Global VoIP Security Threats – Large Scale Validation Based on Independent Honeynets

Markus Gruber*, Dirk Hoffstadt§, Adnan Aziz§, Florian Fankhauser*, Christian Schanes*,
Erwin Rathgeb§ and Thomas Grechenig*

*Vienna University of Technology, Industrial Software (INSO), 1040 Vienna, Austria
{markus.gruber,florian.fankhauser,christian.schanes,thomas.grechenig}@inso.tuwien.ac.at

§University of Duisburg-Essen, Institute for Experimental Mathematics, 45326 Essen, Germany
{dirk.hoffstadt,adnan.aziz,erwin.rathgeb}@uni-due.de

***Abstract*—Voice over IP (VoIP) gains more and more attractiveness by large companies as well as private users. Therefore, the risk increases that VoIP systems get attacked by hackers. In order to effectively protect VoIP users from misuse, researchers use, e.g., honeynets to capture and analyze VoIP attacks occurring in the Internet. Global VoIP security threats are analyzed by studying several millions of real-world attacks collected in independent VoIP honeynet solutions with different capture mechanisms over a long period of time. Due to the validation of results from several honeynet designs we have achieved a unique, much broader view on large scale attacks. The results show similar attacker behavior, confirm previous assumptions about attacks and present new insights in large scale VoIP attacks, e.g., for toll fraud.**

Keywords—Security, Internet telephony, Intrusion detection, Communication system security

I. Introduction

Today, the use of VoIP systems is widespread. Consumers as well as companies use VoIP systems, e.g., for making cheap calls regardless of their current location. This widespread availability of VoIP systems based on the Session Initiation Protocol (SIP) [1] has also lured attackers to misuse the systems. Therefore, many researchers investigate attacks against VoIP systems in order to better secure them.

One method to research threats occurring in networks like the Internet are honeypots and honeynets. However, different approaches to implement honeypots and honeynets exist which capture and analyze attack data in different ways.

In this paper we compare several different approaches for honeynets operated by Vienna University of Technology and University of Duisburg-Essen to get a broader view on the results. We present attacks on VoIP that were common in our research approaches as well as attacks that were different to define best practice approaches for honeynet solutions and to cross-check results captured from different approaches.

Often, researchers independently implement mechanisms in order to collect attack data. However, the collected data is prone to provide only a narrow view on reality. Therefore, by combining the different approaches used in Vienna and Essen we get more insights into attacks on VoIP as well as the honeynet approach itself. That way a much broader view on attacks on VoIP can be obtained than by using only one isolated system.

The remainder of this paper is structured as follows: In Section II related work is presented. Afterwards, Section III describes SIP foundations as well as some basic attacks on VoIP in order to be able to compare different attacks found in the honeynet approaches. In Section IV we present the honeynet approaches designed and operated in Vienna and Essen. Operation details and statistics gained in the honeynets are presented in Section V. In Section VI the attacks found in the independent approaches are analyzed and compared. A discussion of the results follows in Section VII. A conclusion and outlook is finally given in Section VIII.

II. Related Work

Initially, the honeynet idea was described by Spitzner [2]. Since the beginning of honeynets different solutions for honeynets and honeypots (see, e.g., Spitzner [3]) evolved. In the VoIP security area, for example, do Carmo et al. [4] used honeypots as a User Agent (UA) in existing VoIP domains. This work provides a promising solution towards Spam in IP Telephony (SPIT) attacks. However, in order to identify attacks other than SPIT in SIP-based networks it is necessary to monitor and analyze the SIP traffic in more detail.

It is crucial that attackers don't recognize they access honeypots used to capture the original attack traffic to analyze attacker's behavior. Provos and Holz [5] describe how attackers could detect being within a honeynet, especially in virtualized environments. Today, however, virtualization is also used in production systems. Therefore, the use of virtualization is not a sure sign for a honeypot any more. Moreover, some of our honeynets use physical honeypots as well. Additionally, since we also mostly use High Interaction Honeypots with complete SIP implementations, the risk of revealing that our systems are used for tracking attackers is low.

Kang et al. [6] as well as the VoIP Security Alliance (VoIPSA) [7] classified different attacks against VoIP systems. We use parts of this classification to interpret and describe the attacks we monitored in our honeynets.

Nassar et al. introduce a SIP oriented Low Interaction Honeypot [8] that is used in [9] to build an Intrusion Detection System

ISBN 978-3-901882-68-5 © 2015 IFIP

(IDS) to detect SIP attacks. A Low Interaction Honeypot usually has only a limited script-based service implementation. The mentioned IDS works with a so-called security event correlation system to detect attacks. The honeypot is capable of interacting with the attacker and to retrieve information, e.g., a fingerprint, from him.

A simple statistical analysis of VoIP attacks against honeypots is given by Valli [10]. The source data is captured at a honeypot system consisting of several virtualized Low Interaction Honeypots that are logging to the same system. The use of SIPVicious [11] as tool is proven and another tool, called "sipsscuser", is found. The author speculates that the behavior of sipsscuser points to a botnet- or worm-like activity. Some attacks against our honeynets appear to come from botnets. Little detailed information on that is available. However, Dainotti et al. [12] describe SIP botnet detection.

To analyze the attacker's activities thoroughly, it is important to have a more global view of the attack behavior. In [13] Safarik et al. have presented the architecture of distributed honeypots with predefined software images. 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 analyses. This approach requires the installation and maintenance of hardware and software with high resource usage at the remote locations. We have developed a virtually distributed Sensor System [15], where the problem of installation, upgrading and maintenance of hardware and software is solved using the NorNet testbed [16].

III. SIP Foundations and Specific Misuse Cases

VoIP systems enable advanced communication (such as voice or video) over the Internet and other data networks and therefore, are replacing the traditional phone infrastructures. Nowadays, VoIP is widely used in organizations, companies and private environments, as it has the advantage of flexibility and low costs. Many existing devices and applications use standardized VoIP protocols (e.g., SIP [1] for signaling, or Real-Time Transport Protocol (RTP) [17] for media transmission). SIP is a text-based application layer protocol similar to File Transfer Protocol (FTP) used to establish, maintain and terminate multimedia sessions between UAs. The SIP communication uses a request-response-protocol, i.e., the source sends a SIP request message and receives a SIP response message. SIP is an inherently stateful protocol and uses the Hyper Text Transfer Protocol (HTTP) Digest Authentication [18] for user authentication. In its simplest form SIP uses the transport protocol User Datagram Protocol (UDP), but others can also be used, e.g., Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP).

