A Privacy-Preserving Entropy-Driven Framework for Tracing DoS Attacks in VoIP

Zisis Tsiatsikas*, Dimitris Geneiatakis†, Georgios Kambourakis* and Angelos D. Keromytis‡
*Dept. of Inform. and Comm. Systems Engineering, University of the Aegean, Karlovassi, Greece
Email:{tzisis,gkamb}@aegean.gr
†Institute of the Protection and Security Citizen, Joint Research Center, Ispra, Italy
Email: dimitrios.geneiatakis@jrc.ec.europa.eu
‡Department of Computer Science, Columbia University, New York, USA
Email: angelos@cs.columbia.edu

***Abstract*—Network audit trails, especially those composed of application layer data, can be a valuable source of information regarding the investigation of attack incidents. Nevertheless, the analysis of log files of large volume is usually both complex (slow) and privacy-neglecting. Especially, when it comes to VoIP, the literature on how audit trails can be exploited to identify attacks remains scarce. This paper provides an entropy-driven, privacy-preserving, and practical framework for detecting resource consumption attacks in VoIP ecosystems. We extensively evaluate our framework under various attack scenarios involving single and multiple assailants. The results obtained show that the proposed scheme is capable of identifying malicious traffic with a false positive alarm rate up to 3.5%.**

Keywords*—*Session Initiation Protocol, Entropy, Abnormal Traffic, DoS, Anonymity.

I. Introduction

Session Initiation Protocol (SIP) [1] is considered the predominant signaling protocol in Voice over IP (VoIP) ecosystems. In fact, SIP follows the request/response model used in HTTP, thus making it easy to construct and decode its messages. This highly degree of freedom makes SIP services prone to a variety of attacks already covered in the literature in great detail [2]–[6]. In this context, various mechanisms have been proposed to shield the provided multimedia services from attacks and misuses. Nevertheless, in most cases, security evaluation approaches do not take into account the existing audit trails, mainly due to the lack of appropriate tools for examining them. Consequently, it might be mistakenly assumed that the underlying services are secure, while in fact they are prone to several security attacks, *e.g.,* resource consumption or other type of Denial of Service (DoS). These attacks may remain hidden - due to their low impact for example - but they do lurk in the provided service. Note that vulnerability assessment tools such as Nessus (www.nessus.org) and Retina (www.eeye.com) can be used to evaluate system security. However, these tools cannot be used in cases where it is required to prove that the systems are free from attacks. From time to time, various researchers, organizations, and expert groups have highlighted the merit of using audit trails in security analysis. For instance, the National Institute of Standards and Technology (NIST) in [7] mentions that in conjunction with appropriate tools and procedures, audit trail can assist in detecting security violations and flaws in applications.

On the other hand, personal data contained in audit trails are subject to various legal restrictions and regulations. This is because the exposure of sensitive personal information contained in audit trails to unauthorized entities facilitates several malicious acts that clearly violate the users' private sphere [8]–[11]. The most obvious is that an ill-motivated actor is able to obtain access to the user's real identity and to observe which services are being accessed by them, thus violating the principle of user anonymity [12], [13]. In the long term, when this kind of information is systematically collected, the user can be profiled and sensitive information (*e.g.,* preferred services) can be inferred.

Various research works [14]–[18] have been dedicated to the identification of resource consumption attacks as a part of network Intrusion Detection Systems (IDS). However, very few focus on the analysis of VoIP audit trails to identify and distinguish uncommon or suspicious traffic. In this context, the potential of using entropy towards detecting attack incidents has not been totally neglected by the research community. For instance, an entropy based solution has been proposed in [19] to detect IP spoofing DoS attacks by monitoring the distribution of destination/source IP addresses. Similar methods can be also utilized in VoIP services to analyse audit trails (or real data traffic), but their scope is narrowed down to the IP level only. Nevertheless, data coming from the application layer is usually rich of information that can be processed towards identifying security incidents. As further explained in Section V the only published work that touches upon this subject is presented in [20].

In a nutshell, audit trails, especially those of large volume as in the case of multimedia services, are rarely utilized properly so as to prove service abuse. As already pointed out this is mainly due to privacy restrictions. Therefore, as a general rule, any solution focusing on digital forensic analysis should deduce services security level with respect to audit trails (as well), but it is important to do so without violating the privacy of the end-user.

