A Distributed Infrastructure to Analyse SIP Attacks in the Internet

Adnan Aziz, Dirk Hoffstadt, Erwin Rathgeb
University of Duisburg-Essen
Institute for Experimental Mathematics
Ellernstraße 29, 45326 Essen, Germany
{adnan.aziz,dirk.hoffstadt,erwin.rathgeb}@iem.uni-due.de

Thomas Dreibholz
Simula Research Laboratory
Network Systems Group
Martin Linges vei 17, 1364 Fornebu, Norway
dreibh@simula.no

***Abstract*—VoIP systems, based on the Session Initiation Protocol (SIP), are becoming more and more widespread in the Internet. However, this creates security issues and opens up new opportunities for misuse and fraud. The most widespread threat are multi-stage attacks to commit Toll Fraud. To devise effective countermeasures, it is crucial to know how attacks on these systems are performed in reality.**

In this paper, we introduce a novel distributed monitoring system with Sensor nodes located in Norway, Germany and China that allow to detect SIP-based attacks from the Internet. Based on experiences from experiments spanning several years, we propose a new setup which allows simple and straightforward addition of new remote observation points. We have deployed this setup in the NorNet testbed and highlight its advantages compared to a previous setup with physically distributed Sensors. We also present results from a 45 day field test with 13 observation points. These results confirm the advantages of a widely distributed monitoring setup and give some new insights into the behavior of the attackers.

Keywords—VoIP; SIP; STR; misuse; fraud; security; Honeynet; Honeypot; Sensor; Nornet; Toll Fraud; misuse detection

I. INTRODUCTION

Voice over IP (VoIP) communication based on the Session Initiation Protocol (SIP) [1] has evolved as de-facto standard for voice communication. Therefore, support of open IP-based interfaces becomes increasingly important. VoIP is subject to the fraud schemes known from traditional telephony services as well as those known from today's Internet as VoIP blends these technologies. In addition, VoIP opens up new opportunities for misuse and fraud. SIP servers, particularly if they allow access from external networks, are subject to fraudulent registration attempts (known as Registration Hijacking, see Section II) as a prerequisite for calls via compromised SIP accounts. This is extremely attractive for attackers, because they can gain immediate financial benefit by making toll calls (international, cellular, premium services) via third-party accounts. This attack is called Toll Fraud and can cause the account owner substantial financial damage in a very short time. Another strong motivation for such an attack is to obscure the identity of the caller by using a compromised third party account.

To develop effective countermeasures, it is important to know how these attacks are launched in reality. For gathering the required data, we have developed a specialized SIP Honeynet System [2] that has been running since January 2009 and has recorded over 147 million SIP messages. To gain a more global view of the attacker behaviour, we have subsequently developed and evaluated a distributed Security Sensor System [3] allowing attack monitoring in real-time. This system provides distributed, rule-based attack detection by using passive, lightweight Security Sensors installed at different locations in the Internet which send their attack reports to the Sensor Central Service (SCS) server where they are correlated and evaluated.

Based on the experiences with the deployment of this Security Sensor System we now propose a novel setup option where the sensor logic is centralized and collocated with the SCS. This new approach ("Central Sensor") solves many of the deployment obstacles as it only requires tunnelling of SIP traffic from the remote observation points instead of installation of hardware or software there. We have deployed this new Central Sensor concept by using the capabilities provided by the new NorNet [4] research platform where we could already establish thirteen observation points in Norway, Germany and China with very limited effort. With new sites and interfaces added to NorNet – or by extending the setup to other networks – we can easily extend the coverage of our monitoring system.

This paper is organized as follows. The second section includes an overview of SIP fraud and misuse, followed by a discussion of related work in section three. The fourth section discusses the SIP misuse detection system and section V gives details on the NorNet packet forwarding infrastructure. In Section VI we present the first analysis results and findings from the new approach.

II. SIP-SPECIFIC MISUSE

SIP is used to establish sessions (e.g., voice, video) between two user-agents with the user-agent providing the interface with the user, typically by means of specific software (soft phone). For the purpose of this paper, the following SIP message types are relevant: If a user-agent (i.e., SIP device) wants to establish a call via a voice server, it first has to register at the server by sending a REGISTER message with credentials (account name and password). If the extension (SIP account) given in the REGISTER message exists and the password is

ISBN 978-3-901882-58-6

correct, the server acknowledges with a 200 OK message. Else, the SIP server either responds with a 401 UNAUTHORISED message if the password is empty, with a 403 FORBIDDEN message if the password is incorrect or with a 404 NOT FOUND message if the account does not exist. OPTIONS messages allow a user-agent to query a server's capabilities. To ensure that this communication is always possible, the SIP standard specifies that all user-agents must support OPTIONS messages. To finally exploit a third party SIP extension, typically four distinct attack stages are performed [2]:

1. SIP Server & Device Scan

The SIP protocol requires every SIP device to answer SIP packets within a specified time interval. An attacker can use this behaviour to "ping" any single IP address or whole subnets with e.g., OPTIONS packets to identify SIP devices. Even if a user-agent's SIP stack implementation is not standard-compliant and replies only to OPTIONS packets of well-known sources, a scan is nevertheless possible: In this case, the attacker can use REGISTER requests.

2. Extension Scan

To identify active user accounts of known SIP servers, the attacker tries to register at several extensions without using credentials. If the extension exists, the server answers with a 403 FORBIDDEN, because no password is given. If it does not exist, a 404 NOT FOUND is typically returned. The result of this attack stage is a list of existing provider accounts.