For the purpose of this paper, the following SIP message types are relevant: If a UA (i.e., SIP device) wants to establish a call via a voice server in SIP-based networks, usually, a registration at the server is necessary. In order to register, a UA sends a REGISTER message with credentials (account name and password) to the server. After successful registration, the UA can initiate calls using INVITE messages. The OPTIONS messages allow a UA to query a server's capabilities and to discover information about the supported SIP methods, extensions, codecs, etc. without establishing a session. To ensure that this communication is always possible, the SIP standard specifies that an OPTIONS packet must be answered, regardless of its source or existing connections. The attackers use this standard request/response behavior of SIP systems to misuse a third party SIP extension. Four distinct attack stages (SIP Server & Device Scan, Extension Scan, Registration Hijacking and Toll Fraud), also called multi-stage toll fraud, are carried out to accomplish this task. These attack stages were observed during our honeynet field test [19]. In these attack stages every distinct source IP is considered as an attacker.

A. SIP Server & Device Scan

The fact that the SIP protocol requires every SIP device to answer OPTIONS packets can be used by an attacker to "ping" any single IP address or whole subnets with OPTIONS packets to identify SIP devices. Even if a UA's SIP stack implementation is not standard compliant and replies only to OPTIONS packets of well-known sources, a scan may, nevertheless, be possible. In this case, the attacker can try REGISTER requests instead of OPTIONS messages to identify SIP devices.

B. Extension Scan

To identify active extensions (user accounts) of known SIP servers, the attacker tries to register at several extensions, typically without using a password. An extension identifier consists of digit sequences and/or strings. If the extension exists, the server normally answers with a 403 FORBIDDEN, because no password is given. If it does not exist, a 404 NOT FOUND is returned. The result of this attack stage is a complete list of existing extensions (provider accounts).

C. Registration Hijacking

To register at a given extension, the attacker tries to guess the password. This means sending – possibly many – REGISTER messages with different passwords to a specific extension. If a valid password is found, the information is stored by the attacker to use the credentials to register at this extension later on.

D. Toll Fraud

The term multi stage "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 the VoIP functionality to make calls, specifically international calls or calls to premium numbers. Another motivation to use a hijacked account for a call is to obfuscate the caller identity. 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 (A-C of Section III) of multi-stage toll fraud can be executed by using freely available tool suites. A common white-hat attacking tool for SIP is the open source tool suite SIPVicious [11]. It contains several small programs: The first one is a SIP scanner called "svmap". It scans an IP address range for SIP devices, either sequentially or in random order, typically with OPTIONS packets. SIPVicious also provides tools to find active SIP accounts with REGISTER messages ("svwar") and to crack passwords ("svcrack"). If not modified, SIPVicious identifies itself as UA "friendly-scanner".

IV. Honeynet Architectures for Collecting VoIP Security Threats

Multiple approaches for designing honeynet systems exist, with each approach focusing on different attack scenarios, e.g., low interaction vs. high interaction honeypots (see, e.g., Mokube and Adams [20]). However, to get a thorough understanding of attackers, business models and attack behavior a combination of different approaches is required. The honeynets described in this section are used as a basis for the presented further security analyses. They were designed independently and differently to collect and analyze attacks against VoIP systems. This heterogeneous infrastructure allows to capture different attackers and get a broader view on the security state of the art in VoIP. The honeynets captured a huge amount of data which can be used to validate the different approaches of VoIP attack collection, identification and analysis.

A. *Vienna University of Technology Honeynet*

The implemented solution is a complete infrastructure to identify threats and vulnerabilities of VoIP systems as well as gain details of VoIP attacks and trace the behavior of the attackers. It consists of a VoIP honeynet to collect data and an analyzing engine to analyze the captured attacks.

1) Concept of the VoIP Honeynet: The overall goal is to collect as much data about attacks on a VoIP infrastructure as possible in order to determine threats and vulnerabilities of VoIP systems. Therefore, the data collection should be conducted on several layers, e.g., recording calls in order to detect fraud or collecting data packets to get information about attacks at the protocol level.

Figure 1 shows the implemented flexible honeynet solution which allows to scale in the size and on the functionality of the honeynet. A possible attack attempt will be captured by the honeywall. The honeywall verifies if the packet is allowed to be forwarded to the honeypots (data control) and classifies the packet with the signature-based IDS Snort. If the IDS recognizes an attack, a notification will be sent to the operations team. Based on Internet Protocol (IP) firewall rules, packets will be forwarded to the honeypots or rejected. For forwarded packets, the response messages from the honeypots will also be captured, controlled and a notification will be sent before the attacker receives the reply. The dash line indicates that 1 to n honeypots could be in operation.

The proposed approach is extensible to a VoIP honeynet with an uplink to a Public Switched Telephone Network (PSTN) system, in order to capture fraudulent calls to PSTN systems, too.

The honeypots provide VoIP systems which attract attackers. The concept considers that various different VoIP systems are better than only one kind, since this approach may attract different and probably more attackers.

2) Design of a VoIP Specific Honeynet: The basic structure of the implemented VoIP honeynet and the analyzing engine is shown in Figure 1. The honeywall is used as a centralized bidirectional data channel from the Internet to the honeypots and is responsible for *data capture*, *data control* and *notification*. The design uses High Interaction Honeypots in order to gain more accurate details about the attacks. Each honeypot has a unique IP address and is accessible through the data channel. The VoIP specific honeynet has no connection to PSTN systems and can be used for identification of VoIP specific attacks. The concept and the architecture was described in detail in our previous work [21].