In this paper, we capitalize on the idea proposed in [21] and introduce an entropy-driven algorithm for audit trail analysis

in SIP with respect to users' privacy, meaning that no sensitive user data is processed during the analysis. It is argued that the proposed scheme is lightweight in nature, thus it is able to examine large volumes of SIP transactions on-the-fly and take quick and accurate decisions if the traffic under investigation belongs to attack traffic or not. Moreover, our proposal is fully compatible with the SIP standard and requires no special equipment or complex procedures to carry out its goal. We extensively evaluate our scheme by conducting several experiments under different DoS attack scenarios. To the best of our knowledge, none of the existing forensic analysis tools respects end-user's privacy and simultaneously provides proofs of existing security flaws in a formal way as a public service. In this respect, our solution bridges the gap between the limitations of existing approaches to identify security flaws by examining the audit trails, while at the same time is orthogonal to the current defensive approaches.

The rest of the paper is structured as follows. The next section provides background information related to our approach. Section III details on the proposed solution. Section IV evaluates the proposed scheme in terms of effectiveness. The related work is discussed in Section V. Finally, Section VI concludes and provides pointers to future study.

II. Preliminaries

A. Entropy & Itself Information

Entropy is a metric of uncertainty based on mathematical theory of communication introduced by Shannon [22]. This means that entropy quantifies the expected value of the information contained in a message. That is, reduced uncertainty is quantified in a lower entropy and vice versa. As a result, the probability of occurrence (certainty of an outcome) of a symbol contained in a message can provide us with knowledge about hidden redundancy in the information received.

Specifically, considering that a symbol $A(i)$ in a specific set S has probability $P_A(i)$, then the *itself information* (included in that symbol) is by definition:

$$I_A(i) = -\log_b p_A(i) \tag{1}$$

The average of *itself information* connected to the set S is called entropy and is computed using the following formula:

$$H(S) = -\sum_{i=1}^{n} P(i) * \log_b p(i) \tag{2}$$

The entropy of a source set S maximizes when all instances (*e.g.,* messages) contained in that set are equal ($P_A(i) = 1/n$). This means that the uncertainty of the outcome is maximized, while the redundancy in set S is minimized. With respect to *itself information* this fact indicates that all messages (or symbols corresponding to certain fields of the message) contain the same amount of information. Note that the greater the probability of a specific message the less information is included in it. Furthermore, in case where two symbols are independent of each other then the itself information and the entropy metrics are calculated using the formulas (3) and (4) respectively.

$$I(A, B) = I(A) + I(B) \tag{3}$$

$$H(A, B) = H(A) + H(B) \tag{4}$$

TABLE I
SYMBOLS OF INTEREST CONTAINED IN A SIP MESSAGE

Symbol	Corresponds To	Symbol	Corresponds To
S1	First-Line (requested resource)	S2	Via header
S3	FROM header	S4	TO header
S5	Call-ID header	S6	Contact header
S7	entire SIP message	-	-

B. Symbol Definition: Information Theory in the Context of VoIP

To apply the aforementioned principles of information theory in the context of VoIP auditing service, we define in Table I certain parts of a SIP message as the symbols of interest. The selection of these symbols reflects the different types of SIP messages that an aggressor could craft in order to launch a resource consumption attack. For instance, a malicious user could select to replay the same message (by using identical instances of S7) or fabricate different SIP messages by modifying certain segments such as FROM, TO, Call-ID, headers or even the First Line (symbols S1 to S5) depending on the case. For the interested reader, a detailed analysis for resource consumption attacks in VoIP can be found in [2]–[4].

C. Overview of the Proposed Framework

Bear in mind that according to the entropy theory, symbol redundancy indicates lower entropy values. This means that some symbols have greater frequency of occurrence, thus corresponding to less *itself information* compared to other symbols that coexist in the same set of messages. In the ideal case, an audit trail should not contain message redundancies, except those that occur due to retransmissions. Under this observation, we rely on entropy to measure the dissimilarity among different audit trails and determine whether they contain suspicious records or not. This is achieved by calculating the *itself information* for each symbol of interest contained in each message in order to identify if the latter can be classified as attack traffic or not. To accomplish such a comparison we require that one of the cross-evaluated audit trail sets is attack-free. This set is used as a reference (training set) when conducting the analysis.