3. Registration Hijacking

To register at a given extension, the attacker tries to guess the password. This results in sending a sequence of – possibly very many – REGISTER messages with different passwords to a selected extension. If the password is guessed, the information is stored to register at this extension later on.

4. Toll Fraud

The term "Toll Fraud" is used if a person generates costs (toll) by misusing the extension of another person. In this case, an attacker has already successfully hijacked an extension and uses it to make calls. In terms of SIP messages, the attacker first sends a REGISTER message with the correct password. After the 200 OK message from the server, the attacker can initiate calls by using INVITE messages.

The first three stages mentioned above can be executed by using freely-available tool suites. A common white-hat attacking tool for SIP is the open source tool suite Sipvicious [5]. If not modified, Sipvicious identifies itself as user-agent "friendly-scanner".

III. RELATED WORK

In [6], an Intrusion Detection System (IDS) has been built to detect SIP attacks. This system is based on the Low Interaction Honeypot presented in [7]. The IDS detects DoS (Denial of Service) and Call attacks by working with a security event correlation system. The Honeypot is capable of retrieving fingerprint information by interacting with the attacker.

In [8] Valli has performed a statistical analysis of VoIP attacks over the real attack traffic captured via a Honeynet system consisting of several virtualized Low Interaction Honeypots. These Honeypots have logged the target traffic to a file, over which an analysis was performed. The results have shown that primarily Sipvicious is used as a tool. Also another tool called sipsscuser is found. Its behaviour is found similar to a worm or a botnet.

In [9] a system for analysing malicious VoIP traffic based on High Interaction Honeypots is presented. A Honeywall [9], a host between the Internet and the Honeypots, is used to monitor the connected Honeypots and to capture incoming attack traffic to pcap files. Moreover, the NIDS Snort generates alerts based on predefined rules. This system is used for some basic statistical analysis at two locations [10]. In [11] the authors have enhanced their Honeypot System to monitor Toll Fraud calls with real Public Switched Telephone Network (PSTN) access. Also further statistical analyses based on number of packets, country of origin and the attacker's user agent are provided for a time period from August 2011 until December. 2012.

The Honeypot system in [9], [10] and [11] uses only a few Honeypot hosts monitored by the Honeywall which provides the monitoring mechanism and has to be protected against attacks from the Internet. In contrast to the above mentioned approach with only a few Honeypot hosts, we implemented the SIP Trace Recorder (STR) [12] to passively monitor the network traffic for complete subnets by using a router's monitoring port. In our lab environment, it monitors two class C subnets with publically available virtual Honeypots [2]. This allows a more comprehensive view of the attacker's behaviour (e.g., scanning behaviour of a subnet). The captured SIP traffic is stored into a central SQL database to perform comprehensive offline analysis. Due to the passive connection via a monitoring port, our STR is not reachable from the Internet. Our Honeynet system is up and running since December 2009.

Moreover, analyses in [10] and [11] are based only on individual SIP messages. Due to the fact that the attack stages 2 and 3 both use REGISTER messages, a comprehensive evaluation is not possible based on the number and type of SIP messages only. Moreover, different attack variants of the same stage use a different number of SIP messages. To automatically identify the different attack stages and their variants, we combine the corresponding messages to attack clusters by allocating SIP messages based on their source IP address, attack stage allocation and timing [2]. Furthermore, our analysis of the SIP traffic in a Honeynet has revealed that attacks in SIP-based networks show specific message patterns that can be used for detection.

However, to analyse the attacker's activities more comprehensively, it is necessary to increase the area under observation to have a more global view of the attack behaviour. In [13], the architecture of distributed Honeypots with predefined software images is presented. The attack information at the remote locations is pre-processed and stored

in the Dionaea [14] database before periodically forwarding it to the central server for final analysis. The proposed distributed approach requires the installation and maintenance of hardware and software with high resource usage at the remote locations. Our attempts to deploy heavy-weight monitoring solutions as described in [9], [13] at locations outside our labs revealed low acceptance due to the high installation, resource and management effort for the hosting organization and also due to privacy concerns. To cope with these concerns, we designed a first version of the distributed Sensor Security System [3] where light-weight Sensors for signature-based detection are installed on remote hosts and send alarm reports to a central service. We have installed four Sensors at different partner organizations in Germany since November 2012, and we received over two million reports so far by using simple signatures for multi-stage Toll Fraud attacks. A first analysis showed that many IP addresses were detected by all Sensors indicating that the aggregation of distributed Sensor information is actually beneficial [3].

Based on the practical experience with the deployment of this system, we developed the approach described in this paper which further reduces the requirements for the organizations hosting observation points by centralizing the more resource and maintenance intensive components in out lab. In cooperation with NorNet and Hainan University in China we could deploy 13 observation points already and are trying to extend the monitoring network continuously.

IV. SIP Misuse Detection System

A. Overview

In 2009, we implemented a VoIP Honeypot [2] component based on a standard Linux virtual machine with a specially-configured open source VoIP PBX Asterisk [15] server and extended logging functions to analyse the SIP attack behaviour in detail. This machine accepts incoming SIP requests on port 5060 and acts as standard SIP-based server. We configured four SIP accounts with weak passwords to lure the attacker. In this case only the Honeypot is monitored. Since then, we added other components to the system which are shown in Fig. 1 in a typical setup. In addition to the STR, we also implemented a light-weight Security Sensor [16] that can be installed on different hosts in the Internet to analyse the SIP attack traffic in real-time. There is a variety of deployment options like, e.g. software, a virtual machine or a specific hardware (e.g., Raspberry, ALIX). The Security Sensors detect an attack based on pre-defined signatures.