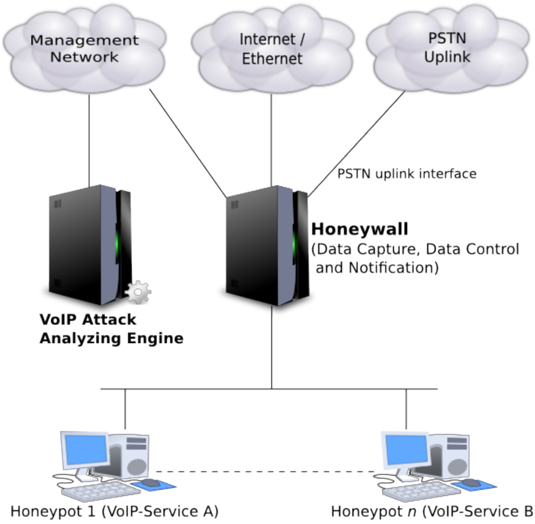

Management Network
Internet / Ethernet
PSTN Uplink
PSTN uplink interface
Honeywall
(Data Capture, Data Control and Notification)
VoIP Attack Analyzing Engine
Honeypot 1 (VoIP-Service A)
Honeypot n (VoIP-Service B)

Fig. 1: Implemented Architecture of a VoIP Specific Honeynet to Identify Threats and Vulnerabilities at Vienna University of Technology

3) PSTN Extension of a VoIP Honeynet: In order to enable calls from a VoIP account to a number in the PSTN system, a special gateway is needed. The PSTN uplink can be an Integrated Services Digital Network (ISDN) modem, a data modem or a third party VoIP provider. We decided to use a third party VoIP provider with support for a prepaid solution to allow better cost control. To activate the uplink interface and to allow calls to PSTN endpoints, credit must be bought from the provider. The VoIP provider sends a notification if a customized limit is reached, in order to top up the credit in time. The PSTN extension is described in detail in our previous work [22].

4) Analyzing Engine: To easily analyze and evaluate the identified threats to VoIP systems, we decided to implement our own analyzing engine. This engine collects all captured data from the honeynet via a separate management network and imports the data to a central database. The analyzing engine is responsible for processing the captured data and carrying out customizable analyses on the data. With this engine all data from the honeywall and the honeypots can be semi-automatically analyzed to gain information about the attacks and the attackers. In addition to the captured data from the honeynet, the analyzing engine uses third party sources (e.g., the whois directory service, phone books, price tables of various VoIP services or UA databases) to gain even more information about the attacks and the attackers. The VoIP attack analyzing engine is described in detail in our previous work [21].

5) VoIP Honeypots: The proposed solution uses only High Interaction Honeypots to get in-depth information about real-world VoIP attacks and to make it more difficult to identify the honeynet. Emulated services which are used in Low Interaction Honeypots are easily detectable by attackers as described by Raffetseder et al. [23].

The introduced solution uses the Asterisk PBX [24] and a VoIP server based on SIP (called *sipListener*), which was specifically implemented for our honeynet solution. The in-house implemented VoIP server, which operates as a SIP proxy server and as UA, has the primary goal of easily recording VoIP communications (such as Spam over IP Telephony (SPIT) messages) and other data about calls. Therefore, all incoming SIP calls are accepted and logged to the file system. We operated different SIP servers to identify different behavior of the attacks against different VoIP servers.

B. University Duisburg-Essen VoIP Attack Analysis System

To understand the SIP misuse behavior it was necessary to analyze the SIP attack traffic. Due to the privacy reasons in Germany it was not possible to access the SIP traffic from the production systems. Therefore, we implemented a honeynet system to capture the SIP attack traffic from the Internet for analysis purposes. As it is not a real productive environment, the whole traffic to this honeynet system is by default attack traffic. We are using a VoIP Honeynet system and a Security Sensor System to analyze SIP attack traffic in local and distributed environments respectively.

1) VoIP Honeynet System: In 2009, we implemented a VoIP honeynet system, consisting of High and Low Interaction Honeypots and a monitoring and analysis component. The High Interaction Honeypot is based on a standard Linux virtual machine with a specially-configured open source VoIP PBX Asterisk server. The Low Interaction Honeypot is based on Dionaea which reacts according to the attackers' behavior and uses a dynamic honeypot configuration in real-time to significantly improve the detection efficiency (see our previous work [25]). These machines accept incoming SIP requests on port 5060 and act as standard SIP server. This setup has four High Interaction Honeypots and one Low Interaction Honeypot, accessible via different public IP addresses. Each honeypot monitors a single IP.

To monitor and analyze the whole network traffic we developed a component called SIP Trace Recorder (STR) [26]. It passively monitors the traffic of different subnets by using the monitoring port of the switch as shown in Figure 2. In our lab environment, it monitors two class C subnets (network A and network B). The network A contains 5 honeypots publicly available over the Internet, whereas, the network B does not contain any honeypot. This allows a more comprehensive view of the attacker's behavior (e.g., scanning behavior of a special network, also how an attacker reacts to the presence and absence of SIP devices in the network). The STR captures the SIP attack traffic to and from the honeynets. Due to the passive connection via a monitoring port, the STR is not reachable from the Internet. The captured SIP traffic is stored into a central SQL database to perform comprehensive offline analyses. It also generates automatic statistical reports, e.g., number of packets per day, clustering the attack traffic according to different attack stages, etc.

2) Security Sensor System: For real-time analyses of SIP attack traffic in distributed environments, the STR is not a suitable option as it performs offline analyses and requires installation of a SQL database along with a STR instance at each site. Therefore, we have implemented a Security Sensor System to perform real-time analyses of SIP attack traffic [15].

