A Trust-based Strategy for Addressing Residual Attacks in the RELOAD Architecture

Oussema Dabbebi, Badonnel Rémi, Festor Olivier

A Trust-based Strategy for Addressing Residual Attacks in the RELOAD Architecture

O. Dabbebi, R. Badonnel, O. Festor
LORIA - INRIA Nancy Grand Est
Campus Scientifique - BP 239
54506 Vandœuvre-lès-Nancy, France
{dabbebi, badonnel, festor}@loria.fr

***Abstract*—Telephony over IP has undergone a large-scale deployment thanks to the development of high-speed broadband access and the standardization of signalling protocols. A particular attention is currently given to P2PSIP networks which are exposed to many security threats. The RELOAD protocol defines a peer-to-peer signalling overlay designed to support these networks. It introduces a security framework based on certification mechanisms, but P2PSIP networks are still exposed to residual attacks, such as refusals of service. We propose in this work to address these residual attacks by integrating into the RELOAD architecture a dedicated trust model coupled with prevention countermeasures. We mathematically defines this trust-based strategy, and describe the considered prevention mechanisms implemented by safeguards and watchmen. We quantify the benefits and limits of our solution through an extensive set of experiments.**

I. Introduction

The emergence of Voice over IP (VoIP) as a service for transmitting voice communications over the Internet has led to the standardization of dedicated signalling protocols [1]. The Session Initiation Protocol (SIP) has become the de-facto standard for establishing and managing VoIP call sessions based on simple text format messages. It uses many header fields similar to HTTP requests and responses, and targets a large scope of applications, including also streaming multimedia distribution, instant messaging and presence information services. Many efforts are currently spent for extending this standard to peer-to-peer networks in order to take advantage of their scalability and robustness properties. The objective is to define an open P2PSIP protocol [2], [3] where the registration and location servers are implemented by a distributed hash table (DHT) which stores the bindings between the address-of-record SIP-URI[1] and the contact SIP-URI. However this design increases the exposure of VoIP networks to new security threats inherited from the peer-to-peer area.

The security of P2PSIP networks is a key challenge. The RELOAD[2] protocol has been introduced as a peer-to-peer signalling overlay to support these networks in a secure manner [4]. This protocol integrates a security framework based on a central certificate enrolment server. Self-signed certificates can also be used in closed networks. The enrolment server affects to each node a Node-ID and public key certificates that are used to sign RELOAD messages as well as RELOAD data stored in the distributed hash table. The connections amongst nodes are also secured using an encryption protocol such as TLS. While this security framework mainly based on certificates permits to reduce the exposure to threats, P2PSIP networks are still exposed to residual attacks related to the routing and storage activities, as highlighted in [4]. For instance, it is trivial for a malicious node to refuse to give the stored information, or to send false routing messages.

We propose in this paper to address these residual attacks through the integration of a trust model coupled with dedicated counter-measures in the RELOAD architecture. The purpose is to complete its security framework in order to minimize the attack surface in P2PSIP networks. Our approach defines a trust-based prevention strategy for the RELOAD architecture; it integrates a distributed trust algorithm and specifies two prevention mechanisms. These ones are activated when a P2PSIP node is considered as untrusted by the other network nodes, or also at the voluntary request of a vulnerable node. The main contributions of this paper are centred on: (a) the integration of an eigentrust-based model into the RELOAD architecture in order to assess the trust level of P2PSIP nodes, (b) the coupling of this model with security mechanisms based on safeguards and watchmen in order to prevent P2PSIP residual attacks, and (c) the performance evaluation of this solution in order to quantify the benefits for RELOAD.

The paper is consequently organized as follows. Section II gives an overview of existing work related to the security of P2PSIP networks. Section III describes our trust-based strategy for RELOAD based on the concept of safeguards and watchmen. Section IV describes the considered trust modelling, while Section V details the coupling with countermeasure mechanisms. Section VI discusses a set of experimental results for evaluating our solution. Finally, Section VII concludes the paper and points out future research efforts.

