Indian J.Sci.Res. 17(2): 37 - 44, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

A NOVEL ANOMALY DETECTION TECHNIQUE USING SIP PROTOCOL FOR VOIP NETWORKS

[1]N Srinivas, [2]Dr M V Ramana Murthy
[1] Research Scholar,Department of Computer Science, Rayalaseema University, Kurnool
[2] Professor, Department of Mathematics & Humanities, Mahatma Gandhi Institute of technology, Hyderabad

Abstract-VoIP applications are emerging today as an important component in business and communication industry. In this paper, we address the intrusion detection and prevention in VoIP networks. It is particularly designed for the signaling protocol SIP. The proposed system mainly consists of two parts. The first one determines the different features that are extracted from the specification of the SIP protocol. In fact, these features should highly characterize the behavior of the signaling traffic so that the evidence of the intrusion is not lost when only these at-tributes are considered for the attack detection goal..Parameters that indicate the Quality of Service such as delay, jitter, packet loss and MOS are analyzed in these scenarios. The simulations results indicate that better choice of voice codecs and statistical distribution have significant impact on VoIP performance. After the attributes extraction step, a detection algorithm is used to classify new SIP profiles in their appropriate class (ei-ther as normal, or as an anomaly). Another feature of this system is its adaptability since a feedback from the detected attacks is possible.

Keywords: VOIP Network. Intrusion Detection, VOIP Protocol

I. Introduction

A growing trend has been noticed in real time voice communication such as Voice over Internet Protocol (VoIP) in the recent years [1]. VoIP enables users to use Internet or intranet as transmission medium for telephone calls by sending voice data in packets using Internet Protocol (IP) rather than by traditional circuit switched Public Switched Telephone Network (PSTN) [2]. VoIP is based on IP and therefore the transmission technology is essentially digital [3]. Because of the digital transmission system, caller's voice is first digitized and then separated in packets using complex algorithms known as codecs. Different codecs like G.711, G.723 and G.729 are used for encoding and decoding, most ofwhich are defined by International Telecommunication Union-the Telecommunication Division (ITU-T). VoIP can be deployed on any IP based data network such as the Internet, Ethernet, Fiber Optic or wireless such as WiMAX and 3G.

The telecommunication technology has also evolved in the recent years to meet the increasing demands of the network users. In the past few years, the IP network has been extended to use wireless access technologies like 802.11 based Wireless Local Area Network (WLAN) [4] and Third Generation (3G)

[5] cellular networks. These networks are already in an excessive demand for real time applications like voice, video and other multimedia related applications. An alternative solution is sought with the success of IEEE 802.16e standard

[6] for Mobile Worldwide Interoperability for Microwave Access (WiMAX) [7] in the metropolitan areas. WiMAX is an access technology which provides wireless data transmission in various ways ranging from point-to-point links to mobile cellular access [8]. It is based on IEEE 802.16 standard, which provides wireless broadband access as an alternative to the cable and Digital Subscriber Loop (DSL) [9]. WiMAX provides basic IP connectivity to the users using mobile broadband data access.

The first stage consists in collecting the VoIP traffic that is either safe, which is free of attacks, that we call here normal and attack traffic that contains traces of attacks evidence. The second stage consists in extracting attributes; those features that keep the most in-formation characterizing the traces without attack and nor-mal traffic evidence loss. The last stage is the classification process that is based on a model able to distinguish between normality and abnormality. This model is built over a set of traces where the corresponding traffic is either labeled as normal or as an attack within the different a priori known VoIP attacks.

The rest of the paper is organized as the following. Section 2 presents the different research works done recently to detect intrusions in VoIP networks. Section 3 discusses the principal components of our framework. Section 4 presents some intrusions that we investigated and developed to at-tack a real VoIP infrastructure. Section 5 depicts the environment of the different experiments we conducted and the different results obtained. Finally, Section 6 presents future work and concludes the paper.