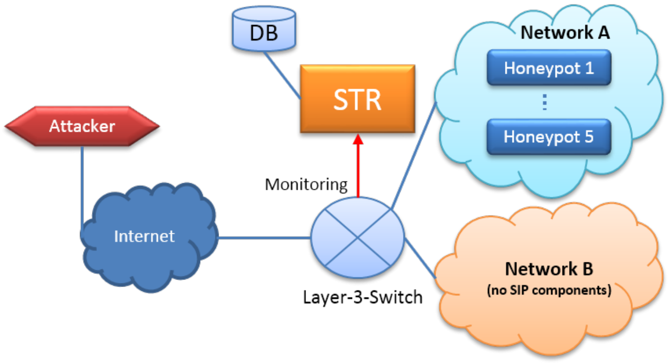


Fig. 2: Implemented Architecture of a VoIP Specific Honeynet to Identify Threats and Vulnerabilities at University Duisburg-Essen

The Central Sensor approach [15], based on the NorNet testbed [16], analyzes the SIP attack traffic over the Internet. In this approach only one sensor, the Central Sensor, combined with a honeypot, receives the SIP attack traffic from different NorNet nodes distributed all over the Internet, as shown in Figure 3. The NorNet nodes are connected to the Internet – via multiple Internet Service Providers (ISPs) – by a router called tunnel-box. The tunnel-box is responsible for routing the SIP attack traffic to the Central Sensor using Generic Routing Encapsulation (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 the responses back to the attacker are handled by the standard Linux implementation. Therefore, only configuration but no installation of additional software at the remote nodes is necessary. The Sensor Central Service (SCS) [15] correlates the attack reports from different NorNet nodes and performs some actions. This new concept has significantly reduced the inhibitions for hosting observation points in other networks.

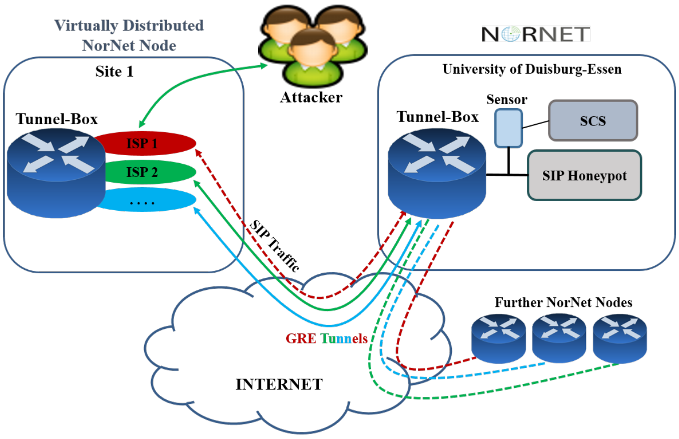


Fig. 3: Architecture of the Central Sensor System

V. Setup, Operation and Statistics of the Independent Honeynets

The honeynets use different architectures for trapping and analyzing VoIP attacks, because the honeynets were designed and implemented independently. They differ in the number of honeypots, the supported VoIP extensions, the used systems, etc. Both universities operate the honeynet solutions for a long time (Vienna started August 2009, Duisburg-Essen started December 2009). These statistics are based on the data collected during a time period of 22 months i.e., January 01, 2013 to October 31, 2014.

For global capturing of VoIP data, it is important to operate the honeynets at different locations. By combining the results of the Vienna and Essen honeynets, a wide spread area could be covered. The different approaches and results could be used to verify the analysis and to get a better understanding of real-life VoIP attacks.

A. Vienna Honeynet

Three different instances of our honeynet architecture are operated in Vienna. One at the Vienna University of Technology and two in a public environment to see differences in the attacks and the attacker behavior between a research network and provider owned IP addresses. Detailed information on the Vienna honeynet can be found in [21, 27, 22, 28].

The first honeynet uses four honeypots with the VoIP server "Asterisk" and four honeypots with an in-house implemented VoIP server called "sipListener". Each VoIP server offers five SIP extensions with simple passwords (e.g., "123"). None of the VoIP servers have a gateway to the PSTN. The IP addresses are close together, i.e., blocks of multiple consecutive IP addresses within a subnet.

The second honeynet uses one honeypot with the VoIP server "Asterisk" and one honeypot with "sipListener". Both servers offer five SIP extensions with simple passwords and none of them have a PSTN gateway.

The third honeynet is based on "Asterisk" as VoIP server only and has a gateway to the PSTN. The PSTN gateway is a prepaid interface and can be activated on demand. In our evaluation period the gateway was activated three times (each session had €100 credit).

The VoIP Attack Analyzing Engine collected the captured attacks from all three honeynets. In the following sections this data set will be called "Vienna".

B. Essen Honeynet

The Essen honeynet consists of five honeypots, four using Asterisk as SIP-based VoIP server, and the fifth honeypot is the Dionaea honeypot with the SIP services. The Dionaea honeypot is configured with ten extensions and the other four honeypots have four extensions each with simple but more complex passwords as in Vienna (e.g., "1234" or "400400") to lure the attackers. The honeypots have no connection to the PSTN. However, after a successful registration hijacking attack, the attacker is allowed to establish simulated outgoing calls. These calls are redirected to internal accounts and are terminated after ten seconds without connecting to the PSTN. This behavior is necessary to log the outgoing telephone numbers and to simulate the call establishment for the attacker. In the following sections the collected data set will be called "Essen".

C. Basic Indicators from the Operation of the Honeynets

Table I presents a short statistic, to get a better understanding of the data which was collected in the honeynets. The numbers can not be directly compared, but the table gives a short impression for the results of the following analyses. The honeynet in Essen collects more SIP packets compared to the Vienna system, because it observes two class C networks (508 IPs) compared to 11 IPs in Vienna. However, in Vienna the honeynet detects a lot more source IP addresses. Therefore, the packet to IP ratio in Essen is higher than in Vienna, because of a different Registration Hijacking behavior and the number of monitored honeynet IP addresses. The extension passwords in Essen are a bit more complex than in Vienna which results in a more intense attack behavior (e.g., 13 million packets per extension due to brute forcing of passwords). The system in Essen provides a larger range of destination IP addresses and collects all SIP messages directed to the honeynet subnets. However, in both honeynets, the origin of attacks is very much alike.

Information	Vienna	Essen
Evaluation period	2013-01-01 to 2014-10-31	2013-01-01 to 2014-10-31
Number of packets	49,543,482	97,108,984
Number of honeypots	11	5
Detected IP addresses	5,607	3,682
Most attackers from	US, EG, DE, PS and FR	US, PS, DE, FR and EG

TABLE I: Basic Collecting and Analysis Information of the honeynets in Vienna and Essen

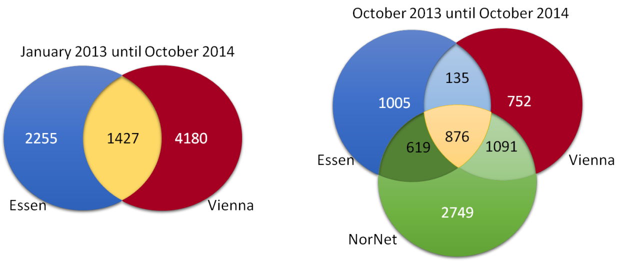
VI. Findings and Correlation of the Honeynets

We presented different honeynet architectures to analyze attacks in SIP-based networks with a broad range of individual features for attack analysis, e.g., monitoring of whole subnets, uplink to PSTN. In this section we present findings and correlations of the captured VoIP attacks in the different honeynet solutions of Vienna and Essen in order to gain insights into globally active attackers and to identify global VoIP security threats. Therefore, the collected data is normalized, classified and analyzed, in order to make the collected data comparable.