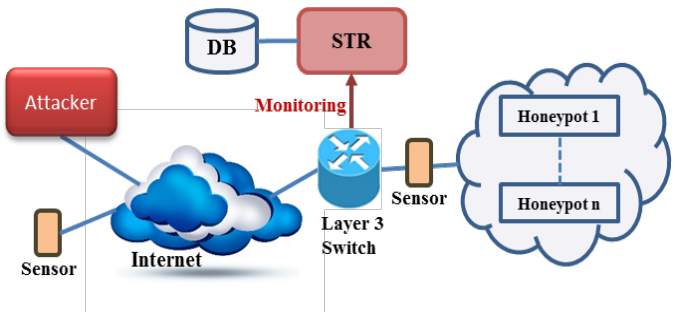

Fig. 1. SIP Misuse Detection Network Architecture

Based on our STR database, we defined attack signatures for the different stages of a Toll Fraud attack as explained in Section VI. If a rule matches, the Sensor generates an alarm report which is logged on the Sensor host. This approach does not require packet recording and therefore, no database installation. This also solves the highly critical data privacy issue in productive environments as no personal information of legitimate users has to be recorded. On the other hand, detection accuracy is potentially lower than with the STR where an offline analysis of all relevant traffic can be performed as it depends on the granularity of the detection rules.

Manually collecting and aggregating the reports from various remote sites is not feasible. To solve this problem, the Sensor Central Service (SCS) was implemented (to be explained in Section IV.B). It collects the report information from each Sensor, aggregates these reports and can also send alarm messages to mitigation components being able to take action against the attacker [3]. The SCS also performs remote configuration and updating of the Sensor rules.

The sites where STR or Sensor components are deployed also require a Honeypot installation if no SIP server is present in the network in order to provoke the attack stages beyond the server scan. Therefore, Sensor deployment means that our third party software and some tools like libpcap and boost libraries along with a standard Linux implementation have to be configured, maintained and updated. This has shown to be a major obstacle for widespread deployment of the Sensors as every organization hosting a Sensor has to be approached separately and also has to continually contribute to the maintenance effort. Ideas to use open testbeds, e.g. PlanetLab, to deploy the software Sensors failed because the testbeds don't provide users with the privileges and exclusive access rights required for the Sensors.

With the introduction of the NorNet testbed [4] (to be explained in Section V), a new opportunity opened up to cope with these issues and to make the deployment and maintenance process more efficient. In the novel approach presented here only one central Sensor combined with a Honeypot receives SIP attack traffic collected from different NorNet nodes distributed all over the Internet. The NorNet nodes are light-weight with a standard Linux implementation. They forward the SIP attack traffic to the Central Sensor using GRE tunnels. The Honeypot at the central location responds to these requests via the same tunnels. The routing tables to forward requests from distributed sites to the Central Sensor and back to the attacker are handled by the standard Linux implementation so only configuration but no installation of additional software at the remote nodes is necessary.

This new concept will also significantly reduce the inhibitions for hosting observation points in other networks. The bandwidth required for the tunnelling approach is higher than for the distributed Sensor approach because all SIP traffic has to be redirected to the central site instead of only forwarding aggregated reports. Due to the relatively low traffic volume of SIP signalling, this would only become an issue for a really high number of observation points in combination with low access bandwidth at the central point. Both central and

distributed approaches use the SIP misuse detection components (Sensor, SCS and Honeypot). In the following subsections only we present a short overview of these components as they have already been described in detail in [3].

B. Security Sensor Component

The Sensor is a light-weight software used for rule-based SIP misuse detection. It is written in C++ using the libpcap [17] and boost [18] libraries. The Sensor component is designed to run on different devices and uses the resources of the hosting device. The attack detection and reporting by the Sensor component is divided into the three phases Listener, Analyser and Action, as shown in Fig. 2.

The Listener module receives the SIP traffic by filtering out other protocols' traffic. The input SIP traffic is enqueued to a FIFO queue which is shared between Listener and Analyser module. The Analyser is the main module of the Sensor component. It dequeues the SIP data from the shared queue and parses it using a SIP parser. It checks for the start-line and some particular header values by using regular expressions. If the header start-line or header values are incorrect or missing, the packets are simply dropped. The parser returns the SIP header values as objects which make the comparison of header values very easy. The Analyser retrieves the detection rules in XML format from the Sensor Central Service (SCS) as described in Subsection IV.C. A rule defines a sequence of particular messages with a time constraint. The Analyser compares every received SIP message to every rule. The Analyser deletes irrelevant messages. A rule is matched if a number of messages are successfully compared according to the predefined sequence in a specified period of time. The Action module takes an action on successful matching of a rule. The simplest action is to log information of every matched rule. Another action is to inform the SCS which aggregates the reports from different Sensor components and then takes some action.

C. Sensor Central System (SCS)

The SCS is responsible to configure the deployed Sensors, update rules and also to perform some management functions like stopping, restarting and updating the Sensors. Multiple instances of Sensors are attached to the SCS via the Internet as shown in Fig. 3. A main task of the SCS is to aggregate and correlate the attack reports received from the individual Sensors to get more information about attackers and attack behaviour.