[1]Corresponding Author

II. Related Work

Intrusion detection research for VoIP networks is currently at its infancy stage. In our knowledge, the research works done in this direction use the same basic methods implemented during the last three decades for detecting intrusions in the TCP/IP traffic.Some researchers use the same directions as those of the Snort IDS [9] which is based on a pattern matching technique that looks over packets' streams for recognizing pat-terns in the packet header and/or payload. Others use some classification techniques that consider statistical measures. In their initial form, these measures consisted in monitoringFor the first case, we cite the "Scidive" and "Spacedive" presented in [14]. These two basic systems are based on a simplistic correlation engine between the events of the signaling and the media stream protocol to detect a few types of attacks. They are also based on the Snort detection engine where only a simple extension is done for stateful and cross-protocol detections.

For the second case, a team in LORIA [7] uses the same method as that of Skinner and Valdes presented in [13] which is a Bayesian model called TCP EBayes. While TCP Ebayes uses only the TCP protocol to detect anomalies, the authors in [7] use the SIP protocol to detect the same basic anomalies as those targeting TCP such as syn flooding and port scanning. Therefore, instead of using the number of open TCP connections, the number of unique IP addresses and the number of unique ports as in TCP EBayes to detect port scanning and IP sweeping, the number of open RTP ports, the maximum number of waiting dialogs, etc. are used. There are many problems related to this technique. As an example, only bursts of traffic are considered as evidence of an anomaly. As a result, only the flooding at-tacks may be detected. In addition to this, the system was not experimented for the VoIP network case due to the lack of a real testbed. The original goal of the TCP EBayes is to detect abnormality; that is the detection is binary. This is not an appropriate method in particular for an overlay networks application where the administrator should be in-formed about the type of the attack for the next stage that consists in launching an appropriate counter measure.

Recently, the state machines are used to detect some intrusions in VoIP networks [12]. The proposed approach utilizes not only the state machines of network protocols but also the interaction among them. However, the different at-tacks tested by this mechanism are simplistic since there is no an in-depth study of the SIP protocol and almost all the defined attacks are launched by a third party. In an operational network, these attacks are hard to perform because of the different security mechanisms that are made in place by the telco operator such as those defined by the 3GPP [1]. However, these attacks are only possible in a LAN.

III. Systematic Framework

Since the different IDS techniques that are starting to come up with the emerging VoIP protocols are in their in-fancy stage or use the same vulnerable techniques as those implemented during the last decades on the classical IP net-works, we have to introduce novel techniques to detect the real intrusions that focus mainly on the new emerging VoIP protocols. In the following, we present a novel architecture that is able to detect anomalies and to correctly classify normal signaling traffic generated by the current VoIP net-works.

There is a variety of goals for this mechanism. First, it detects the whole a priori known attacks by an automatic learning. Second, it easily discriminates the different attacks and the safe VoIP traffic. Third, it recognizes new anomalies; those that are not learnt during the first step. These new anomalies may be due to the new vulnerabilities discovered and exploited by potential attackers. In addition, this system is a complete one since it not only detects attacks but also focuses on the relevant VoIP features that should be considered for the detection goal. Another dimension of this mechanism is that it not only uses a stateful detection technique but also looks at different protocols used for establishing and maintaining the VoIP communications.

Moreover, it generates statistical measures, corresponding to the different features, between the current packet (resp. transactions or dialogs) and the last packets (resp. transactions or dialogs) for the goal of VoIP intrusion detection. Finally, It is an extensible mechanism because it is able to learn the different classes of traffic (normal or attack) and adaptively consider new attacks and new normal forms by simple updates. It is also insensitive to IP spoofing and handles client mobility.

We mention that this mechanism is used as a first step before launching counter measures. Once the attack is detected, it sends to the corresponding reaction mechanism the different features that characterize the traffic that has caused the intrusion for appropriate counter measures.We notice that this mechanism is implemented either in a device or as a logical module placed in front of a user agent; be it a client or a server, or in front of a VoIP server

3.1Framework Architecture

The different components of the proposed system are depicted in Figure 1. The first part consists in defining a profile that corresponds to a set of attributes that summarizes a VoIP flow and catches the evidence of normality and anomaly.

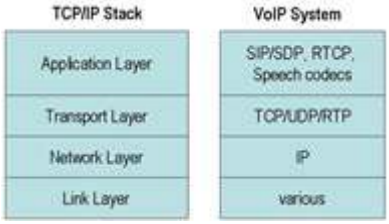

Figure 1. VoIP intrusion detection architecture.