II. Related Work

Due to their open and distributed nature, P2PSIP networks are particularly exposed to security attacks. These latter include (1) attacks targeting the signalling protocols, such as SIP caller ID spoofing, call hijacking, and spam over IP telephony,

[1]Uniform Resource Identifier
[2]REsource LOcation And Discovery

(2) attacks targeting the media transport protocols, such as audio stream eavesdropping, and (3) attacks targeting the peer-to-peer overlay network, such as sybil attacks, routing attacks and eclipse attacks [5], [6]. A large variety of techniques, addressing different network and security requirements, has already been proposed for countering them [7].

Significant efforts have been spent for securing the VoIP layer. For instance, VoIP SEAL [8] implements a two-stage detection mechanism for preventing unwanted communications: the first stage contains different modules which analyse the VoIP call by looking at the information which is available before actually answering the call. The second stage consists of modules which actually interacts with the caller or the callee to refine the detection results. A risk management strategy is defined in [9] for assessing the risk level, and dynamically adapting the exposure of the VoIP infrastructure through the activation or deactivation of dedicated security countermeasures. In the same way, a game theoretical model is introduced in [10] for deriving optimal defensive strategies based on throttling and replication mechanisms specifically designed for P2PSIP networks. A survey of protection techniques is also given in [11] arguing in favour of using and combining complementary techniques, which is fully in line with our integrated solution.

Other approaches are focused on the security of the peer-to-peer overlay of P2PSIP networks. For instance in [12], the authors detect and prevent identity assignment attacks in the DHTs based on packet tracking, IP address restriction and identity verification techniques. A method for securing the routing process is discussed in [13]. The authors propose to counter bad table routing entries by imposing specific constraints with respect to the nodes which can fill each slot of the routing table. In order to ensure that a given key is delivered to the proper node, they also propose to secure the message forwarding process by detecting faulty paths and applying redundancy techniques based on multiple routes. As previously mentionned, a security framework based on certification techniques is defined by the RELOAD protocol. An enrolment server permits to affect identities and certificates to nodes, and encryption protocols permit to secure the connections amongst these nodes.

While the RELOAD security framework constitutes a sound basis for reducing the attack surface of P2PSIP networks, trust and reputation techniques are needed for addressing the residual attacks that certification cannot cover, such as refusals of service. These techniques have already shown their benefits in VoIP networks [14]. For instance in [15], the authors suggest filtering audio spam, by applying trust paths familiar from the PGP web of trust. A subjective based trust model is also introduced in [16] in order to prevent routing attacks by simply avoiding malicious nodes. The integration of trust mechanisms into RELOAD constitutes therefore a key requirement for completing its security framework and addressing residual attacks based on dedicated countermeasures.

III. A Trust-based Strategy for the RELOAD Architecture using Watchmen and Safeguards

We propose in this paper a trust-based strategy for the RELOAD protocol coupled with dedicated security countermeasures. The objective is to provide a complementary solution to the certification mechanisms in order to detect and also to treat residual attacks. These attacks include in particular the refusals of service that can be observed during the storage process when an attacker refuses to register or to provide a P2PSIP entry, and also the refusals of service that can be observed during the routing process when an attacker voluntarily drop P2PSIP messages or provide incorrect routing messages [4]. While the certification permits to sign and control the operations that are done by nodes in the P2PSIP networks, it does not permit to assess their behaviour and to execute corrective treatments.