A. Identification of Globally Active Attackers

In the independently implemented honeynet systems, which are also geographically apart from each other, we have observed some common attackers, based on different IP addresses. This counting method is valid, since it is unlikely that the IP addresses are spoofed, because an attacker wants to get the answer from the server when an attack is successful and it is not a Denial of Service (DoS) attack. The number of identified unique source IP addresses in our evaluation period (January 2013 to October 2014) is shown in Figure 4. 1427 common IP addresses from 67 countries were identified in the honeynets in Vienna and Essen (Figure 4a). This corresponds to about one third of all identified IP addresses in Vienna and about two-thirds in Essen. To further analyze this scanning behavior of the attackers we compared the attack traffic from the honeynets with the NorNet Central Sensor System [15], a distributed infrastructure to analyze the SIP attack traffic over the Internet, and found some common attackers in all the independent setups, as shown in Figure 4b. The NorNet Central Sensor started working in October 2013. Therefore, we considered data collected over a period of 13 months, i.e., from

October 2013 to October 2014. The large overlapping between Vienna and NorNet shows, that different IP ranges are important. Vienna has 11 IP addresses and gets higher overlapping with NorNet than Essen honeynet with two Class C networks.



(a) Vienna and Essen

(b) Vienna, Essen and NorNet

Fig. 4: Numbers of Unique and Common Source IP Addresses in Different Honeynets

We identified 876 common IP addresses (IPs) among Vienna (with a total of 2854 unique IPs), Essen (2635 IPs) and NorNet (5335 IPs). It further endorses the above mentioned hypothesis that attackers scan a wide range of IP addresses while performing SIP-based VoIP attacks, because a large IP-range was observed and these attackers were identified in each of them.

To identify globally active attackers we analyzed and compared the origins of the identified source IP addresses in each honeynet. Figure 5 shows the distribution of the top 10 origins of the attackers in the honeynets in Vienna (5607 attackers), Essen (3682 attackers) and for the common attackers in Vienna-Essen (1427 attackers), respectively. The top origins of the attacks are almost the same countries, but slightly different in the distribution. In the honeynets the origin of one-third of the attackers is United States. To identify global VoIP security threats we focused on the common attackers, even though the identification of the origin countries of the individual honeynets are very similar to the common attackers. Most common attackers are from the United States, Germany and France.

B. Behavior of Globally Identified Attackers

To understand the behavior of globally identified attackers we had a closer look at the used SIP UAs to recognize the tools used. In both setups we observed the same major UAs, as seen in Figure 6. The graph shows that in both setups a major number of attacks is performed using UAs that identify themselves as *friendly-scanner*, i.e., the SIPVicious toolbox. In the Essen setup the UAs, e.g., *sip/cli* is, at some points, comparable to the friendly-scanner. However, in Vienna setup, the friendly-scanner is always on the top. Analysis of older SIP attack data reveals some change in the UA trends. From 2009 to 2012 a significant number of attacks was performed using *sundayddr* but over time this attack intensity has decreased. Meanwhile a new UA, *VaxSIPUserAgent*, was witnessed, which seems to have replaced *sundayddr*. This trend can be clearly seen in both setups. Since May 2014 we have also observed a new UA, using eight random characters as UA name. This *random UA* can be easily observed in both setups. This behavior shows that attackers are making changes to the previously existing attack tools or developing some new attack tools to camouflage the SIP-based VoIP attacks.

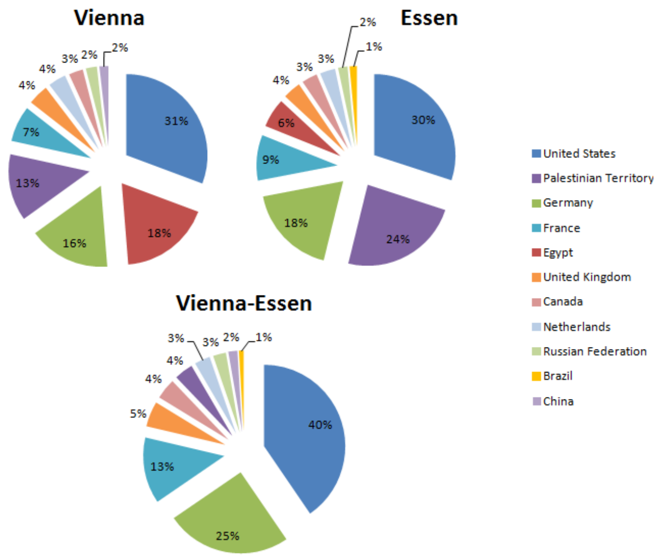


Fig. 5: Top ten Originating Countries of Attackers in the Honeynets in Vienna, Essen and common Vienna-Essen

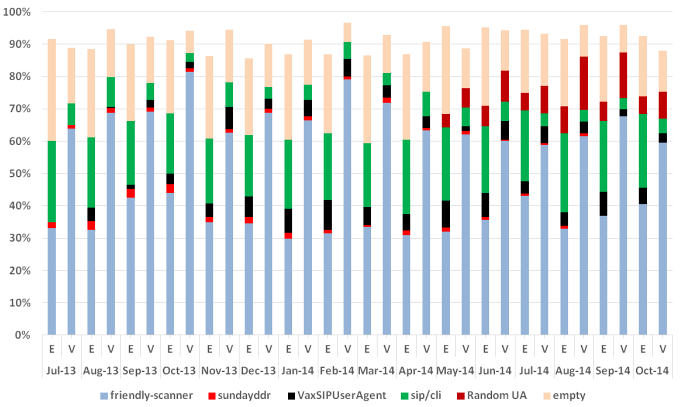


Fig. 6: Trend of the Main Identified SIP User Agent Strings per Attacker in Vienna (V) and Essen (E)

