Literature Review: A less attack-prone, Internet deployment of iLanga

Radu Courage Samuel
5 Carlisle Street Grahamstown 6139
Email: g11r3764@campus.ru.ac.za Cell: +2772 850 2466
Supervisors: Mosioua Tsietsi and Prof Afredo Terzoli
Computer Science Department, Rhodes University

June 2011

1 Introduction

iLanga is a Voice over Internet Protocol (VoIP) based telecommunication system developed at Rhodes University. Using iLanga, the voice information travels to its destination in individual network packets across the Internet. Contrary to the traditional Public Switched Telephone Network (PSTN) that works by carrying analog voice on copper wires over dedicated circuits. iLanga has a rich set of features that include interactive voice responses, music on hold, conferencing facilities, voicemail, call hold, call transfer, multiple lines and least cost routing. However, due to the nature of the Internet attacks, iLanga is likely to suffer these attacks regardless of its excellent features.

This literature review explores how attacks such as voice spam or Spam over Internet Telephony (SPIT), toll fraud, brute force attempt, Denial of Service (DoS) and Distributed Denial of Service (DDoS), and eavesdroppers [1] can be achieved. These attacks are mentioned as prevalent security issues within vulnerable VoIP networks [1]. Emphasis will be on using open source tools to add protection to the system. Furthermore, it looks into security for Linux, Asterisk Private Branch Exchange(PBX), MySQL database server and Kamailio proxy server as the components that make iLanga.

2 Vulnerabilities

2.1 Weak passwords

Passwords are used to verify a user's identity. Therefore, passwords used in authentication processes of any critical system should be strong as not to be cracked easily [2]. The first and generally the important key step of security mechanisms in computer systems is the password of the system users [2]. If the users choose their passwords without any restrictions on the characteristics of the key words or without any advice for strong characteristics, it is known that they pick the ones that will be remembered easily and be short. Then, those kinds of passwords have the potential to be the easy targets for password crackers and or system hackers. Therefore, only one "weak" password in the system might endanger the whole system security [2].

2.1.1 Attacks on password security

- According to Singh [3] the following are known methods of attack on password security.

  1. Observation - an intruder can watch while a password is being typed.
  2. Eavesdropping - an intruder can record the interaction between the user and the system and to out the password.
  3. Cryptanalysis - an intruder copies a password file and analyses it.
  4. Password search - a program can be used to carry out an exhaustive search for a password of a given length and maximum search are quoted for random passwords.

2.2 Brute force attacks

The attacker simply guesses username and password combinations until he finds one that works. Weak passwords are easily guessed. Automated tools can be used for brute force attacks that can make thousands of requests per minute with credentials generated from a large list of possible values [4].

According to Federal Bureau of Investigation (FBI) Situational Intelligence Report[1] of Charlort Division the following two scenario's happened:

1. "*In March 2009, the Charlotte Division was notified of an intrusion into a VoIP server located at an undisclosed corporation in Greenville, South Carolina. It was determined that the intruder, using a Romanian based IP address, first conducted a port scan and determined port 5060 was utilized on the compromised server. Port 5060 is the standard port used for Session Initiation Protocol (SIP). SIP is responsible for the setup, modification, and termination of sessions in an IP-based network and is typically the protocol used for VoIP servers. Then the hacker conducted a brute force attack and was able to crack the passwords to two extensions on the VoIP server due to weak passwords. The logs show several password attempts per second, indicating a script was used by the hacker. The hacker then proceeded to make 1,376 calls from the compromised phone extensions*

[1] http://publicintelligence.net/ufouo-fbi-voip-server-intrusions-in-north-carolina-banks-and-businesses/

attempting to trick victims into providing their bank account information. "

2. "*In February 2009, a non-profit organization located in Charlotte, North Carolina, experienced a computer intrusion into their VoIP server. A review of the server logs revealed IP addresses resolving to France and Florida as being responsible for the intrusion. The intrusion took place through port 5060 and compromised SIP on a server running Trixbox Community Edition. After gaining access, the hackers made approximately 1,850 calls from the compromised system. The calls were made to customers of small regional banks soliciting credit card information via touch-tone phone. After victims provided their account information, "money mules" across the country made ATM withdraws using the compromised accounts and sent a portion of the proceeds to Romania.* "

In the report analysis of the two cases it was noted that:

- Both attacks were made through port 5060.
- The intruders set up additional extensions on the compromised VoIP servers.
- They then notified victims of a problem with their financial accounts through automated phone calls or mass text messages to cell phones.