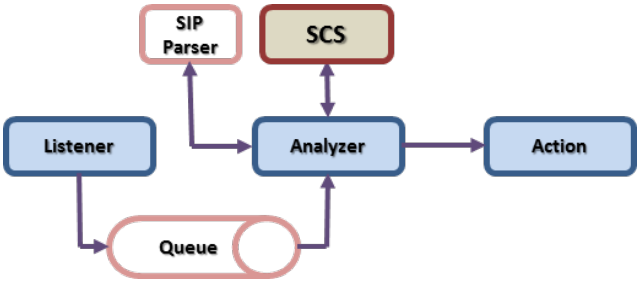

Fig. 2. Sensor Architecture

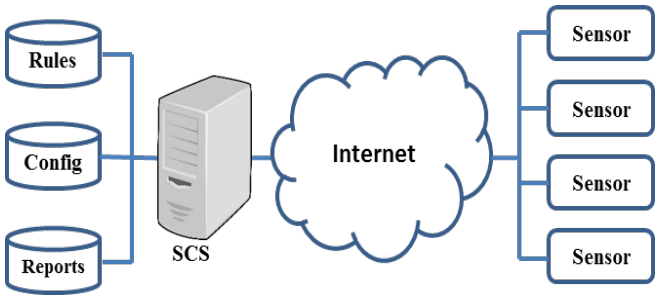

Fig. 3. SCS Architecture

The SCS and Sensors communicate via a HTTPS-based interface. The Sensor acts as a client only and communicates with the server using XML messages exchanged via persistent HTTPS connections. The server identity is guaranteed by using an own Certificate Authority (CA). Furthermore, the Sensor authorizes itself by sending a sensor ID and a secret with every request. HTTPS keep-alive allows to keep the connection persistent over a long time period.

D. Honeynet System

Our VoIP Honeynet contains four High Interaction SIP Honeypot modules with different public IP addresses that act as regular SIP proxy servers. The Honeypots are virtual machines, which make it easy to set up further SIP components at any time. The extended High Interaction VoIP Honeypot component [16] is a standard Linux virtual machine with a specially configured open source VoIP PBX Asterisk [15] server and extended logging functions. This machine accepts incoming SIP requests on port 5060 and acts as standard SIP-based server. All requests are answered according to the SIP standard. This active component is necessary to analyse the whole multi-stage attack chain. For example, the attack tool Sipvicious [5] begins with an SIP OPTIONS scan and normally continues with a REGISTER scan only if it receives a reply from the target host. If there is no reply, the tool proceeds with the next host in the network and the next attack stage is not triggered. We have configured the same four SIP accounts with weak passwords (i.e., password identical to account name) on each Honeypot. So a potential attacker can easily misuse one of these Honeypot accounts. After a successful Registration Hijacking attack, the attacker is able to establish simulated outgoing calls (Toll Fraud). The dialled number is redirected to an internal account, but the call is not accepted. This behaviour is necessary to log the outgoing telephone numbers and to simulate the call establishment for the attacker. The fake call is terminated by the Honeypot System after 10 seconds, and there is no real call switching to the Public Switched Telephone Network (PSTN). The whole process is logged by the STR and it is possible to analyse all stages of an attack.

In order to check for the performance, we have deployed Sensors on low performance (Raspberry Pi[1] and FRITZ!Box[2]) and high-performance devices (PC and Virtual Machines). The Central Sensor we are using is running on a Virtual Machine (VM) with 1 Gbit/s link and sufficient hardware resources.

[1] Raspberry Pi: http://www.raspberrypi.org/
[2] FritzBox: http://www.avm.de/de/Produkte/FRITZBox/index.php

Thus the performance of the Central Sensor is very high with zero packet loss.

V. The NorNet Central Sensor Setup

In order to observe SIP attacks at different sites, it is necessary to forward SIP packets to a Sensor/Honeypot – and generate packets in response – at many different locations within the Internet. However, these tasks require special permissions (particularly, exclusive access to the SIP well-known ports) and are therefore not easily possible with testbeds like PlanetLab [19]. We have therefore utilized the new NorNet testbed infrastructure.

A. The NorNet Research Testbed

The NorNet research testbed [4] is a distributed testbed infrastructure with systems distributed all over Norway as well as several international locations. NorNet consists of a 3G wireless (denoted as NorNet Edge [20]) as well as a wired part (denoted as NorNet Core [21][23]). For our SIP analysis, NorNet Core is of most interest for us, since its systems have unrestricted Internet access and are therefore exposed to attacks from the Internet.

NorNet has been established for research on multi-homed systems. Its sites are therefore connected to multiple Internet service providers (ISP) simultaneously. Particularly, multi-homing requires rule-based routing, i.e. routers apply multiple routing tables. The actual table used for routing a certain packet is then selected by configured routing rules. Therefore, NorNet already provides the necessary infrastructure for routing rule configuration.

B. NorNet Core

A NorNet Core site consists of several research systems that are connected to the Internet – via multiple ISPs – by a router called "tunnelbox". A tunnelbox takes care of routing packets among NorNet Core sites via tunnels over different ISP combinations. Some more information as well as the technical details are provided in [21], [22]. Since the tunnelboxes are equipped with public IPv4 addresses, they could – in theory – also run SIP honeypot Sensors as an additional service. However, this would imply the need for super-user permissions on the tunnelboxes (a security as well as stability threat for the whole research testbed) and possibly affect the routing performance (a problem for other users of the testbed). We have therefore designed a more advanced solution.

C. Packet Forwarding for the SIP Honeypot

Our NorNet-based SIP Central Sensor approach is illustrated in Fig. 4. The SIP honeypot server for all NorNet Core sites, the central Sensor and the SCS are located at the University of Duisburg-Essen. This single server is therefore easy to maintain, since it is just a dedicated virtual machine at our local site. Particularly, we have also full control over its configuration and resources. Also, possible problems with the server do not affect the tunnel boxes.