3.2Dierent Components

The first step of the system consists in extracting the different attributes that characterize the different attacks and the normal network flows. These attributes are determined by using a set of known VoIP attacks based on SIP according to its specification (RFC 3261 [10]). We determine three different profiles that are used to characterize the SIP signaling flows. The first is the packet-based where each flow corresponds to a set of attributes extracted from packets and the different measures that correlate the current packet being analyzed with the previous ones. The second is based on transactions. A transaction, as defined in RFC 3261 [10], consists of a request that invokes a particular method, or function, on a server and at least one response. We note that SIP is based on an HTTP-like request/response transaction model. The third profile is based on a dialog. A dialog is a peer-to-peer SIP relationship between two user agents that persists for some time. The INVITE method is the only way defined in RFC 3261 to establish a dialog. The dialog-based profile corresponds to a session where not only signaling and description protocols are considered, but also RTP [11] and other protocols that are used for media transfer. The third profile is complementary to the cross protocol used by ”Scidive” [14].

Due to space limitation, we only present in the following the different experiments and results when considering the packet-based profile. The method does not differ between the three determined profiles. However, only the set of at-tributes is different from one determined profile to another.

Notice that a combination of these profiles by merging the three profiles into a single one containing the union of all attributes of these profiles may lead to another technique. Combining the different alerts generated by each profile may also lead to a new technique.M are fixed by experience. For instance, a period of 2 seconds is used for the time window and 200 flows preceding the current one are used for the other window. The intrinsic attributes can be defined to belong to a first class, the at-tributes related to the time window are defined to belong to a second class and the attributes related to a window of M flows are defined to belong to a third class. The attributes of the second set can equally be called expert knowledge attributes, since a security expert determines the attributes that belong to this set.At the transmitter; some selected audio packets are intentionally delayed before transmitting. If the delay of such packets at the receiver is considered excessive, the packets are discarded by a receiver which is not aware of the stenographic procedure.

The payload of the intentionally delayed packets is used to transmit secret information to receivers aware of the procedure, so no extra packets are generated. For unaware receivers the hidden data is “invisible”. LACK may be used in four basic scenarios illustrated in Fig. 4. In scenario (1), one packet is selected from the RTP stream and its voice payload is substituted with bits of the steganogram. In scenario (2) chosen packets are delayed by a certain time and then sent through the communication channel. In scenario (3), if an excessively delayed packet reaches a receiver unaware of the stenographic procedure, it is discarded. In scenario (4), if the receiver knows about the hidden communication, then instead of deleting the packet the receiver extracts the payload.

The second step of the proposed mechanism is the detection process that uses as input the profile extracted from the network flows as described above. Once the profiles are determined, the detection step could be thought of as a classification problem: we wish to classify each profile into one of a finite set of possible categories; normal, one possible.Attack type, or a new observation probably corresponding to a new attack. Given a set of profile records, where one of the features corresponds to the class label of the profile (i.e. normal, attack or new), classification and induction algorithms can construct a model that is able to summarize each category by using the most significative attributes to each category. Notice that it is also possible to use unsupervised classification techniques to classify the profiles.

A rapid growth has been noticed in various wireless technologies in recent years. This has resulted in an increase in demand for wireless data services and multimedia application such as VoIP, streaming audio and video [12]. In order to provide good service and to meet the user demands, research has been in progress both in wireless technologies and VoIP network system. VoIP is becoming more and more popular especially after the deployment of WiMAX network in many countries [13]. Different aspects of VoIP over WiMAX have been addressed by researchers. The authors in [14] have investigated the data and voice support in the WiMAX network. The aim of their work was to examine the QoS deployment over WiMAX network and compare the performance obtained using two different WiMAX services classes i.e. UGS and ertPS. The author in [15] has pointed out different factors like delay, jitter and packet losses and discussed how WiMAX network can deal with them. In [16], the authors have considered a fixed WiMAX network in order to evaluate the performance of VoIP.

They have measured the performance of different transmission schemes in term of cumulative good put, packet rate, sample loss rate and Mean Opinion Score (MOS) using R-score specified by ITU-T. In [17], the authors have proposed a traffic- aware scheduling algorithm for VoIP applications in WiMAX networks. They have studied the proposed mechanism is experienced using supervised classification techniques. In fact, a set of known attacks is played against a SIP user agent; may it be a server or a client. The corresponding flows generated from each attack are labeled with their appropriate attack type. The normal traffic is collected from a real world infrastructure of a telecommunication operator.