As already pointed out, we capitalize on the idea introduced in [21] to identify abnormal behavior in multimedia communication services. In their preliminary analysis the authors demonstrated that audit trails can be a valuable source of

information related to the investigation of attack incidents. In this paper we extend the above referenced initial work in the following ways: (a) We extensively assess its potential under several different attack scenarios, (b) We offer a generalized way to calculate and calibrate the detection parameters used during the classification of traffic into normal or not, (c) We introduce a novel metric, namely *actual information distance*, aiming to compare different sets of traffic. From the analysis it is shown that this metric can be used to identify resource consumption attacks with high certainty, and (d) We argue that in order to identify security incidents we should examine the message not as a whole, but instead combine the information stemming from different parts of the SIP message.

As we detail in the following section, the proposed method is also able to preserve users' privacy because all data is hashed before they can be fed into the decision engine.

III. Anonymous Identification of Abnormal Traffic

A. Metrics Definition

We define the following metrics used by the proposed tracing scheme.

Actual (itself) Information (AI): measures the randomness of a message included in a particular set. Taking into account that in the proposed model a SIP message is consisted of S1 to S6 symbols, we compute the randomness of each individual message, named *actual itself information* using formula (5).

$$AI(S) = \sum_{i=1}^{n} I_S(i) \tag{5}$$

Theoretical Maximum (TM): defines the theoretical maximum randomness value that a message can hold in a particular set. This value is computed by formula (6), where n is the maximum number of symbols contained in the message.

$$TM(i) = -n * \log_b P_S(i) \tag{6}$$

Normal Average Distance (NAD): represents the average randomness distance of an attack-free traffic from its theoretical maximum value. Its value is computed by formula (7).

$$NAD = Avg(TM - AI) \tag{7}$$

Actual Information Distance (AID): measures the distance of an examined audit trail message from its theoretical maximum. Its value is computed by formula (8).

$$AID = TM - AI \tag{8}$$

Normal Threshold (NT): defines the threshold that should not be exceeded by the AI of an examined message in order this message to be classified as normal. The NT value relies on NAD adjusted by a parameter δ, which in turn relies on the characteristics of the examined traffic.

Audit Trail Entropy (ATE): this last metric, computed by formula (9), represents the overall randomness included in an audit trail based on the sum of entropy values per message in that set.

$$ATE(S) = \sum_{i=1}^{n} H_S(i) \tag{9}$$

B. The proposed scheme

Initially, we anonymize the audit trail data by hashing the pre-defined symbols per message. Specifically, for each message contained in the audit trail, we employ SHA-1 to obtain the hash of every symbol defined in Table I. Hashing allow us to keep symbol frequency unmodified, while obscuring the initial values. This means that the initial information (*i.e.,* the whole message) can be retrieved only if the audit trail becomes available. In case that it is needed to identify the exact initial messages, the audit trail is anomyzed and each of the attack messages is compared against the anonymized ones. If there is a match then we extract the initial message for further examination.

Naturally, other anonymization techniques [23], such as hiding, permutation or enumeration can also be utilized here. However, such approaches require keeping metadata information in secure storage for the case where the initial messages need to be retrieved. This fact constitutes the above-mentioned schemes more complex, and of course vulnerable to attacks, as this additional information is required to be stored in a secure manner. Also, as reported in [24] anonymization can have severe undesirable outcomes if implemented incorrectly.

Next, security analysis is applied to the anonymized data for measuring the uncertainty included in the audit trail. More specifically, in the proposed model we compute: (a) the AI per message, (b) the AID for the examined set, and (c) the ATE over the whole set of messages contained in the audit trail file. In order to identify abnormalities (which may indicate a DoS attack) we assume that there exist at least one attack-free audit trail, to be used as a training set for calculating the NT as well as the NAD metrics (see Section III.A). Then, the computed values are checked against the corresponding thresholds in order to have the messages classified as attack or normal traffic. To extract the exact message details and reveal additional information related to the attack message(s) we use the hash values included in the malicious set and search for the corresponding values in the audit trail. It should be noted that there is no need to access the initial values since there is no match between these values. The initial values are retrieved only if the hash values match. This way, we can publicize information and outsource data for security related analysis that otherwise are considered private.

IV. Evaluation

A. Setup

For assessing the effectiveness of the proposed method in detecting abnormalities in SIP traffic we used the well-known open source *Kamailio* (http://www.kamailio.org/w/) as a VoIP server. For generating the background and attack traffic we employed *sipp* (http://sipp.sourceforge.net/) and *sipsak* (http://

TABLE II
DESCRIPTIONS OF THE SCENARIOS EVALUATED. EACH ONE EXECUTED FOR A PERIOD OF 120 SEC.