However, all attack traffic has to be forwarded from the remote tunnelboxes to the honeypot server, and all responses have to take the same way back to the attacker. This is achieved as in the illustrated example:

- The attacker performs a SIP attack on the external IP address of ISP 1 on Site 1 (denoted as ISP1_external), i.e. the tunnelbox of Site 1, by sending a SIP packet (e.g. a SIP Registration message).
- The tunnelbox performs Destination Network Address Translation (DNAT), i.e. it translates the SIP packet's destination address to an internal address (denoted as Honeypot_Site1_ISP1_internal). This private IP address belongs to the SIP Honeypot and uniquely identifies the tunnelbox's specific interface (i.e. ISP1_external in this case). We denote this interface as probe interface. The DNAT rule also filters the traffic of interest; in our case: UDP and TCP packets to port 5060 (i.e. the well-known SIP port).
- For each probe interface, there is a Generic Route Encapsulation (GRE, [24]) tunnel between the corresponding tunnelbox and the SIP Honeypot. The private addresses of the SIP Honeypot can be reached via this tunnel. That is, after DNAT, the attack packet is forwarded over the corresponding tunnel directly to the SIP Honeypot. All tunnels between a site and the SIP Honeypot use the same ISP, the so-called default ISP. This is the ISP that is used for all management traffic, i.e. it has the best connectivity. In the example, this is ISP 2 for Site 1.

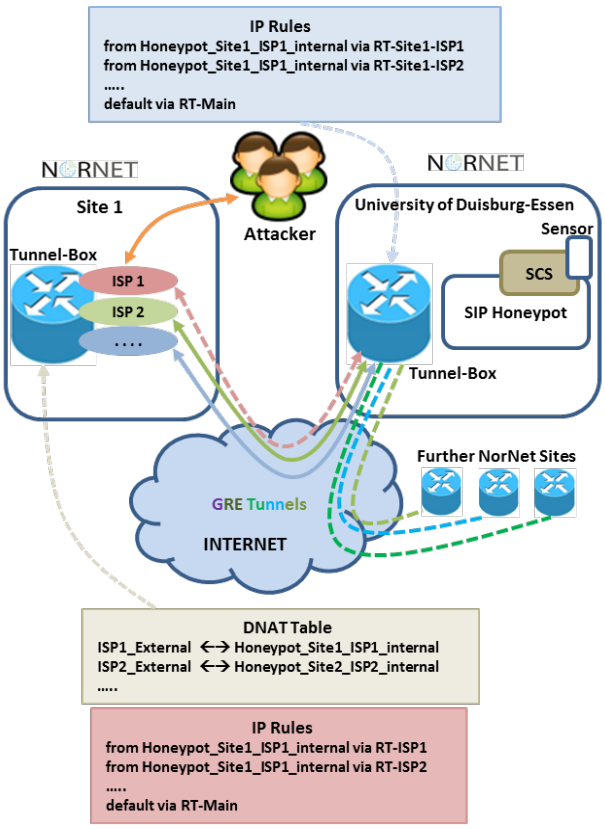

Fig. 4. NorNet Central Sensor Approach

- Each GRE tunnel is terminated at the SIP honeypot. We denote these tunnel endpoints, which are configured with the private IP addresses, as probe endpoints. The attack packet reaches the endpoint with the address Honeypot_Site1_ISP1_internal. Here, it can just be handled as a "normal" incoming SIP packet by the software. The software may then send a response back, i.e. from Honeypot_Site1_ISP1_internal to the attackers address.
- Of course, the response has to be forwarded via the original interface. Therefore, a routing rule is necessary to put all traffic from Honeypot_Site1_ISP1_internal into the tunnel to Site 1 for ISP 1, by applying the corresponding routing table (here named RT-Site1-ISP1) by using an appropriate routing rule. The response then gets forwarded to the tunnelbox of Site 1.
- At tunnelbox of Site 1, a similar routing rule ensures that traffic from Honeypot_Site1_ISP1_internal is routed via the default routing table of ISP 1 (here named RT-ISP1) by again using a routing rule. Before leaving the router, the DNAT rule finally replaces Honeypot_Site1_ISP1_internal by ISP1_external. The response reaches the attacker. For him, the response looks like it would come from the tunnelbox of Site 1.

VI. RESULTS

We have deployed the Security Sensor System to analyse the SIP attacks at different locations in the Internet. In this paper we have considered two approaches (distributed and central). For the distributed approach we have installed Sensors in Berlin, Munich and Essen in Germany, which monitor the company's network. For our central approach one centralized Sensor is deployed in our lab, which collects SIP attack traffic tunnelled there from different NorNet nodes located in Norway, Germany and China. These nodes are not only geographically apart from each other but there is also a reasonable distance among the IP addresses (ranging from 77.0.0.0 to 210.0.0.0).

The STR [12] analysis of SIP attack traffic has identified the scan behaviour for different stages of a multi-stage Toll Fraud attack. On the basis of this information we have defined three simple XML-based rules for Server Scan, Extension Scan and Registration Hijacking. The rules for Extension Scan and Registration Hijacking are same in both approaches. However, the rule for the Server Scan is different in the central approach. Normally, the Server Scan is detected if an attacker sends OPTIONS packets to multiple destinations in a subnet. In the central approach only one IP address is monitored, and a scan is considered as Server Scan if an attacker sends at least two OPTIONS packets to different NorNet nodes.

In order to check the detection accuracy of the rules we have also captured the attack traffic with the help of the STR. Further we have performed offline analysis on the captured attack traffic to check for false-positives and false-negatives. We have observed some attacks in the captured data which were not detected by the Sensor due to timing conditions. Therefore, we optimized the existing attack signatures for the new attack behaviour.