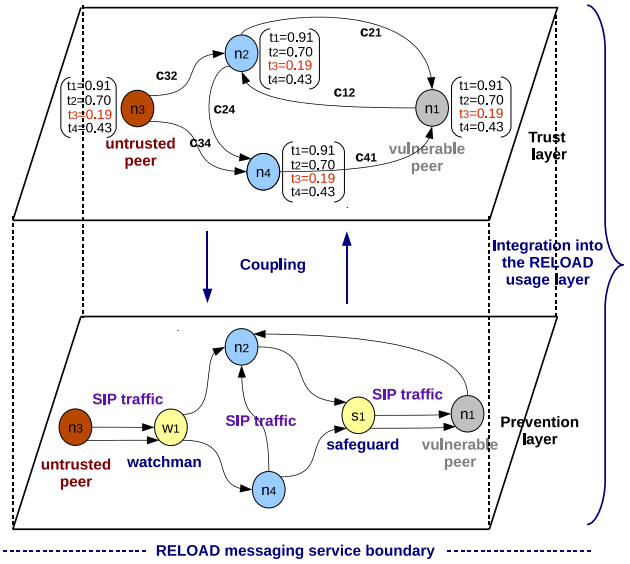


Fig. 1. Overview of our trust-based prevention strategy for RELOAD

As depicted in Figure 1, our approach consists in introducing in RELOAD a mathematical support for quantifying the trust level of P2PSIP nodes, and coupling this modelling with prevention mechanisms. Our trust mathematical model relies on the distributed eigentrust algorithm, whose benefits have already been demonstrated in peer-to-peer applications. It is implemented in the usage layer defined in the RELOAD architecture. When this algorithm is executed, each P2PSIP node locally assigns a local trust score to the P2PSIP nodes with which it interacts in the network. The local scores are then aggregated by the eigentrust algorithm in order to converge by transitivity to a global trust score t_i for each P2PSIP node n_i (represented as a vector of trust scores in Figure 1). All the nodes in the P2PSIP network participate in computing these scores in a distributed and node-symmetric manner. These values are then exploited by the RELOAD architecture in order to determine if prevention mechanisms have to be executed when P2PSIP nodes want to interact with others.

Several prevention strategies can be envisioned based on this model, by interacting with the routing, forwarding and storage components defined in the RELOAD architecture. The most natural approach corresponds to the avoidance strategy for reducing the impact of untrusted P2PSIP nodes in the network. In that case, the architecture minimizes the interactions with P2PSIP nodes scored with a low trust value. For instance during the routing process, P2PSIP messages can be voluntarily forwarded only to nodes scored with high trust values. The RELOAD architecture allows us to implement more elaborated strategies. In particular, we consider a prevention scheme which integrates the concept of safeguard and watchman logical components. The safeguard logical component (depicted on the prevention layer in Figure 1) is requested on a voluntary basis by a P2PSIP node when it considers his local trust level is low. The objective is to secure a vulnerable P2PSIP node by introducing a front node implementing complementary security mechanisms. This technique is typically used by a node which is vulnerable to malformed messages or to denial of service attacks. In that case, the safeguard plays the role of an intermediate node implementing applicative firewall rules (inbound P2PSIP traffic). The watchman logical component (also described on the prevention layer of Figure 1) complements the safeguard component. It is activated when a P2PSIP node is evaluated as untrusted by the other nodes. In that case, the watchman is responsible for regulating the outbound P2PSIP traffic of the untrusted node. These two components can be implemented as specialized P2PSIP proxy servers, regrouped into pools of servers in the RELOAD architecture.

IV. Eigentrust-based Modelling

Our prevention strategy is supported by an eigentrust-based modelling for assessing the trust and reputation of P2PSIP nodes. In order to integrate this algorithmic basis into the RELOAD architecture, we have considered three main trust criteria. These ones directly relate to the main operations that a P2PSIP node can perform in the network.

A. Considered RELOAD trust criteria

The first and most natural criterion, called P2PSIP routing trust, permits to quantify the capability of a P2PSIP node to properly route messages in the RELOAD architecture. While the certification mechanism defined in RELOAD permits to prevent that a compromised P2PSIP node tamper a routing message, this compromised node can drop routing messages or send itself unproper ones. The assessment of this criterion can be performed over the RELOAD routing component. It can be done by P2PSIP nodes along the routing path in case of recursive routing, or directly by the initiator P2PSIP node in case of iterative routing. Let consider the case of a node establishing a P2PSIP session with another node using an iterative routing. In that case, the initiator node is in direct contact with the intermediate nodes that are involved in the routing process, and can easily track P2PSIP nodes which drop routing messages or send inconsistent ones. In accordance with the eigentrust algorithm, we introduce two variables $sat^r(i,j)$ and $unsat^r(i,j)$. From the perspective of node n_i, these variables represent respectively the number of satisfactory and unsatisfactory actions performed by a node n_j with respect to the routing activity. Each time the node n_i observes that the intermediate node n_j drops a message or generates an inconsistent one, it increments the $unsat^r(i,j)$ variable, otherwise it increments the $sat^r(i,j)$ variable. The level of satisfaction noted s^r_{ij} with respect to the routing activity is then derived from these two variables, as defined by Equation 1. In the same way, two other variables s^s_{ij} and s^c_{ij} will be introduced to quantify the level of satisfaction for the two other considered criteria.