The SIP attack data sets from both honeynet setups were clustered using the STR [26] tool. In STR, the SIP messages are grouped on the basis of source IP address, SIP message type and timing, to cluster them according to different stages of multi-stage toll fraud. A Server Scan occurs when the OPTIONS packets are received at multiple destinations from the same attacker. An Extension Scan is identified when a number of REGISTER packets are sent to the same destination from same source IP with different to-user header value. A Registration Hijacking attack is reported when an attacker sends a number of REGISTER packets to the same destination with the same to-user header field but different credentials. Figure 7 shows the percentages of attacks for each stage of the multi-stage toll fraud attack. The percentages of attacks in both setups are different because of the dissimilar architectures described earlier in Section IV. In the honeynet system in Essen two class C networks and in Vienna 11 IP addresses are observed. Therefore, we only include the SIP messages directed to the honeypot hosts to ensure the comparability of the setups. The number of Server

Scan and Extension Scan attacks are comparable in the setups, because only the honeypot hosts are responding. Despite the temporary connections to the PSTN, the Vienna setup has less toll fraud calls than Essen. Only one honeynet has a gateway to the PSTN in Vienna, whereas, in Essen, incoming calls are accepted and redirected to the internal network where calls are terminated after ten seconds without establishing a real connection to the PSTN. This behavior indulges the attacker to try more and more to perform toll fraud calls.

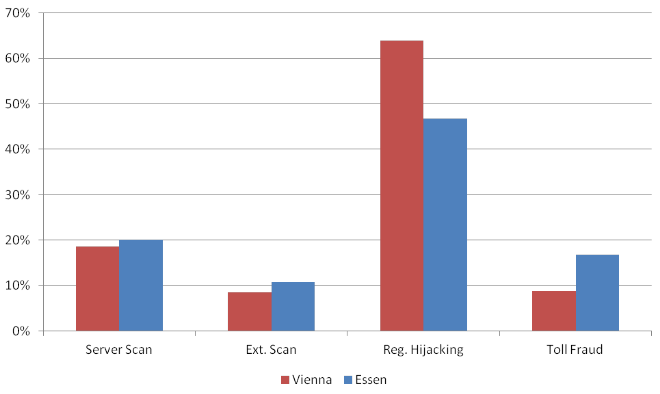


Fig. 7: Distribution of VoIP Attack Types in the Honeynets in Vienna and Essen

The number of common IP addresses (also see Figure 4) suggests that only a small number of attackers are recurring in the honeynets. Figure 8 shows the number of identified attackers per day of occurrence. For a clearer view the y-axis is shown in a logarithmic scale. More than 90% of the attackers were identified on less than 7 different days and only a small number of attackers was recognized more often. We found an average occurrence of the same IP address of 2.5796 days in Vienna and 3.4929 days in Essen. For further analyses we focused on the globally active attackers which were periodically identified in the honeynets.

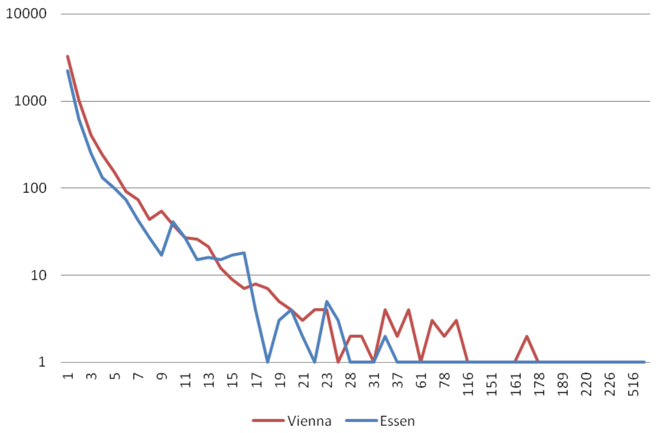


Fig. 8: Maximum Number of Days an Attacker is Recognized in the Honeynets in Vienna and Essen

The top globally active attackers in the honeynets have the same source IP address. Table II shows the identified long-lived scanners in the honeynets with more than 300 days. All of them send only SIP OPTION packets with exactly the same UA and the same TO-Address. Some of the SIP TO-Addresses (e.g., “nm2”) were not defined at the honeypots, but the attacker used exactly the same string periodically. It seems that the attacker was not interested in the specific response for this TO-Address, but rather for any request from the VoIP server. Most long-lived scanners are from China and the USA. *Days V* and *Days E* represent the days between first identification and last identification in the honeynet in Vienna and in Essen respectively. In both honeynets the attacker with the most days was last identified on 21th of August 2014. However, the independent honeynets recognized long-lived scanners over almost the same duration of days. With the end of the top long-lived scanners the number of SIP messages with the UA string “sundayddr” decreased, as seen in Figure 6.

IP	Days V	Days E	Method	UA	TO
219.X.X.X (CN)	595	597	OPTIONS	sundayddr	100
115.X.X.X (CN)	582	596	OPTIONS	sundayddr	100
114.X.X.X (CN)	500	524	OPTIONS	sundayddr	100
198.X.X.X (US)	367	373	OPTIONS	*empty*	nm2
66.X.X.X (US)	329	336	OPTIONS	*empty*	nm2
202.X.X.X (LA)	312	322	OPTIONS	sundayddr	100
71.X.X.X (US)	314	318	OPTIONS	*empty*	nm2

TABLE II: Identified Long-Lived Scanners in Both Honeynets (Vienna (V) and Essen (E)) With More Than 300 Days Between First and Last Identification

C. Distributed Toll Fraud Attacks and Their Behavior

To understand the behavior of global toll fraud attacks, we considered the attackers who tried to establish a phone call in the setups. In Vienna and Essen, 1581 and 1523 different IPs were found respectively. In both honeynets 184 common IP addresses were identified. These 184 IP addresses could be mapped to 14 countries.