To evaluate the results for the NorNet scenario we have taken a time period of one and a half month i.e., from October 15, 2013 to November 30, 2013. During this time interval the 11 different sites with 13 nodes in total (see TABLE I.), deployed at different locations in research, industrial and educational environments, were functional. We have observed 857 different attackers on the basis of different source IP addresses. These attackers have attacked different NorNet nodes as shown in the TABLE I. . It shows the IP subnet and the number of attackers which attacked specific NorNet nodes. Moreover, the number of attack instances per attack stage is presented.

In the specified time interval we have not observed any call establishment (INVITE packet) from the attacker side. The information in columns 4 and 5 shows that in most of the cases not all of the attackers are performing the Server Scan. This behaviour indicates the possibility that attackers share attack information with each other. Considering the number of attacks, especially Registration Hijacking, at node N10 we can say that attackers seem to be more interested in the research and company networks than in the university networks. The vast majority of attacks was detected correctly as a comparison with the STR data confirmed. However, due to the pre-defined thresholds of our detection rules some of the attack instances were not detected by the Sensors because either the number of packets sent by an attacker was less than the specified threshold or the timing conditions were exceeded. This can be fine-tuned by reducing the packet threshold or extending the timing conditions. This, however, would lead to an increase in sensor reports and traffic between Sensors and SCS.

TABLE I. ATTACKED NORNET NODES

NorNet Node Name	ID	IP Subnet	Attacked by number of different IPs	Number of Attacks		
				Server Scan	Ext. Scan	Reg. Hijacking
Simula II	N1	77.88...	444	345	107	3
University of Essen II	N2	89.246...	303	255	67	16
Hainan University II	N3	113.59...	150	150	0	0
NTNU Trondheim	N4	129.241...	181	131	17	4
Universitetet i Tromsø	N5	129.242...	178	125	16	3
University of Essen I	N6	132.252...	163	121	21	15
Universitetet i Stavanger	N7	152.94...	150	103	12	7
Universitetet i Agder	N8	158.36...	168	113	16	2
Universitetet i Bergen	N9	158.37...	143	100	12	8
Simula I	N10	158.39...	176	124	15	4,013
Høgskolen i Narvik	N11	158.39...	167	115	15	1
Universitetet på Svalbard	N12	158.39...	164	114	14	1
Hainan University I	N13	210.37...	214	214	0	0

We are currently working on further optimization of the Sensor rules. We have created a matrix (see TABLE II.) from the attack traffic in our database to further analyse attacker's behaviour. The diagonal elements in the matrix indicate the number of attackers that have attacked only this particular node and other matrix entries represent the number of attackers who have attacked the two nodes given by the element position. The colour coding of the matrix gives a visual indication of the attack intensity ranging from green (low) to high (red). The comparison of diagonal values with others indicates that the attackers are more interested in scanning multiple nodes than the single nodes. Also the attackers are following some scanning behaviour to scan subnets. For example, node N7, N8, N9 and N10 are close to each other. Therefore, a high number of attackers have attacked more than one of these nodes or subnets. Similarly N4 and N5 belong to very close subnets so the higher number of attackers. The node N6 is in our research network which has been capturing the attack traffic since 2009. The green column for N5 shows that fewer attackers are interested in our network as it is already known to them. The red colour of column N1 indicates that a number of the attackers, attacking multiple nodes, are scanning a very large range of IPs (77.0.0.0 - 210.0.0.0) to perform multi-stage Toll-Fraud attacks.

TABLE III. shows the scanning behaviour of different attackers. Most of the attackers have scanned only one NorNet node (428) and their number decreases as the number of nodes scanned by an attacker increase. However, there exist ten attackers who have attacked all NorNet nodes and these nodes are not in a very close proximity with respect to their IP addresses and physical locations. This behaviour indicates that the attackers are scanning large IP ranges during the attacks. The IP addresses of NorNet nodes are located in Norway, Germany and China. We have evaluated attacks from the same source IP at different nodes with respect to the timing to find out the scanning behaviour of attackers. We have considered only those attackers, who have attacked 12 or 13 nodes. The analysis has shown that for the nodes in Norway which are close to each other or belong to a very close IP range, the attacker took from few minutes to an hour to scan the IP range.

TABLE II. ATTACKER'S BEHAVIOUR

	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	N12	N13
N1	54												
N2	73	32											
N3	60	48	28										
N4	80	63	58	21									
N5	82	62	57	88	18								
N6	64	55	47	43	42	17							
N7	74	51	50	46	46	29	22						
N8	72	47	49	50	52	29	49	23					
N9	67	49	47	45	47	28	41	58	20				
N10	68	48	41	45	46	28	40	49	44	17			
N11	72	53	50	55	50	35	51	64	61	53	24		
N12	71	52	52	51	54	34	50	62	59	53	67	25	
N13	78	59	64	52	48	47	48	43	44	42	50	49	35

TABLE III. ATTACK DISTRIBUTION

# of Nodes	# of Attackers
1	428
2	154
3	56
4	39
5	29
6	16
7	14
8	23
9	37
10	19
11	15
12	13
13	10

However, it took an attacker one week to a month to scan all the nodes. It indicates that attackers are using some automated tools (e.g., sipvicious) to attack a big range of IPs to perform multi-stage attacks. In addition to the NorNet Sensors (Centralized), we have also deployed real Sensors (Distributed) at different locations in Germany e.g., Essen, Berlin and Munich. In order to see if the deployment option has an impact on the results, we have compared the attackers from the NorNet setup to those we have identified in our distributed setup. Among 857 NorNet attackers we have also observed 108 in our distributed setup. The majority of these attackers were reported by all or multiple Sensors. This behaviour also supports the above mentioned result that the attackers scan a large IP range while performing the SIP-based attack.

