maintain relationships with both strong and weak ties and to initiate real-time communications with each other. There are three typical services in an SNS: the subscription, the invitation of new friends to expand their own social network, the notification of the state updates of their friends, and email exchanges among them. The following describes how subscribers can extract cross-media relations in each service.

A newcomer starts to subscribe to an SNS through a transaction over the web although the invitation to the subscription may be sent by email. In this web transaction, the newcomer fills in a sign-up form including his name and contact addresses by email and/or phone. By submitting the sign-up form, he can send a token in his customized phone contact address. Then, he can save the token corresponding to the URL of the web site as a filter condition. When he receives an incoming communication request destined for his contact address with the token, he can identify the caller as one of the subscribers in the SNS and decide whether to accept the request.

Next, a subscriber can expand his social network in the SNS by inviting his friends to add to his network or being invited by his friends to be added in her network. Such an invitation is generally delivered by email asking the invitee to respond at the SNS web site. If the invitee accepts the invitation, he can receive his friend contact address in the HTTP response. The format of the contact address, in raw or hashed, depends on the preference of the owner of the contact address. By adding the contact address to his white list, the invitee can prepare to label calls or text messages from the friend.

When notifying the status updates of a subscriber's social

network, the notification message can contain the list of hashed contact addresses of the friends of his friend. Generally, users prefer concealing their own contact addresses from friends in the second degree. Thus, the hashed format of their contact addresses, rather than the raw format, is appropriate.

Among the members in his social network, a subscriber often exchanges emails through the SNS server. When he wants to talk with a girl of his friend, but does not know her contact address, he needs to send an email asking her contact address for a real-time communication. If he can receive an email response telling the acceptance and her contact address, he can send a call request with the Message-ID of the email response. Therefore, she can identify him as a person corresponding to the previous email. Reversely, if he is asked and accepts her request, he needs to save the Message-ID of the email response in order to label a later call from her.

Thus, in these services in an SNS, a subscriber can extract cross-media relations, prepare to label incoming calls or other real-time communication requests, and identify the caller or requester as a specific subscriber or one of the subscribers.

5. IMPLEMENTATION DETAILS

We assume that our proposal has minimal impacts on a SIP proxy server. The following are required implementation for a SIP proxy server, a caller and a callee. For each end, we describe what kind of functions our proposed mechanisms require to implement in a SIP User Agent (UA), a web browser, and an email client.

5.1 Implementation for a SIP Proxy Server

A SIP proxy server needs to forward the SIP References header. Specifically, an inbound SIP proxy server needs to allow the sub-addressing in the destination address in the To header and Request-URI. When the server determines the destination user name, the server just needs to ignore the string after the plus separator.

5.2 Implementation for a Callee

A SIP UAS (User Agent Server) working with a filtering system for incoming requests needs to add filter conditions depending on the values of three SIP headers: From, To, and References. The filter conditions consist of the originator address in the addr-spec parameter of the From header, the destination address in the addr-spec parameter in the To headers, and the referred message identifier in the refer parameter of the References header. With regard to originator addresses, the stored conditions are in either raw or hashed format. The hash algorithm for each address is also stored as part of the filter conditions. These filter conditions are to be stored as a user configuration at a local terminal or a remote server such as a SIP inbound proxy server. Specifically for originator addresses belonging to an organization, the filtering system links to a directory service using LDAP. Therefore, the filtering system can decide whether to accept incoming requests based on these filter conditions. If accepted, the SIP UAS should inform the user of the matched information in order to ask the user's final decision whether to accept it.

In a web browser, a plug-in program should support following functions: generating and storing a token when a user is filling in a sign-up form, and extracting and storing contact addresses in the HTTP response over TLS. After generating a token, if the user agrees, the plug-in program stores the token corresponding to the timestamp of the generation and the URL to which the sign-up form sent in an HTTP request. After extracting contact addresses in the HTTP response over TLS, if the user agrees, the plug-in program adds their contact addresses to his white list. Each contact address should also be stored with the hash algorithm if the address is in the hashed format, the timestamp of the response received, and the URL from which the response came.

Regarding to an email client, an IMAP (Internet Message Access Protocol) [18] client should be dedicated to our proposed mechanisms. This is because the required functions are executable without any user interaction, as long as the client can fetch saved outgoing and incoming legitimate emails. This IMAP client should support following functions: extracting and storing contact addresses in a vCard from incoming email messages and extracting and storing the message identifiers in the Message-ID headers from outgoing emails. These two extracting functions run periodically, but the extracted information does not always need to synchronize with saved outgoing emails. After a user deleted an outgoing email, the corresponding message identifier may remain for be looked up by a filtering system for a certain period of time. The message identifier should be stored as the filter conditions, corresponding with the timestamp of the email sent and the destination address in the To header.