We analyzed the toll fraud call numbers from the setups in more detail and, similar to the common IPs, we observed common dialed numbers in the honeynet systems. Table III shows the top callee numbers, observed in the setups, dialed by different IPs/attackers from different countries. This way we identified 281 phone numbers which were seen in both honeynets from different source IP addresses and also from different countries. The wide distribution of the source IP addresses (also of the origin countries, e.g., Germany, Great Britain and US) for the same probing phone numbers indicates that a globally active botnet or well-connected attackers with shared information carried out the probing calls, in order to identify VoIP systems with a connection to the PSTN. Most of the listed destination phone numbers are located in Israel and we have also seen that a high number of calls to Israel are originating from Europe and Palestinian territories. The dialing number countries are almost the same in both setups.

After detailed analysis we identified a similar behavior of the attacks, e.g., after a successful registration hijacking attack the attackers tried to establish a phone call to the PSTN network (toll fraud). Only in a few cases the attackers tried to call another VoIP extension. We identified some common source IP addresses used for toll fraud attacks in both honeynets as well as common callee phone numbers from different attackers in the honeynets.

Phone Number	# Diff. IPs		Origin Vienna	Origin Essen
	Vienna	Essen		
+97259XXXXXXX (Israel)	18	10	CA, DE, EU, FR, NL, PS, US	DE, EU, FR, PS, US
+44190XXXXXXX (Great Britain)	18	6	CA, DE, EG, NL, PS	EG, PS
+97254XXXXXXX (Israel)	6	2	DE, FR, NL, PS, US	PS
+97059XXXXXXX (Palestine)	6	10	AT, FR, PS, US	AT, FR, PS
+97259XXXXXXX (Israel)	13	8	GB, PS, US	PS
+20102XXXXXXX (Gambia)	8	7	DE, EG, US	CA, CZ, DE, EG, FR, US
+20102XXXXXXX (Gambia)	6	4	DE, EG, NL	DE, EG
+97259XXXXXXX (Israel)	3	3	DE, GB, US	DE, US
+97259XXXXXXX (Israel)	3	1	FR, PS, US	US
+97259XXXXXXX (Israel)	3	1	DE, EU, PS	PS

TABLE III: Top Dialed Numbers From Different IPs Observed in Vienna (V) and Essen (E)

Finding this attacking approach in both honeynets confirmed our assumption from our previous paper [28], that the attacks are divided into a probing phase and a misuse phase. In the probing phase attackers tried to find accounts with weak passwords on VoIP servers with PSTN connections. After they successfully hijacked an account they tried to establish a call to one or more PSTN numbers to validate if the PSTN connection works and the country can be called from this VoIP server. In most cases another IP address is used for the misuse phase as for the probing phase. After a detailed analysis we can not find any source IP address from the misuse phase in the collected data from the honeynet without a PSTN connection.

VII. Discussion

The introduced honeynet setups are suitable for collecting and analyzing VoIP attacks. The honeynet setups collected a lot of data from attacks against VoIP systems and the systems show similar results of various analyses over the whole evaluation period. In some months we detected little deviations but over the whole evaluation period the peaks were compensated and similar results were identified. By comparing the results of the honeynet solutions we could identify, that heterogeneous honeynet implementations can increase the number of captured attacks from different attacking sources.

The research groups in Vienna and Essen validated the results of the analyses from each other and found the same results independently from each other. This indicates the correctness of the independent data collection and data analysis algorithms of the different approaches. Moreover, the comparison of the local honeynet evaluations with the global NorNet system has confirmed that the same attackers scan large network ranges by using the same tools and scan behaviors over a long period of time.

The behavior of toll fraud attacks for VoIP systems with an active connection to PSTN are similar to the behavior described in [28]. An attacker or a group of attackers found our VoIP system and tried to call PSTN numbers (called probing phase) to validate if a PSTN call can be established. If the probing phase is passed successfully the VoIP system is misused to forward costly calls. In most cases to African countries (e.g., Ethiopia or Sudan). The duration between identification of an active PSTN connection until the full consumption of the credits (i.e., €100) is only a few days. This means, that one weak password is enough to create high costs for the operator/user of the VoIP system. We also identified that attackers favor well-known VoIP systems (e.g., an Asterisk VoIP Server) instead of unknown or self-implemented VoIP servers. In our honeynets the Asterisk honeypots were accessed more often than other ones (e.g., the sipListener honeypots or the Dionaea Low Interaction Honeypots), which indicates that the attackers choose their victims selectively (e.g., based on the UA string). We also changed the IP addresses of the Asterisk and the sipListener honeypots to validate this behavior and we saw again a higher access rate to the Asterisk honeypots.

The similar behavior from the independent honeynet setups indicate that the results of a single honeynet can be used to make forecasts of VoIP attacks world-wide. In specific details the results may be different, however, the attackers scan large parts of the Internet in order to find vulnerable VoIP servers with different tools. These tools and other properties of the attacks can also be identified with a single honeynet. Global attack effects in the Internet can only be verified if multiple observation points are deployed in different countries, because a single honeypot has only a limited local view. With new sites added to the NorNet testbed we can easily extend the coverage of our monitoring system without spending effort in new local honeypot systems. Furthermore, the attack behavior could be changed in the future due to the fact that we already identified new attack tools like VAXSipUserAgent or a tool which uses random UA identifiers. This result verifies that attackers enhance their tools and that it is necessary to develop and improve attack detection and mitigation components.

VIII. Conclusion and Further Work

The researchers at Vienna University of Technology and at University of Duisburg-Essen designed and operated honeynet solutions for trapping VoIP attacks. Both groups operated the honeynets for more than five years and captured many VoIP attacks. To extend the view on the local results of Vienna and Essen we combined the approaches and used the data captured in Vienna and Essen to broaden the view on the state of the art of global VoIP attacks in the Internet.

The honeynet setups in Vienna as well as in Essen were designed independently, but cross-checked from each other to verify the results for this paper. By verifying the results of both universities we could increase the precision and confidence of the results, e.g., peaks in the number of attacks. Both, Vienna and Essen used assumptions in their previous publications which could be confirmed by the combined analyses, e.g., business model of toll fraud attacks. New insights into large scale VoIP attack behavior could be identified, e.g., attacker scanning behavior in different net segments.