When training the classification model with a learning database containing a variety of attack and normal flows, a feedback from the detected attacks is used to improve the successful detection rate. As a matter of fact, if some at-tacks are not detected (false negatives) or some normal traffic is classified as an attack (false positives) then an expert is in charge to check whether other attributes should be considered, or this misclassification is due to the second stage (i.e. the detection model). The reason for taking other at-tributes into consideration consists in lessening the information and intrusion evidence loss when transforming the raw network traffic into a set of attributes. However, if the misclassification is due to the classification process then the classification technique should be tuned to increase the successful detection rate of the different tested flows belonging to the learning database, for instance.

3.3 Detection Models

In the proposed mechanism, we call a detection model the method that learns automatically the different samples present in the learning database. As a result of the learning step, a classification model is built with which new unlabeled instances are classified in their appropriate category (attack type or normal). If the corresponding class is an at-tack then an alert is generated, otherwise the flow is considered as normal. Since we use a learning database in which all flows are labeled in their appropriate class, we may use different supervised classification techniques for the task of the building process. There are many candidate techniques available in the data mining literature. In the following, we focus on decision trees induction algorithm as the technique for learning labeled flows and classifying new ones for the detection goal. However, any other supervised or unsupervised one may be used for this goal. For more details on decision trees, see for instance [6].

In Section 5.3, we give some examples of the decision tree obtained from the different experiments we conducted over the different attacks presented in Section 4.We note that the building process is done off-line while the detection process may be performed either on-line or off-line depending on the security policy of the information system.

IV. The Considered Attacks

SIP is widely used in VoIP systems and there are numerous attacks that can be performed against the SIP signaling protocol. The attacks are ranging from syntactical attacks; those that do not follow the SIP grammar provided by RFC 3261, to different denial of service (DoS) attacks in the overlay networks. Other attacks are the same as those that exploit known flaws such as buffer-overflows against servers. Only the attacks that affect directly the signaling protocol are investigated since the syntactical attacks and different flaws that are due to the programming errors have been widely investigated and current IDSs detect a variety of these attacks. In the following, different attack types corresponding to SIP attack scenarios are discussed. These at-tacks can be divided into three categories namely; information gathering, service theft and DoS.

In the following, we list representative attacks we investigated that we gather into the three categories. We give for each category its significance and some flow examples of the corresponding SIP attack Scenario. SIP directory scanning, QoS degrading are investigated but are not listed be-low due to space limitation.

4.1Information Gathering

Generally, an attacker has to perform many actions in or-der to achieve her malicious goal. These actions correspond to an attack scenario composed of many elementary attacks. Information gathering is one type of these elementary at-tacks, where the attacker may first collect information about the target server to get its version to check whether there is any known vulnerability to exploit. The attacker may also seek for some security credential variable variations such as nonce variation where the second step of this attack scenario might be a replay attack. Password guessing and directory scanning correspond to other information gathering attack types. For instance, the directory scanning attack, which involves checking for existing valid user identities in the registrar database, may be followed by a password guessing attack after a valid username was found.

4.1.1Nonce Variation Determining

According to RFC 3261 [10], SIP provides a stateless challenge based mechanism for authentication brought from HTTP authentication provided by RFC 2617. The “Digest” authentication is introduced in SIP for message authentication and replay protection only and without considering message integrity or confidentiality. One credential variable of this mechanism is the “nonce” that is used to compute the hash value of the authenticated response message using for example the MD5 hash algorithm. To check whether replay attacks are possible, the attacker may check if the nonce is changed for every authenticated message or it is renewed periodically, say for

instance once every second. In this last case, replay attacks remain possible.

4.1.2 Directory Scanning

This elementary attack consists in collecting valid identities corresponding to legitimate clients in the operator databases. It may be performed using different SIP message flows. It is considered as an information gathering attack since we only try to find valid URIs for a further malicious intention. It may be considered as the step that precedes another elementary attack such as identity theft by using a dictionary to guess the password of the identity that was discovered during this first stage. We should mention that this attack may be omitted particularly for those identities that are in the red list. In fact, the corresponding operators may add appropriate mechanisms for such lists. However, this attack is tested against many platforms of different operators and the experiments are successful.