Scenario Number	Description
SN1	30 legitimate users establishing 5 calls/sec. The maximum number of calls per user/sec is 2. This scenario contains no attack traffic.
SN1.1, SN1.2, SN1.3	These 3 sub-scenarios use the background traffic of SN1 and single source SIP INVITE flood attack traffic with a rate of 5, 12 and 30 calls/sec.
SN2	30 legitimate users establishing 5 calls/sec. The maximum number of calls per user/sec is 5. This scenario contains no attack traffic.
SN2.1, SN2.2, SN2.3, SN2.4	These 4 sub-scenarios use the background traffic of SN2 and single source SIP INVITE flood attack traffic with a rate of 8, 20, 40 and 80 calls/sec.
SN3	30 legitimate users establishing 2 calls/sec. The maximum number of calls per user/sec is 600.
SN3.1, SN3.2, SN3.3, SN3.4	The last 4 sub-scenarios use the background traffic of SN3 and multiple source SIP INVITE flood attack traffic with a rate of 25, 50, 175, 350 calls/sec.

sipsak.org/) respectively. The VoIP server records all the traffic, which will be used for offline analysis by the proposed framework.

We implemented fourteen scenarios summarized in Table II in an effort to assess the effectiveness of our scheme to identify DoS and traffic abnormalities in general. In all the scenarios it is introduced different (legitimate) background traffic, while various attacks have been simulated in order to examine if they can be traced by the proposed solution and to which degree. We should also stress out that the rate of traffic used in each scenario included in Table II corresponds to the rate the tools (sipp, sipsak) are pre-configured to operate with. Scenarios SN1, SN2 and SN3 serve as references for attack-free traffic in order to assess the proposed solution under different traffic patterns, and therefore are used for calculating the NT as well as the NAD metrics for the sub-scenarios.

B. Analysis

Figure 1 illustrate snapshots of the distribution of the AI metric for scenarios SN1, SN1.1, SN1.2 and SN1.3. Note that similar distributions have been recorded for the remaining scenarios. When compared to the other scenarios, the AI in SN1 is closer to its TM value due to many retransmittions and the call pattern used. That is, many retransmissions occurring in a short period of time may falsely indicate DoS traffic. Although, we rely on a simulated environment, this is also the case for real architectures, where users build a specific call pattern during a particular period of time [25], [26].

In all the attack sub-scenarios the AI metric obtains lower values due to excessive symbol repetitions in the examined set of messages. This behavior is distinctively depicted in Figures 1, as the attack traffic is increased gradually for scenarios SN1.1 to SN1.3 respectively. For instance, in SN1, the TM is

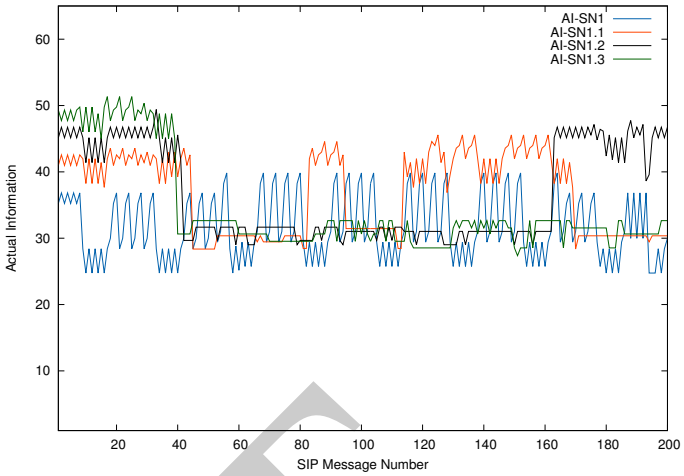

Fig. 1. Sample of actual info (AI) for scenarios SN1, SN1.1, SN1.2 and SN1.3.

46.06 and the average AI 31.78, while in attack sub-scenarios, say SN1.1, both the TM and average are increased to 67.78 and 36.75 respectively. Recall that lower values in AI is a strong indication of uncommon behavior. This indication can be used also in cases where an attack-free audit trail is not available. However, in such an unusual case, we should take into account either the theoretical users' behavior or employ other techniques (as in [27], [28]) aiming to estimate the appropriate threshold. It is also relevant to note here that the values related to TM vary among different scenarios, since the examined set includes different number of recorded messages.