5.3 Implementation for a Caller

A SIP UAC (User Agent Client) should support the References header extension to convey the referred message identifier in an outgoing request. To set the message identifier, a caller can manually copy from the Message-ID header at any email client and paste it at a SIP UAC.

A web server should respond to an accepted sign-up form with the contact address which will be used in future correspondence. The contact address should be set in an HTTP header extension or HTML META tag.

On the other hand, an email client does not need any additional functions for a caller since attaching vCards has been widely deployed.

6. CONCLUSIONS

To label incoming calls, we proposed to use cross-media relations between the calls and previous contacts through transactions over the web or through email exchanges. These cross-media relations are expressed in two types of information. First, relations can be as potential callers' contact addresses in either raw or hashed format, and second, they can be expressed as weakly-secret information in the callee's customized contact address or the message identifier of the callee's outgoing email. By enhancing existing filter conditions, our proposed mechanisms enable a callee to label incoming requests, not only from persons or organizations with weak ties, but also from those with different or no caller IDs. As a result, we expect to avoid most of the false pos-

itives that occur during filtering, quantities in our survey representing 17 percent of the incoming calls for cell phones and 29 percent of the incoming calls for landlines.

In addition to the effect of reducing false positives, we expect to observe two secondary effects from the enhancing filtering. One of these secondary effects is the ability to trace after delivery the customized contact address including the weakly-secret information. The weakly-secret information will identify the person who sold the contact address when the caller sells the contact address of a callee to a third party.

Another secondary effect of our proposed filtering system is increased security as a result of maintaining hashed contact addresses as a filter condition, rather than gathering contact addresses in a raw format. By collecting hashed data, our system protects against viruses which spread using gathered routable addresses as target addresses.

The work described in this paper is the first step in ongoing efforts to integrate anti-SPIT calls work with anti-spam email one. We are currently working on implementing our proposed mechanisms to examine their effectiveness and usability for filtering incoming calls.

7. REFERENCES

[1] J. Rosenberg and C. Jennings. The Session Initiation Protocol (SIP) and Spam. RFC 5039, IETF, January 2008.

[2] M.S. Granovetter. The Strength of Weak Ties. *Amer. J. of Sociology*, 78:1360–80, May 1973.

[3] J. Sermersheim. Lightweight Directory Access Protocol (LDAP): The Protocol. RFC 4511, IETF, June 2006.

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261, IETF, June 2002.

[5] J. Peterson and C. Jennings. Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). RFC 4474, IETF, August 2006.

[6] Federal Trade Commission. National Do-Not-Call Registry. C.R.F. Part 310, Telemarketing Sales Rule, June 2003.

[7] R. Shacham and H. Schulzrinne. HTTP Header for Future Correspondence Addresses. Internet-draft, IETF, May 2007. `http://tools.ietf.org/html/draft-shacham-http-corr-uris-00.txt`.

[8] D. Raggett, A.L. Hors, and I. Jacobs. HTML 4.01 Specification. Technical report, W3C, December 1999.

[9] F. Dawson and T. Howes. vCard MIME Directory Profile. RFC 2426, IETF, September 1998.

[10] T. Berners-Lee, R. Fielding, and L. Masinter. Uniform Resource Identifier (URI): Generic Syntax. RFC 3986, IETF, January 2005.

[11] K. Murchison. Sieve Email Filtering: Subaddress Extension. RFC 5233, IETF, January 2008.

[12] H. Schulzrinne. The tel URI for Telephone Numbers. RFC 3966, IETF, December 2004.

[13] P. Resnick. Internet Message Format. RFC 5322, IETF, October 2008.

[14] R. Sparks. The Session Initiation Protocol (SIP) Refer Method. RFC 3515, IETF, April 2003.

[15] D. Worley. The References Header for the SIP. Internet-draft, IETF, February 2009. `http://www.ietf.org/internet-drafts/draft-worley-references-02.txt`.

[16] E. Rescorla. HTTP Over TLS. RFC 2818, IETF, May 2000.

[17] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, IETF, August 2008.

[18] M. Crispin. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. RFC 3501, IETF, March 2003.