Figure 2 shows a possible SIP scenario flow that may be used to perform this attack. According to the first messages exchange, a "401 Unauthorized" response is received when the identity corresponds to a known valid user whereas "403 Forbidden" is received in the other case. Therefore, an attacker may repeat this scenario and according to the response, she concludes whether the requested identity is

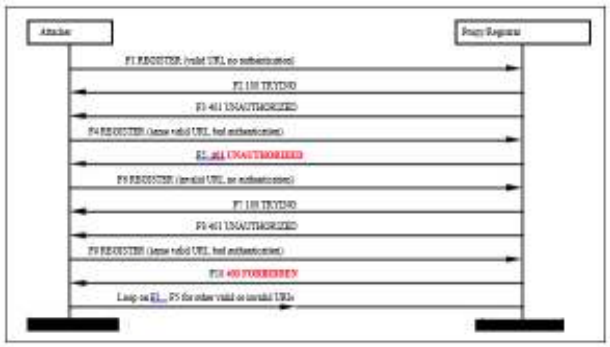

Figure 2. Directory scanning attack.

valid or not. This attack may be also performed using the OPTION request method. In fact, according to the response, one can know whether the corresponding URI mentioned in the "To" header field is valid or corresponds to an unknown user.

4.2 Identity And Service Theft

While the above attacks consist in collecting information about users and servers, this attack kind consists in stealing the identity of a legitimate user that either has mistakenly left his password unprotected for different reasons or an attacker has intentionally cracked his password by performing appropriate attacks such as those based on dictionary or moreover any brute force technique. Another kind of this attack type consists in using a service to which the user is not authorized or to which he is not subscribed.

Password guessing One well known attack uses a dictionary to find out a user password, or a brute force technique by exploring a large number of possibilities. There-fore, an attacker may use a series of passwords for a specific identity, discovered during the last stage. She may succeed to discover the correct password of this entity in particular when the corresponding user has not chosen an appropriate password.

4.3Denial Of Service

The DoS attack is a technique that is largely used since the introduction of computers. Its goal is to make a tar-get resource unavailable to its legitimate users. This kind of attack can be divided into two categories. The first one is based on the flooding DoS whereas the second one involves sending a malformed packet that causes the end-point to crash. When performing the DoS attack, an atacker can send a huge number of successive REGISTER requests against a registrar or many INVITE requests to a target client. On the other hand, an attacker may follow the dialog when sending the INVITE to a legitimate client and can stop the flow of the SIP signaling by sending a BYE re-quest just after he receives the OK response from the target client.

4.3.1DoS Against A Server

A DoS attack against a server is a flooding attack that involves sending a non restrictive number of requests against a server such as a registrar. This type of attack may be also extended to a distributed DoS (DDoS) attack where the attacker recruits many zombies over the Internet and each compromised machine sends huge numbers of such legitimate requests.

4.3.2DoS Against A Legitimate Client

When performing a DoS attack against a legitimate client, an attacker tries to disturb a legitimate client based on continuous INVITE requests without establishing the call since the attacker cancels the call each time the user answers the request.

V. Experiments

5.1The Environment Setup

We participate in the French Oscar project that aims to detect anomalies in overlay networks with France Telecom group as a partner. We were provided with a tcpdump traffic of 2 hours collected from an operational testbed. The collection was done downstream of an SBC (Session Border Controller). This collection was done in November 2006 where approximately 1640 clients used the VoIP SIP testbed during this period. The result after filtering the tcpdump collection and keeping only the traffic corresponding to SIP and RTP protocols consists of about

200 MBytes for each hour. We manually and meticulously analyzed all the packets corresponding to the SIP protocol and found that there are some syntactically malformed SIP packets according to the SIP grammar provided by RFC 3261 [10]. We filtered the corresponding packets since we do not consider this at-tack kind as explained in Section 4. We then assumed that the filtered collection is free from signaling attacks and con-ducted our experiments by injecting the attacks described in Section 4 into the collected set. In fact, we implemented a tool that behaves as a user agent client that launches different attacks, against a VoIP overlay network infrastructure using SIP as the signaling protocol, that are presented in Section 4.