$$s^r_{ij} = sat^r(i,j) - unsat^r(i,j) \tag{1}$$

The second trust criterion, called P2PSIP resolution trust, aims at quantifying the capability of a P2PSIP node to properly store and provide P2PSIP entries. These entries correspond to the binding between the public address (address-of-record SIP-URI) of a P2PSIP node and its location (typically given as a contact SIP-URI containing an IP address and a port number). This resolution is required to join a destination node from its public address (e.g. sip:alice@example.com). The RELOAD certification mechanisms permit to control that the binding has been written by the proper node and has not been modified by an intermediate. However, they cannot guarantee that a storing node maintaining the RELOAD hash table will not refuse to cooperate and to provide this binding. We therefore introduce into our trust modelling two variables $sat^s(i,j)$ and $unsat^s(i,j)$ in order to quantify respectively the number of requests that are satisfied or not by the P2PSIP nodes responsible for storing the corresponding bindings. As previously defined with the routing trust criterion, the satisfaction level s^s_{ij} is derived from the $unsat^s(i,j)$ and $sat^s(i,j)$ variables.

The last trust criterion, called P2PSIP call trust, permits to evaluate the behaviour of P2PSIP nodes as callers. The objective is to prevent unwanted communications that might be initiated by them. After having resolved the SIP-URI, a call session is established between the caller and the callee. While the certification permits to authenticate the caller, it does not guarantee that this P2PSIP node (or a set of P2PSIP nodes) will not generate unwanted call sessions such as automatic or human commercial calls. We integrate into our trust modelling a level of satisfaction, with respect to this criterion, noted s^c_{ij} and calculated from $unsat^c(i,j)$ and $sat^c(i,j)$ variables. We can notice that the levels of satisfaction defined for our three trust criteria are not necessarily correlated. For instance, a P2PSIP node can show a high level of satisfaction with respect to the routing activity, and a low level of satisfaction with respect to its calls.

B. Aggregation into global trust values

These levels of satisfaction $s^r_{ij}, s^s_{ij}, s^c_{ij}$ correspond to local trust values which are then normalized by the eigentrust algorithm into $c^r_{ij}, c^s_{ij}, c^c_{ij}$. For instance, c^r_{ij} is given by the ratio between $max(s^r_{ij}, 0)$ and $\sum_j max(s^r_{ij}, 0)$. The same operation

is performed for calculating c_{ij}^s and c_{ij}^c from respectively s_{ij}^s and s_{ij}^c values. The transitivity property described by Equation 2 is then exploited by the eigentrust algorithm. This equation shows how the global trust value t_{ij}^r of a P2PSIP node n_i with respect to the routing activity of another P2PSIP node n_j can relate to the opinions of the P2PIP node n_i's friends.

$$t_{ij}^r = \sum_m c_{im}^r . c_{mj}^r \ with \ \sum_m t_{im}^r = 1 \qquad (2)$$

This transitivity relationship is the basis of the eigentrust algorithm and is used to quantify the global trust value t_i for each node n_i at the network scale, as formalized in [17]. In our case, the algorithm permits to derive three global trust values for each P2PSIP node n_i, noted t_i^r, t_i^s and t_i^c, corresponding to the considered trust criteria. The aggregation of local trust values into global trust values can be performed in a centralized manner or in a distributed manner. Both of these solutions can be envisioned in the context of the RELOAD architecture. We argue in favour of the distributed and secure version of the eigentrust algorithm which is consistent with the scalable and distributed nature of peer-to-peer networks, and whose fast convergence properties have already been analysed [17]. As previously mentioned, we consider that the global trust values t_i^r, t_i^s and t_i^c are not necessarily correlated. We do not try to aggregate them, but they can be represented as a tuplet (t_i^r, t_i^s, t_i^c). These global trust values are then exploited by our prevention layer integrated into the RELOAD architecture, in order to protect the P2PSIP infrastructure.