In order to further analyse the attack behaviour we have analysed the number of attackers against different attack stages as shown in Fig. 5. We have selected only those attackers which showed up in NorNet and in the real Sensors as these should have the same behaviour in both setups. It is observed that the number of attackers reported in both environments for different attack stages are quite similar, which is another indication that the centralized setup works as expected.

The graph shows that more than 75% of these attackers have performed only a Server Scan indicating that there might be hosts specialized in scanning only. It is interesting to see that several hosts performed only Extension Scans without any preceding Server Scan. Since Sipvicious was used in these attacks and this tool only supports Extension Scans for previously known server addresses, we can conclude that either the information from the scans is shared or the attackers change their addresses in the course of the attack. Up to 17 attackers have executed a Server Scan as well as Extension Scans. Our data shows that if an attacker performing both stages finds several servers, he will also perform Extension Scans on all of them. Only one attacker performed a complete multi-stage attack with massive Registration Hijacking attempts.

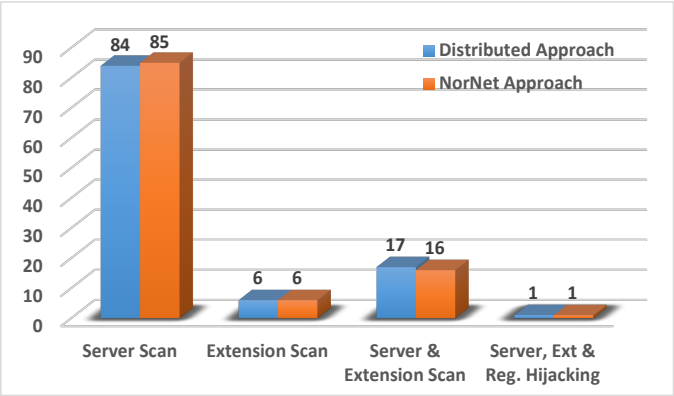

Fig. 5. Number of Attackers per Attack Stage

In addition to Sipvicious (known as friendly-scanner) and Sundayddr, we detected a new user agent, VaxSIPUserAgent, also mentioned in [11]. It is based on an SDK, which allows SIP users to add different SIP-based features to their software applications and web pages. In addition to the information given in [11], we identified three different versions (3.0, 3.1 and 3.2) of VaxSIPUserAgent, all having the similar header structure. Fig. 6 shows that this user agent was observed the very first time in November 2011 and then only sporadically showing that attackers were experimenting with it.

Since September 2013 this attack tool has been enhanced (versions 3.1/3.2) and a large amount of attack traffic has been generated using this attack tool. Besides this increase in the VaxSIPUserAgent attack traffic we have also observed a sudden decrease in the Sundayddr traffic. This analysis indicates that attackers are switching the attack tool suites. Moreover, we have observed the VaxSIPUserAgent attack traffic from various attackers directed to all NorNet nodes, which are widely distributed over the Internet. This behaviour clearly indicates that alike Sipvicious, this new tool is capable of attacking a big range of the IP addresses on the Internet.

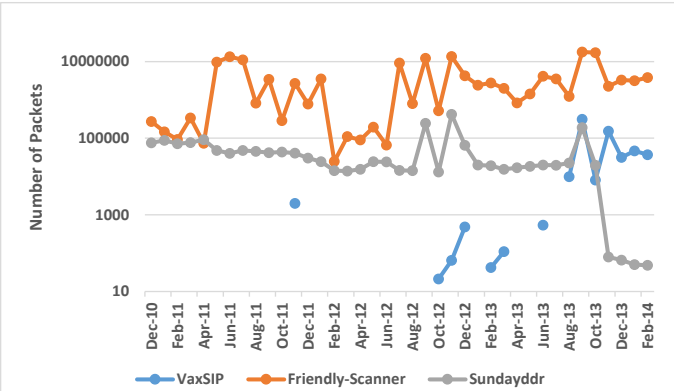

Fig. 6. Number of Packets per User Agent

VII. CONCLUSION AND OUTLOOK

In this paper, we have introduced our improved Security Sensor system to analyse the behaviour of attackers and to identify multi-staged attacks in a global, real-time Internet environment. We have presented two deployment scenarios. In the first scenario, we have deployed lightweight rule-based Sensors at different locations, analysed the attack traffic at the Sensor site, produced reports according to the specified rules and sent them to our Sensor Central Service over the Internet. In the second scenario, a centralized Sensor was deployed at our lab, analysing attack traffic tunnelled to it from all over the world using the NorNet testbed. We have also presented the architectural details of how SIP packets are sent to the Central Sensor via tunnelling and how the replies are sent back.

The analysis of the results has shown that a substantial number of attackers scan quite large sections of the Internet for SIP servers - which can only be seen if multiple observation points are deployed throughout the Internet. The results from the NorNet scenario have shown that attackers are more likely scanning a whole range of IPs or subnets instead of scanning specific nodes or limited subnets. Also, we have found out that a significant share of the attackers performing distributed attacks in the NorNet environment were also reported by the light-weight Sensors deployed at other locations. Moreover, our analysis showed an enhanced version of the attack tool VaxSIPUserAgent.

The results support the assumption that attackers scan a large range of the IP address space while performing multi-stage Toll Fraud attacks. The analysis of results has also shown that not all the attackers were involved in all stages of multi-staged Toll Fraud, which indicates that attackers share the scanning information with each other or they change the IP addresses to perform the next stages of multi-stage Toll fraud.