We used the first data set corresponding to the first hour as a learning dataset after having peppered it with attacks that are launched against the operational infrastructure. No-tice that there are machines that are connected to this infrastructure playing the role of attackers. The different attacks that are launched against the infrastructure are successful. As for example, the nonce variation of the proxies and registrars present in the infrastructure is determined and some users indentities are discovered.

The second dataset corresponding to the second collection hour was used as a test data set. For this case, we also launch SIP attacks against the operational infrastructure.

We note that some attacks that are launched during this phase are new; i.e. they are not present in the first data set. The goal of restricting the presence of new attacks in the new data set is to evaluate the efficiency of the detection model towards new attacks.

5.2 Data Pre-Processing

Raw tcpdump traffic collected from a monitored network is not appropriate for a direct use by the detection models. Therefore, a transformation function, which transforms the raw traffic transformation into attributes records without in-formation and intrusion evidence loss, is used to generate well formed data as input for the detection models. At-tributes extraction, as described in Figure 1, summarizes VoIP raw traffic into attributes records. Each SIP signaling flow is transformed into a record composed of different attributes extracted from the raw flows according to the procedure presented in Section 3.2. We give in the following paragraphs a description of the two attributes types namely; intrinsic and expert knowledge attributes. Intrinsic attributes are grouped into a class that we call “first class” and the other type corresponding to the different attributes computed according to the last flows preceding the current one.

Table 1. First Class Attributes List.

Attribute	Description
SCN	The value of the status code if it is a response (200, 180, etc.) else it is set to “NULL”
Reason Phrase	The reason phrase informed from the response (OK, UNAUTHORIZED, etc.)
Method	The value of the method informed from the request (INVITE, REGISTER, etc.)
From URI	It corresponds to the logical initiator of the request informed in the “From” header field
To Tag	The value of the tag parameter informed in the “To” header field. It is used to follow a dialog between two UAs
UserName	This corresponds to the credential value of the username parameter specified in the “Authorization” header field
Nonce	It corresponds to the credential value of the nonce parameter specified either in an “authorization” header field or in the “WWW-Authenticate” header field
Response	This corresponds to the response parameter specified in the “Authorization” header field as a response to the challenge

We mention that the different attributes presented in Table 1 are intrinsic; others are extracted by considering known attacks. As an example, the last three attributes preceding the current one using the different attributes values indicated in the first class.

A time window of N seconds (2 seconds for instance) is used for this purpose. These attacks are relevant for VoIP DoS flooding attacks and other attacks that send the same requests with different values such as password guessing or nonce variation. The different attributes of this class are automatically constructed and are summarized into the “Same To-URI” attributes that examine the flows in the last

N seconds that have the same logical recipient as the cur-rent flow. We note that the logical originator is not taken

into account to calculate the different attributes in order to avoid URI spoofing where an attacker may forge a “From URI” header field. However, in a real world, the provider of the service may use ingress filtering and in this case, we may consider the logical initiator of the flow. Since this is not always the case, we do not use it here and consider all possible situations.

Third class A novice attacker may send many requests in a short time window. The second class attributes is sufficient enough to detect the corresponding attack. However, other attackers will take then time and use stealthy techniques to bypass this approach. Therefore, a larger time window to detect these attacks is needed to detect. For this reason, we introduce the third class that considers the last M flows (M = 200 for instance) preceding the current one to calculate the corresponding attributes. The attributes of this class are calculated according to the last M flows preceding the current one.

VI. Results

We conduct different experiments over the two data sets presented in Section 5.1. We trained our algorithm over the first data set presenting the first collection hour that contains different attack types as those presented in Section 4. We notice that there are new attacks which are only present in the test data set that corresponds to the second hour of col-lection. These new attacks correspond to the DoS against These rules have many advantages in detecting anomalies in signaling flows. Since the rules have the "IF

... THEN ..." format, they may be used as a model for a rule based intrusion detection system. Moreover, a VoIP security expert may assess the different rules and can add, delete or modify some of them if needed.

Using the ruleset generated by the training data set, new flows are examined by checking the different rules for a match. If there is none rule that matches then the flow is considered as new and should be examined to check whether it corresponds to a new attack. If so, we examine the corresponding traffic and if it corresponds to a new attack, we re-inject its traffic in the learning data base to generate its corresponding rule.