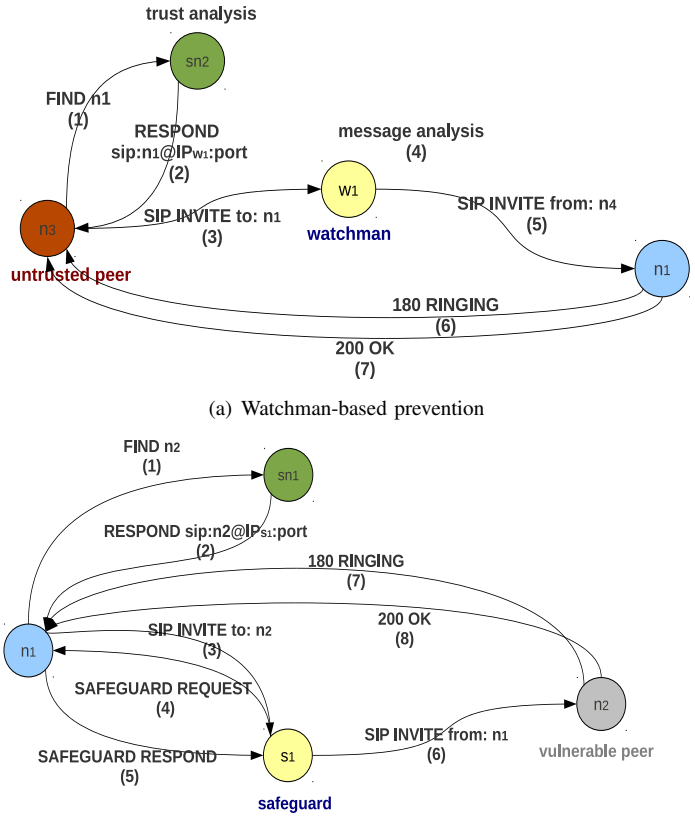
V. RELOAD Prevention Mechanisms

Based on this modelling, we define two prevention mechanisms for addressing the residual attacks of the RELOAD architecture. These mechanisms are represented by a prevention layer coupled with the trust layer, as overviewed in Figure 1. They are integrated into the usage layer of RELOAD, and permit to reduce the probability of an attack when P2PSIP nodes are detected as untrusted. These mechanisms, described in Figure 2, complement the avoidance strategy, which consists in avoiding or refusing the interactions with untrusted nodes in the P2PSIP network.

A. Watchman-based prevention

The first prevention mechanism, based on the concept of watchman, permits to control the interactions of an untrusted node in the P2PSIP network. When the trust layer detects a P2PSIP node with a critical global trust value, the RELOAD architecture does not reject this node, but rather activates a watchman responsible for monitoring the outgoing P2PSIP traffic and countering unproper messages if necessary. For instance, if the trust value t_i^c of a P2PSIP node n_i is low, the watchman permits to analyse the distribution of call sessions initiated by this node in order to detect SPIT[3] and DoS attacks. Consequently, it can delay or even reject unproper messages in order to prevent them. The watchman is a logical

[3]SPam over Internet Telephony



(a) Watchman-based prevention

(b) Safeguard-based prevention

Fig. 2. Prevention mechanisms for the RELOAD architecture

component of the prevention layer. It can be implemented as a dedicated proxy server with security features; these proxies being regrouped into a pool of servers. The P2PSIP network requests the untrusted node to pass through this watchman in order to interact with the other nodes, as long as its trust value stays low. The eigentrust algorithm updates this trust value over time based on the experience of the other nodes. The watchman participates also to this update and may voluntarily degrade or increase this trust value based on its analysis results. Figure 2(a) illustrates the operating of the watchman component. The P2PSIP node n_3 corresponds to a node detected as untrusted by the eigentrust algorithm, with a low t_3^c trust value. As a consequence, the P2PSIP network requests the node n_3 to communicate through the watchman proxy server noted w_1. When the P2PSIP node n_3 wants to establish a call session with another node n_1, it contacts its super-node noted sn_2 in order to obtain the location of the node n_3 (contact SIP-URI) using a FIND message (step 1). The super-node sn_2 knows the global trust values of n_3 from the trust layer, and redirects n_3 to the watchman w_1 (steps 2 and 3). This latter analyses the message of node n_3 (step 4). It then determines if the node n_3 is authorized or not to pursue the establishment of the call session. This authorization depends on the analysis results performed by the watchman w_1. This latter can delay or reject the session if the distribution