Currently, additional interfaces are added to the NorNet nodes and we will be able to participate and extend our coverage. In addition, we are in contact with additional network providers in order to extend our number of observation points. As the centralized approach seems to work as expected, we are currently refining and tuning the detection rules originally developed for the distributed Sensor approach. We will continue our observations in order to recognize additional attacker behaviour patterns. We are furthermore developing an online live analysis tool that can show the up-to-date attack situation in the Internet in a web browser, in order to provide guidelines for securing SIP systems to the VoIP community.

REFERENCES

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

[2] D. Hoffstadt, A. Marold, and E.P. Rathgeb, "Analysis of SIP-based threats using a VoIP Honeynet System," in Conference proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 2012.

[3] D. Hoffstadt, E. Rathgeb, M. Liebig, Y. Rebahi, and T. Q. Thanh "A Comprehensive Framework for Detecting and Preventing VoIP Fraud and Misuse," International Conference on Computing, Networking and Communication (ICNC), February, 2014.

[4] T. Dreibholz: “The NorNet Testbed: A Platform for Evaluating Multi-Path Transport in the Real-World Internet”, in Proceedings of the 87th IETF Meeting, Berlin/Germany, July 30, 2013.

[5] Sipvicious. http://blog.sipvicious.org (2013, Jan)

[6] M. Nassar, S. Niccolini, R. State, and T. Ewald, “Holistic VoIP Intrusion Detection and Prevention System”, Proceedings of the 1st International conference on Principles, systems and applications of IP telecommunication (IPT Comm,), 2007.

[7] M. Nassar, R. State, and O. Festo, “VoIP Honeypot Architecture”, in 10th IFIP/IEEE International Symposium on Integrated Network Management, Munich, Germany, 2007.

[8] C. Valli, “An Analysis of Malfeasant Activity Directed at a VoIP Honeypot”, Proceedings of the 8th Australian Digital Forensics Conference, 2010.

[9] M. Gruber; F. Fankhauser; S. Taber; C. Schanes; T. Grechenig, "Trapping and analyzing malicious VoIP traffic using a honeynet approach", Internet Technology and Secured Transactions (ICITST), 2011 International Conference for , vol., no., pp.442,447, 11-14 Dec. 2011

[10] M. Gruber; F. Fankhauser; S. Taber; C. Schanes; T. Grechenig, "Security Status of VoIP Based on the Observation of Real-World Attacks on a Honeynet", Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom) , vol., no., pp.1041,1047, 9-11 Oct. 2011

[11] M. Gruber; C. Schanes; F. Fankhauser; T. Grechenig, "Voice calls for free: How the black market establishes free phone calls — Trapped and uncovered by a VoIP honeynet", Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on , vol., no., pp.205,212, 10-12 July 2013

[12] D. Hoffstadt, S. Monhof, and E. Rathgeb, “SIP Trace Recorder: Monitor and Analysis Tool for Threats in SIP-based Networks”, Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, August, 2012.

[13] J. Safarik; M. Voznak; F. Rezac; P. Partilal; K. Tomala, "Automatic analysis of attack data from distributed honeypot network", Proceedings of the SPIE, Volume 8755, id. 875512 7 pp. (2013)

[14] Dionaea Honeypot, http://dionaea.carnivore.it/, 2014

[15] Digium, Inc., “Asterisk IP PBX, VoIP Gateway, IVR & Open Source Communications”.http://www.asterisk.org/, 2013

[16] D. Hoffstadt, N. Wolff, S. Monhof, and E. Rathgeb “Improved Detection and Correlation of Multi-Stage VoIP Attack Patterns by using a Dynamic Honeynet System”, International Conference on Communication (ICC), June, 2013.

[17] TCMPDUMP: Tcpdump/Libpcap public repository. http://www.tcpdump.org. (2013, Nov)

[18] BOOST: Boost C++ Libraries. http://www.boost.org (2013, Jan).

[19] B. Chun, D. Culler, T. Roscoe, A. Bavier, L. Peterson, M. Wawrzoniak, M. Bowman: “PlanetLab: an overlay testbed for broad-coverage services”, SIGCOMM Comput. Commun. Rev. 33, 3 (July 2003)

[20] A. Kvalbein; D. Baltrūnas; K. Evensen; J. Xiang; A. Elmokashfi, S. Ferlin-Oliveira: “The NorNet Edge Platform for Mobile Broadband Measurements”, in Computer Networks, Special Issue on Future Internet Testbeds, 2013.

[21] E. G. Gran; T. Dreibholz; A. Kvalbein: “NorNet Core – A Multi-Homed Research Testbed”, in Computer Networks, Special Issue on Future Internet Testbeds, 2013.

[22] T. Dreibholz; E. G. Gran: “Design and Implementation of the NorNet Core Research Testbed for Multi-Homed Systems”, in Proceedings of the 3nd International Workshop on Protocols and Applications with Multi-Homing Support (PAMS), pp. 1094–1100, DOI 10.1109/WAINA.2013.71, ISBN 978-0-7695-4952-1, Barcelona, Catalonia/Spain, March 27, 2013.

[23] E.G. Gran; T. Dreibholz, A. Kvalbein: “NorNet Core – A Multi-Homed Research Testbed”, in Computer Networks, Special Issue on Future Internet Testbeds, DOI 10.1016/j.bjp.2013.12.035, ISSN 1389-1286, January 3, 2014.

[24] D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, “GRE: Generic Routing Encapsulation”, RFC 2784, March 2000