The successful detection rate is over 99% by applying the different rules on the training data set. This result means that the different attributes that are determined during the extraction step efficiently characterize the different flows and differentiate between the different attack classes and the normal traffic.

.However, the last attack is tested in our local infrastructure. Some rules that are generated automatically from the training data set are given in Table 2.Table 3 gives the different detection rates of the different classes (normal and the different attack types) in the test data set.The old intrusions correspond to those attacks that are present in the training and test data sets. There only two new attacks that are present only in the test data set. The first is the nonce variation determining attack and the second is the DoS against a client attack. While the nonce variation

Rule	Meaning
Method= REGIST ER, diff username rate < 0:1% >class guesspassword	If the method is REG-ISTER and the diff diff username rate is less than 0:1% then this flow is a password guessing attack.
Default: New	If none of the rules matches then the current flow to a new network and momentarily considered as a new attack.

We have also used Snort to detect these attacks. We con-figured it with the latest rules. None of the attacks cited above are detected by Snort since all the packets of the two data sets are well formed and there is none rule in the Snort database that corresponds to any of the attacks cited above. In addition, it is very hard to write the corresponding Snort rules because pattern matching techniques are not appropriate for this kind of attacks.

VII. Conclusion

In this paper, we introduce a framework for detecting anomalies in signaling flows related to the SIP protocol targeting the VoIP networks. The main idea behind our proposal is the attributes extraction from the signaling flows that highly characterize attacks and differentiate between normality and abnormality in a VoIP environment. To take into consideration new VoIP attacks, our mechanism con-siders new attributes that are relevant for characterizing them. A feedback from new attacks contributes to extend the ability of this framework in detecting other attack variants and new ones.The different experiments show that our mechanism issuccessful to detect almost all known attacks and new ones collected in a real tested.

References

[1] Zander S., Armitage G., Branch P., A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials, 3rd Quarter 2007, Volume: 9, Issue: 3, pp. 44-57, ISSN: 1553-877X

[2] Petitcolas F., Anderson R., Kuhn M., Information Hiding – A Survey: IEEE Special Issue on Protection of Multimedia Content, July 1999

[3] Murdoch S.J., Lewis S., Embedding Covert Channels into TCP/IP. Information Hiding (2005) 247-26

[4] Szczypiorski K., HICCUPS: Hidden Communication System for Corrupted Networks. In Proc. of: ACS'2003, October 22-24, 2003 Międzyzdroje, Poland, pp.31-40

[5] Servetto S. D., Vetterli M., Communication Using Phantoms: Covert Channels in the Internet. In Proc. of IEEE International Symposium on Information Theory, June 2001.

[6] Birke R., Mellia M., Petracca M., Rossi D., Understanding VoIP from Backbone Measurements, 26th IEEE International Conference on Computer Communications (INFOCOM 2007), 6-12 May 2002027-35, ISBN 1-4244-1047-

[7] Choi Y., Lee J., Kim T.G., Lee K.H, Efficient QoS Scheme for Voice Traffic in Converged LAN, Proceedings of International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'03), July 20-24, 2003, Montreal, Canada.

[8] Miloucheva I., Nassri A., Anzaloni A., Automated Analysis of Network QoS Parameters for Vo

[9] Bartoli M., et al., Deliverable 19: Evaluation of Inter-Domain QoS Modelling, Simulation and Optimization, INTERMON-IST-2001-34123

[10] Schulzrinne H., Casner S., Frederick R., Jacobson V. - RTP: A Transport Protocol for Real-Time Applications, IETF, RFC 3550, July 2009

[11] Adhicandra, "Measuring data and voip traffic in wimax networks," Arxiv Preprint arXiv:1004.4583, 2010.

[12] Tucker, E. 2006. Can voice be the killer App for WiMAX Available from: http://www.openbasestation.org/Newsletters/November2006/A perto.htm [Last Accessed on 15th March, 2012.

[13] K. Pentikousis, E. Piri, J. Pinola, F. Fitzek, T. Nissilä and I. Harjula, "Empirical evaluation of VoIP aggregation over a fixed WiMAX testbed,"