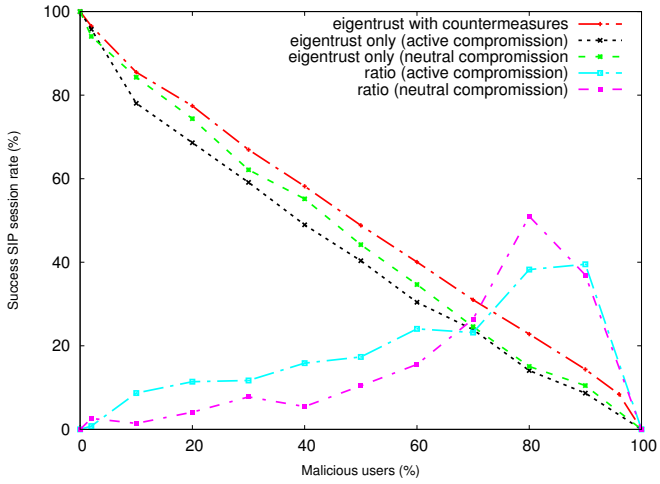


Fig. 3. Evaluation of the success rate of P2PSIP sessions

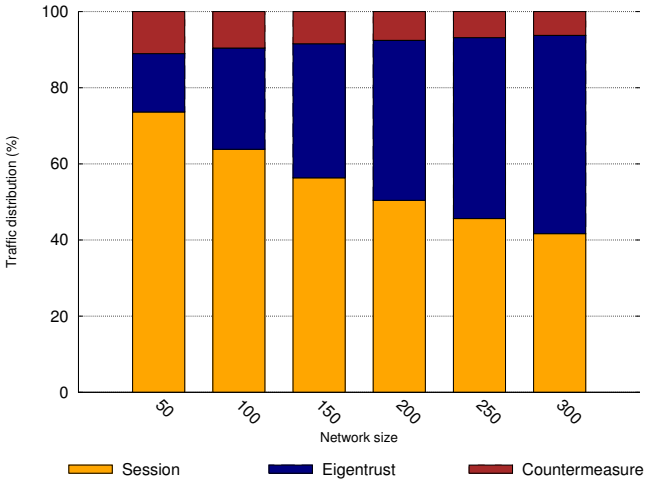


Fig. 4. Evaluation of the message overhead

of calls initiated by node n_3 reveals a potential attack (i.e. high call rate). The nature of the treatments executed by the watchman may vary depending on the criticality of the untrusted node (i.e. if a new degradation of the trust value is observed). In the scenario depicted in Figure 2(a), the authorization is given to node n_1 to establish the call session with node n_3 (steps 5 to 7). This strategy permits to minimize the probability of attacks generated by the untrusted node, while maintaining this node in the network.

B. Safeguard-based prevention

We introduce also a second prevention mechanism based on the concept of safeguards. The objective of a safeguard is to protect vulnerable nodes in the RELOAD architecture. The safeguard logical component, part of the prevention layer, is activated on the request of a vulnerable node, i.e. a node which estimates itself as untrusted. It permits to control its ingoing traffic in order to prevent attacks. It is implemented as a proxy server which is capable of complementing the vulnerable node with security features. A typical scenario is the case of a P2PSIP node sensitive to a malformed message due to an implementation vulnerability. If this vulnerability cannot be solved by upgrading this node, a safeguard can be requested by the node in order to support its security. The choice of requesting or not a safeguard is done in a voluntary manner by the node. The safeguard can then filter and prevent malformed message attacks through the implementation of applicative firewall rules. The nature of this filtering may vary depending on the observed trust values of the source nodes. Another scenario is the case of a P2PSIP node targeted by distributed denial of service attacks. The node can request a safeguard implementing dedicated security features (such as audio CAPTCHA test techniques) in order to minimize its exposure. The safeguards are regrouped into a pool of servers in the RELOAD architecture. From a technical point of view, the vulnerable node modifies and updates its P2PSIP entry with the contact URI of the considered safeguard, so that its public address is associated to this safeguard. These operations are done with the signature of the node, using the certification mechanisms of RELOAD. Figure 2(b) illustrates the operating of the safeguard mechanism. The vulnerable node n_2 is protected by the safeguard s_1 in order to prevent distributed denial of service attacks. The P2PSIP entry of n_2 binds the address-of-record SIP-URI of this node with the contact SIP-URI of the safeguard s_1 (e.g. $sip{:}n2@example.com$ associated with the IP address ip_{s_1}). Let consider that the P2PSIP node n_1 wants to establish a session with the node n_2. It requests its super-node sn_1 in order to obtain the contact SIP-URI of n_2 (step 1). The super-node provides the contact SIP-URI associated to $n2$, which in fact corresponds to the IP address of the safeguard s_1. The node n_1 then contacts the safeguard s_1. This latter analyses the inbound traffic of n_2, activates dedicated countermeasures (steps 4 and 5), and decides if the session is finally authorized or not (steps 6 to 8). The safeguard and watchman components are complementary and target the residual attacks that the certification mechanisms of RELOAD cannot manage alone.