For all the scenarios the NT metric is adjusted to the corresponding traffic pattern using the δ parameter. In our case, this parameter is equal to the St. Dev. value calculated over the messages that consist the corresponding normal traffic set. This means that in order to deduce if a particular message is part of an uncommon traffic pattern we compute its AI (according to equation 5) and compare it with the NT value. The statistics for all the scenarios are summarized in Table III.

To evaluate the accuracy of the proposed solution in identifying DoS attacks we use legacy IDS error assessment metrics, namely False Positive (FP) and False Negative (FN) [29]. The first one is related with messages detected as abnormal but they belong to the legitimate traffic, while the latter involves messages detected as normal but they belong to abnormal traffic. In this context, the attack traffic is logged in parallel and independently in order to use it on a later stage to validate the correctness of our proposal to classify a message as malicious or not. The results of this analysis are summarized in Table III as well. To further validate the outcomes, we also analyse considerable volume of legitimate traffic having similar patterns to SN1, SN2, SN3. In all these cases, no false alarm was detected meaning that our solution is sound. Regarding the results derived from the rest of the scenarios we were able to detect only FP. Particularly, in all the scenarios, we identify accurately all the attack traffic, while the FP value for all SN1 to SN3 sub-scenarios fluctuates between 1% to 3.5%.

TABLE III
FALSE ALARM RATIO AND STATISTICS FOR ALL THE SCENARIOS

Scen.	Traf.		FP		Stats.			
	RC	AC	In.	%	TM	St. Dev	Thrsh.	AI MV
SN1	219	-	-	-	46.60	4.78	14.88	31.78
SN1.1	443	199	0	-	52.70	4.88	19.76	36.60
SN1.2	715	464	8	1.1	56.89	5.54	20.42	35.76
SN1.3	963	721	-	-	59.46	5.79	20.67	35.54
SN2	891	-	-	-	52.80	4.76	13.04	40.13
SN2.1	892	438	32	3.5	58.80	5.21	18.25	39.43
SN2.2	1095	644	33	3.0	60.58	5.55	18.59	38.97
SN2.3	2683	895	28	1.0	62.34	5.78	18.82	38.60
SN2.4	3655	1389	29	-	65.01	5.94	18.98	38.22
SN3	2275	-	-	-	60.91	4.39	14.39	46.51
SN3.1	5031	1422	39	0.7	67.78	4.43	18.82	45.85
SN3.2	5769	1798	35	0.6	68.96	4.53	18.92	45.70
SN3.3	9683	3899	32	0.33	73.44	4.81	19.2	45.03
SN3.4	17317	7800	41	0.23	78.47	5.10	19.49	44.75

Bear in mind that the rate of FP is highly affected by possible retransmissions and users' call behavior depending on the case.

In this point, one might argue that an FP of 3.5% is quite significant. However, in forensic analysis, privacy-preserving solutions need to always balance between security and privacy. We argue that this percentage is very promising; however, along with the calibration of the metrics currently used in our model, there might exist additional parameters that may affect its behavior and thus lead to better results. This is an issue worth of investigating in a future work. It is also important to note that if we solely consider the whole message as an independent symbol (S7), then the AI will receive the maximum theoretical TM value of this set. This happens because every SIP message, either legitimate or not, always presents some additional fields or parameters that uniquely differentiate it from any other. Obviously, if doing so, one will end-up believing that the audit trail under investigation is attack-free. Thus, our model makes use of the AI metric which involves information stemming from different, but clearly defined, symbols of the SIP message structure.

V. Related Work

This section examines related work on the topic. Note that we only consider proposals that deal with DoS attacks and also employ entropy and/or audit trail analysis for identifying security flaws. Hence, other works on the general filed of intrusion detection in SIP and related protocols [30], [31] remains out-of-scope of this paper.

The authors in [19] propose a system that analyzes the level of entropy in the distribution of source and destination IP addresses with aim of protecting IP services against spoofing attacks. According to the authors, all active (TCP/UDP) sessions are examined if they follow the normal entropy distribution. In case a violation of the normal pattern is detected the session is dropped. A similar approach is followed in [32], where the authors propose a system able to flush out DoS attacks by assessing the level of entropy in distributions of source and destination IP address for traffic traversing one or more network links. In more detail, the authors point out that after identifying upper and lower entropy thresholds for each link under normal conditions, and comparing them with current source and destination entropy values, different flavors of DoS incidents can be identified. The authors in [33] propose a solution for protecting web services against distributed DoS. Their scheme is based on attack-tree model and utilizes entropy to identify abnormalities. Initially, an attack-tree is constructed to obtain an abstraction of the router-level Internet graph. Next, for each router, entropy is calculated having as input immediate packet flows. Finally, an alert is raised every time entropy falls below a threshold.