As a part of the future work, the honeypots could be made more enhanced in functionality in order to trap more sophisticated attackers. For example, the use of an additional gateway from the honeynet to another external system or the use of other VoIP servers (maybe with known vulnerabilities) would make it more attractive to attackers. We saw that the different approaches work well, however, the solutions should be extended to capture on more different IP address ranges.

By combining the results of various honeynets with different research approaches, as applied by Vienna and Essen, validation of results was possible and new attack patterns could be found. With the high number of captured attacks precise analyses are possible which can further improve VoIP security protection mechanisms.

References

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

[2] L. Spitzner, "The Honeynet Project: Trapping the Hackers," *Security & Privacy Magazine, IEEE*, vol. 1, no. 2, pp. 15–23, 2003.

[3] ——, "Honeypots: Definition and Value of Honeypots," 2003.

[4] R. do Carmo, M. Nassar, and O. Festor, "Artemisa: An Open-source Honeypot Back-end to Support Security in VoIP Domains," in *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2011, pp. 361–368.

[5] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, 1st ed. Addison-Wesley Professional, 2007.

[6] H. J. Kang, Z.-L. Zhang, S. Ranjan, and A. Nucci, "SIP-based VoIP Traffic Behavior Profiling and its Applications," in *MineNet '07: Proceedings of the 3rd annual ACM workshop on Mining network data*, 2007, pp. 39–44.

[7] VoIP Security Alliance, "VOIPSA, VoIP Security and Privacy Threat Taxonomy," 2005, [Online], Available: http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf (accessed December 09, 2014).

[8] M. Nassar, R. State, and O. Festor, "VoIP Honeypot Architecture," in *10th IFIP/IEEE International Symposium on Itegrated Network Management*, 2007, pp. 109–118.

[9] M. Nassar, S. Niccolini, R. State, and T. Ewald, "Holistic VoIP Intrusion Detection and Prevention System," in *Proceedings of the 1st International Conference on Principles, Systems and Applications of IP Telecommunications*, ser. IPTComm '07, 2007, pp. 1–9.

[10] C. Valli, "An Analysis of Malfeasant Activity Directed at a VoIP Honeypot," 2010.

[11] S. Gauci, 2014, [Online], Available: http://blog.sipvicious.org (accessed December 09, 2014).

[12] A. Dainotti, A. King, K. Claffy, F. Papale, and A. Pescapè, "Analysis of a "/0" Stealth Scan From a Botnet," in *Proceedings of the 2012 ACM conference on Internet measurement*, 2012.

[13] J. Safarik, M. Voznak, F. Rezac, P. Partila, and K. Tomala, "Automatic Analysis of Attack Data From Distributed Honeypot Network," *Proc. SPIE, Mobile Multimedia/Image Processing, Security, and Applications*, vol. 8755, 2013.

[14] "Dionaea Honeypot," 2014, [Online], Available: http://dionaea.carnivore.it/ (accessed December 09, 2014).

[15] A. Aziz, D. Hoffstadt, E. Rathgeb, and T. Dreibholz, "A Distributed Infrastructure to Analyse SIP Attacks in the Internet," in *IFIP Networking Conference*, 2014, pp. 1–9.

[16] T. Dreibholz, "The NorNet Testbed: A Platform for Evaluating Multi-Path Transport in the Real-World Internet," in *Proceedings of the 87th IETF Meeting*, 2013.

[17] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RFC 3550: RTP – A Transport Protocol for Real-Time Applications," 2003.

[18] J. Franks, P. M. Hallam-Baker, J. Hostetler, S. D. Lawrence, P. J. Leach, A. Luotonen, and L. C. Stewart, "RFC 2617: HTTP Authentication – Basic and Digest Access Authentication," 1999.

[19] D. Hoffstadt, A. Marold, and E. Rathgeb, "Analysis of SIP-Based Threats Using a VoIP Honeynet System," in *11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012, pp. 541–548.

[20] I. Mokube and M. Adams, "Honeypots: Concepts, Approaches, and Challenges," in *Proceedings of the 45th Annual Southeast Regional Conference*, ser. ACM-SE 45, 2007, pp. 321–326.

[21] M. Gruber, F. Fankhauser, S. Taber, C. Schanes, and T. Grechenig, "Trapping and Analyzing Malicious VoIP Traffic Using a Honeynet Approach," in *The 6th International Conference on Internet Technology and Secured Transactions (ICITST)*, 2011, pp. 442–447.

[22] M. Gruber, C. Schanes, F. Fankhauser, M. Moutran, and T. Grechenig, "Architecture for Trapping Toll Fraud Attacks Using a VoIP Honeynet Approach," in *Network and System Security*, ser. Lecture Notes in Computer Science, J. Lopez, X. Huang, and R. Sandhu, Eds. Springer Berlin Heidelberg, 2013, vol. 7873, pp. 628–634.

[23] T. Raffetseder, C. Kruegel, and E. Kirda, "Detecting System Emulators," in *Information Security*, ser. Lecture Notes in Computer Science, J. Garay, A. Lenstra, M. Mambo, and R. Peralta, Eds. Springer Berlin / Heidelberg, 2007, vol. 4779, pp. 1–18.

[24] Digium Inc., *Asterisk.org*, 2014, [Online], Available: http://www.asterisk.org/ (accessed December 09, 2014).

[25] 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," in *International Conference on Communications (ICC)*, 2013, pp. 1968–1973.

[26] D. Hoffstadt, S. Monhof, and E. Rathgeb, "SIP Trace Recorder: Monitor and Analysis Tool for Threats in SIP-based Networks," in *8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2012, pp. 631–635.

[27] M. Gruber, F. Fankhauser, S. Taber, C. Schanes, and T. Grechenig, "Security Status of VoIP Based on the Observation of Real-World Attacks on a Honeynet," in *The Third IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*, 2011, pp. 1041–1047.

[28] M. Gruber, C. Schanes, F. Fankhauser, and T. Grechenig, "Voice Calls for Free: How the Black Market Establishes Free Phone Calls – Trapped and Uncovered by a VoIP Honeynet," in *Eleventh Annual International on Privacy, Security and Trust (PST)*, 2013, pp. 205–212.