VI. Performance Evaluation

In order to evaluate the performance of our prevention strategy, we have conducted an extensive set of experiments based on the p2ptrust simulator [18]. During these experiments, we have considered a P2PSIP network composed of up to 300 nodes. A subset of these P2PSIP nodes interact as malicious nodes and generate attacks. When an attack is successfully performed on a given P2PSIP node, the targeted node can be disabled from the network (neutral compromission), or can become a new malicious node (active compromission). Another subset of nodes represent a pool of proxy servers which can be activated as watchmen in the RELOAD architecture. In a first series of experiments, we were interested in evaluating the benefits and limits of our prevention strategy (eigentrust coupled with countermeasures) in comparison to an avoidance strategy (eigentrust only). We

have quantified the rate of successful P2PSIP sessions in the network while varying the percentage of malicious nodes from 0% to 100% in the network; the number of nodes being set to 150. The experimental results are described in Figure 3 where we have plotted respectively the success rate for our prevention strategy (active compromission) and the avoidance strategy (active and neutral compromissions). We have also plotted two additional curves corresponding to the ratio between these two strategies. During these experiments, we have observed a benefit of up to 8% in comparison to the avoidance strategy in case of active compromission. As we expected, this benefit is less important in case of neutral compromission: the difference with our prevention strategy is of 5% on average with the active compromission, and falls to 3% on average with the neutral compromission. It is evident that there is no benefit of using our strategy when the percentage of malicious nodes is of 0% (no malicious nodes) or 100% (all the nodes are malicious), but these scenarios are extreme.

Another important issue is to evaluate the scalability of this solution. In a second series of experiments, we have quantified the message overhead while varying the size of the P2PSIP network from 50 to 300 nodes. We have considered that 20% of the network nodes are malicious. Figure 4 represents the distribution of the signalling traffic for the different network sizes. It permits to distinguish the relative importance of the regular messages due to the establishment of P2PSIP sessions, from the overhead messages related to the eigentrust algorithm and the countermeasures (watchmen). This figure clearly shows that the eigentrust maintenance represents the most important part of the traffic overhead. For instance with 50 nodes, the overhead messages represent 25% of the overall signalling traffic. We can decompose this 25% into 14% due to the eigentrust algorithm and 11% due to the countermeasures. When the network size growths to 300 nodes, this percentage goes to 59%, with 52% due to eigentrust and 7% due to countermeasures. When we analyse the number of messages (absolute values), we obtain the same statement: the countermeasure messages have a linear behaviour while the eigentrust messages have a quadratic one. Our prevention strategy is therefore strongly dependent on the performance of the eigentrust algorithm, and its scalability directly relates to the scalability of eigentrust.

VII. Conclusions and Future Work

The RELOAD protocol integrates a security framework based on certification techniques for supporting P2PSIP networks. We propose in this paper a trust-based prevention strategy for completing the RELOAD architecture, and addressing the residual attacks that the current framework does not cover. Our approach relies on the coupling of a trust layer based on the eigentrust algorithm with a prevention layer implementing countermeasure mechanisms. We have identified trust metrics for the RELOAD architecture, and have described a mathematical modelling supporting their assessment and aggregation. From this modelling, we have designed two dedicated prevention mechanisms based on the concept of watchmen and safeguards. They permit to minimize potential attacks from untrusted nodes and to protect vulnerable ones. We have also evaluated the proposed approach through an extensive set of experiments. In particular, we have quantified the benefits (up to 8%) and limits with respect to the session success rate, and have analysed the scalability properties by assessing the traffic overhead in various configurations.