To the best of our knowledge the only work that focuses on analysis of security incidents and audit trails in converged networks is given in [20]. More specifically, the authors rely on a predetermine attack pattern to identify malicious activity. This is done by combining information stemming from multiple sources. Unfortunately, the authors do not provide any results related to the accuracy of their approach. The most relevant work to ours is that of [21] where the authors introduce a method for detecting abnormalities in SIP based VoIP traffic. As already pointed out in section II, the current paper capitalizes on this aforementioned work by refining its parameters and extensively assessing its potential under different attack scenarios.

VI. Conclusions And Future Work

SIP-based services confront several security issues mainly due to the open and text-oriented nature of the protocol. In this direction, researchers are seeking novel proposals that are able to promptly identify security breaches and apply effective methods of control. In this context, audit trails can be a valuable source of information towards the detection of attacks. Unfortunately, so far, little has been done in VoIP realms for exploiting audit trails in this way. This is mainly because audit trails containing application data are rich of users' private information, and thus any method for processing them should take into careful consideration the privacy of the end-user. In this paper, we capitalize on an idea proposed in [21], that is, the use of entropy principles to detect abnormalities in raw application data. Specifically, through extensive experimentation, we extend, calibrate and assess the effectiveness of the initial idea, thus offering a complete formalized framework that can be used to trace and detect DoS attacks in VoIP ecosystems. We argue that our framework is lightweight, practical, privacy-preserving, and retains full compatibility with the SIP standard. Also, its accuracy is very high, materialized in a 3.5% FP.

Apart from future work directions already identified in Section IV, we are planning to further assess our proposal by

using large volumes of real SIP traffic, while we investigate possibilities to introduce the proposed technique in a collaborative IDS such as those described in [34].

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "Sip: Session initiation protocol," United States, 2002.

[2] S. Ehlert, D. Geneiatakis, and T. Magedanz, "Survey of network security systems to counter sip-based denial-of-service attacks," vol. 29, no. 2, 2010, pp. 225 – 243.

[3] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert, and D. Sisalem, "Survey of security vulnerabilities in session initiation protocol," vol. 8, 2006, pp. 68–81.

[4] A. D. Keromytis, "A comprehensive survey of voice over ip security research," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 514–537, 2012.

[5] A. Keromytis, "Voice over ip: Risks, threats and vulnerabilities," in *Proceedings of the Cyber Infrastructure Protection (CIP) Conference*, 2009.

[6] A. D. Keromytis, "Voice-over-ip security: Research and practice," *Security Privacy, IEEE*, vol. 8, no. 2, pp. 76–78, 2010.

[7] M. Swanson, B. Guttman, N. I. of Standards, and T. (U.S.), *Generally accepted principles and practices for securing information technology systems*. National Institute of Standards and Technology, Technology Administration, U.S. Dept. of Commerce, [Gaithersburg, Md.] :, 1996.

[8] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1450006, Jul. 2012.

[9] O. Tene, "Privacy: The new generations," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1710688, Nov. 2010.

[10] L. Sweeney, "Uniqueness of Simple Demographics in the U.S. Population," *LIDAP-WP4 Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA: 2000*, 1000.

[11] P. Golle, "Revisiting the uniqueness of simple demographics in the us population," in *Proceedings of the 5th ACM workshop on Privacy in electronic society*, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 77–80.

[12] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2009.

[13] F. Pereniguez, R. Marin-Lopez, G. Kambourakis, S. Gritzalis, and A. Gomez, "Privakerb: A user privacy framework for kerberos," vol. 30, no. 67, 2011, pp. 446 – 463.

[14] S. Ehlert, G. Zhang, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, and D. Sisalem, "Two layer denial of service prevention on sip voip infrastructures," vol. 31, no. 10. Amsterdam, The Netherlands, The Netherlands: Elsevier Science Publishers B. V., Jun. 2008, pp. 2443–2456.

[15] J. Ioannidis and S. M. Bellovin, "Implementing pushback: Router-based defense against DDoS attacks," in *Proc. Internet Society Symposium on Network and Distributed System Security*, 2002.

[16] R. Mathew and V. Katkar, "Survey of low rate dos attack detection mechanisms," in *Proceedings of the International Conference & Workshop on Emerging Trends in Technology*, ser. ICWET '11. New York, NY, USA: ACM, 2011, pp. 955–958.

[17] J. Mirkovic and P. Reiher, "D-ward: A source-end defense against flooding denial-of-service attacks," vol. 2, no. 3. Los Alamitos, CA, USA: IEEE Computer Society Press, jul 2005, pp. 216–232.

[18] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A framework for a collaborative ddos defense," in *Proceedings of the 22nd Annual Computer Security Applications Conference*, ser. ACSAC '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 33–42.

[19] W. Ehrlich, K. Futamura, and D. Liu, "An entropy based method to detect spoofed denial of service (dos) attacks," in *Telecommunications Modeling, Policy, and Technology*, ser. Operations Research/Computer Science Interfaces, S. Raghavan, B. Golden, and E. Wasil, Eds. Springer US, 2008, vol. 44, pp. 101–122.

[20] J. Pelaez and E. Fernandez, "Voip network forensic patterns," in *Computing in the Global Information Technology, 2009. ICCGI '09. Fourth International Multi-Conference on*, aug. 2009, pp. 175 –180.

[21] D. Geneiatakis and A. D. Keromytis, "Towards a forensic analysis for multimedia communication services," in *Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications*, ser. WAINA '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 424–429.

[22] C. E. Shannon, "A mathematical theory of communication," vol. 27, 1948.

[23] G. Kuenning and E. L. Miller, "Anonymization techniques for urls and filenames," Tech. Rep., 2003.

[24] N. Ramakrishnan, B. J. Keller, B. J. Mirza, A. Y. Grama, and G. Karypis, "Privacy risks in recommender systems," vol. 5, no. 6. Piscataway, NJ, USA: IEEE Educational Activities Department, Nov. 2001, pp. 54–62.

[25] P. O. S. V. De Melo, L. Akoglu, C. Faloutsos, and A. A. F. Loureiro, "Surprising patterns for the call duration distribution of mobile phone users," in *Proceedings of the 2010 European conference on Machine learning and knowledge discovery in databases: Part III*, ser. ECML PKDD'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 354–369.

[26] D. Zhang, A. V. Vasilakos, and H. Xiong, "Predicting location using mobile phone calls," vol. 42, no. 4. New York, NY, USA: ACM, Aug. 2012, pp. 295–296.

[27] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, ser. IMW '02. New York, NY, USA: ACM, 2002, pp. 71–82.

[28] A. N. Hussain, "Measurement and spectral analysis of denial of service attacks," Ph.D. dissertation, Los Angeles, CA, USA, 2005, aAI3196820.

[29] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skorić, "Measuring intrusion detection capability: an information-theoretic approach," in *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, ser. ASIACCS '06. New York, NY, USA: ACM, 2006, pp. 90–101.

[30] G. Karopoulos, G. Kambourakis, and S. Gritzalis, "Privasip: Ad-hoc identity privacy in sip," vol. 33, no. 3. Amsterdam, The Netherlands, The Netherlands: Elsevier Science Publishers B. V., Mar. 2011, pp. 301–314.

[31] S. Ehlert, C. Wang, T. Magedanz, and D. Sisalem, "Specification-based denial-of-service detection for sip voice-over-ip networks," in *Internet Monitoring and Protection, 2008. ICIMP '08. The Third International Conference on*, 29 2008-july 5 2008, pp. 59 –66.

[32] W. Ehrlich, K. Futamura, and D. Liu, "An entropy based method to detect spoofed denial of service (dos) attacks," in *Telecommunications Modeling, Policy, and Technology*, ser. Operations Research/Computer Science Interfaces, S. Raghavan, B. Golden, and E. Wasil, Eds. Springer US, 2008, vol. 44, pp. 101–122.

[33] G. Gandhi and S. Srivatsa, "An entropy algorithm to improve the performance and protection from denial-of-service attacks in nids," in *Computer and Electrical Engineering, 2009. ICCEE '09. Second International Conference on*, vol. 1, dec. 2009, pp. 603 –606.

[34] M. Locasto, J. Parekh, S. Stolfo, A. Keromytis, T. Malkin, and V. Misra, "Collaborative distributed intrusion detection," Department of Computer Science, Columbia University, Tech. Rep. CUCS-012-04, 2004.