As future work, we are planning to evaluate and compare the performance of our prevention solution using alternative trust algorithms. Moreover, our approach providing an additional security feature to the RELOAD architecture, we are interested in designing self-configuration mechanisms for the security framework of this architecture.

References

[1] J. Davidson, J. Peters, M. Bhatia, and S. K. S. Mukherjee, *Voice over IP Fundamentals*. Cisco Press, 2007.

[2] D. Bryan, B. Lowekamp, and C. Jennings, dSIP: A P2P Approach to SIP Registration, IETF Internet Draft, http://tools.ietf.org/html/draft-bryan-p2psip-dsip-00, February 2007.

[3] D. Bryan, P. Matthews, E. Shim, D. Willis, and S. Dawkins, Concepts and Terminology for Peer to Peer SIP, IETF Internet Draft, http://tools.ietf.org/html/draft-ietf-p2psip-concepts-03, October 2010.

[4] C. Jennings, E. Rescorla, S. Baset, and H. Schulzrinne, RE-source LOcation And Discovery (RELOAD), IETF Internet Draft, http://tools.ietf.org/html/draft-ietf-p2psip-base-18, August 2011.

[5] H. Song, M. Matuszewski, and D. York, P2PSIP Security 0verview and Risk Analysis, IETF Internet Draft, http://tools.ietf.org/html/draft-matuszewski-p2psip-security-requirements-06, Jan 2010.

[6] Y. Mao and A. Swaminathan, Threat Analysis for Peer-to-Peer Networks, IETF Internet Draft, http://tools.ietf.org/html/draft-mao-p2psip-threat-analysis-00, Sep 2009.

[7] J. Seedorf, "Security Challenges for Peer-to-Peer SIP," *EEE Network*, vol. 20, no. 5, pp. 38–45, 2006.

[8] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner, "Spam over Internet Telephony (SPIT) Prevention Framework," in *Proc. of the IEEE Global Communications Conference, Exhibition and Industry Forum (GLOBECOM'06)*, San Francisco, USA, November 2006.

[9] O. Dabbebi, R. Badonnel, and O. Festor, "A Broad-spectrum Strategy for Runtime Risk Management in VoIP Enterprise Architectures," in *Proc. of the IEEE Integrated Network Mgmt Conference (IM'11)*, 2011.

[10] S. Becker, H. J. Abdelnur, J. L. Obes, R. State, and O. Festor, "Improving Fuzz Testing Using Game Theory," in *Proc. of the IEEE Network and System Security Conference (NSS'10)*, Melbourne, Australia, 2010.

[11] V. M. Quinten, R. van de Meent, and A. Pras, "Analysis of Techniques for Protection Against Spam over Internet Telephony," in *Proc. of the EUNICE European Summer School (EUNICE'07)*, 2007.

[12] T. Cholez, I. Chrisment, and O. Festor, "Evaluation of Sybil Attacks Protection Schemes in KAD," in *Proc. of the International Conference on Autonomous Infrastructure, Mgmt and Security (AIMS'09), 2009*.

[13] C. Miguel, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," *SIGOPS Operation System Review*, vol. 36, pp. 299–314, December 2002.

[14] W. Yang and P. Judge, "VISOR: VoIP Security Using Reputation," in *Proc. of The IEEE International Conference on Communications (ICC'08)*, Beijing, China, 2008, pp. 1489–1493.

[15] J. Heikkil and A. Gurtov, "Filtering SPAM in P2PSIP Communities with Web of Trust," in *Proc. of the Security and Privacy in Mobile Inf. and Comm. Systems Conference (MobiSec'09)*, Turin, Italy, June 2009.

[16] X. Zheng and V. A. Oleshchuk, "Trust-based Framework for Security Enhancement of P2PSIP Communication Systems," in *Proc. of the 4th International Conference for Internet Technology and Secured Transactions, (ICITST'09)*, London, England, 2009.

[17] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," in *Proc. of the 12th International Conference on World Wide Web*, ser. (WWW'03). New York, USA: ACM, 2003, pp. 640–651.

[18] P2P Trust Simulator, University of Pennsilvania, Penn Engineering School, http://rtg.cis.upenn.edu/qtm, 2009.