2.3 Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) attacks

2.3.1 DoS attack

A DoS attack is characterised by an explicit attempt to prevent the legitimate use of a service [5, 6].A network based DoS attack can be achieved in two basic attacks methods [5] :

1. By consuming available resources
2. By bringing the system to a faulty state

These two methods can be combined to consume the available resources by bringing several system processes into a state which needs a lot of resources. Limiting the availability by bringing the system into a faulty state requires compromise either the whole system or only a particular process [5] .

A DoS attack by flooding create resource exhaustion, long term busy signals, and force disconnections of in-session calls. Additionally, brute force attacks cause CPU depletion thus causing a DoS condition.

2.3.2 DDoS attack

A distributed denial of service attack uses multiple hosts to prevent legitimate users from using a service [4]. A DDoS attack is achieved the same way as a DoS attack but the difference is that in a DDoS attack there are multiple hosts. Attackers recruit multiple hosts by:

1. Automatically [4] scanning remote machines, looking for security holes. A discovered vulnerability is then exploited with attack code.
2. Distributing attack software by E-mail attachments and other digital means.

2.4 Toll fraud

Toll fraud refers to unauthorised access and use of a VoIP network which involves the establishment of toll bearing calls, especially to international toll numbers [1]. It is a serious threat because it utilises the organisations bandwidth and also incurs heavy costs.

2.5 Eavesdropping

Eavesdropping on VoIP networks or calls takes place when unauthorised third parties monitor call signal packets. By eavesdropping, third parties can learn user names, passwords, and phone numbers, thereby gaining control over dial plans, voicemail, call forwarding, and billing information [1]. More importantly, third parties may also gain access to confidential business and personal information by eavesdropping on actual VoIP conversations.

2.6 Spam over Internet Telephony (SPIT)

Spam is well known from the email paradigm. In general it refers to any unsolicited communication [7]. In the context of Internet Protocol (IP) telephony SPIT usually refers to unsolicited bulk calls [7, 8]. However, three different forms of SPIT are identified in[7]:

1. Call SPIT, which is defined as a bulk unsolicited set of session initiation attempts in order to establish a multimedia session.
2. Instant Message SPIT, which is defined as a bulk unsolicited set of instant messages.
3. Presence SPIT, which is defined as a bulk unsolicited set of presence requests in order the initiator of SPIT to become a member of the address book of a user or potentially of multiples users.

This is very common in VoIP because of low cost especially when applied over the public internet. Traditional voice networks do not suffer from unsolicited calls due to the large cost the caller has to pay to send voice spam over [7].Spam is not random but rather well planned and systematic.

3 Countermeasures

3.1 Password security

A strong or secure password is a password that can not be easily guessed or cracked .

- Guidelines[2] for creating a strong or secure password are :

  1. Do not use only words such as john or numbers such as 1234 or dictionary words such as jacaranda
  2. Do not use words in a foreign languages because password cracking programs check against word lists that encompass dictionaries of many languages.
  3. Do not use the same password for all machines. If one machine is compromised then other machines are safe.
  4. Do not write down your password. The best way is to memorise it.
  5. Do not use personal information when creating a password. If an attacker knows your identity, then your password can be easily deduced. Avoid using your date of birth or your name, etc
  6. Do not invert recognisable words. Inverting a bad password will never make it secure. An example nauj which is juan in inverted form.

- The following will enhance password strength as stated in :

  1. Make a password at least eight characters long. The longer the password, the better. Message Digest 5 (MD5) passwords should be 15 characters or longer while Data Encryption Standard (DES) passwords have a maximum of eight characters.
  2. Mix upper and lower case letters in a password.
  3. Mix letters and numbers in password especially in the middle rather than at the beginning or the end.
  4. Include non-alphanumeric characters such as $, &, and > to improve the strength of your password. This is no possible if using DES passwords.
  5. Always create a password that you can remember.

3.2 Ways to mitigate brute force attacks

Blake's paper [1] proposed the use of intrusion detection and other monitoring tools is the best way to detect brute force attacks. He added that checking logs for irregularities such as multiple log-on attempts. According to Digium the company that created Asterisk PBX system [9] fail2ban can be used as a reactive way to prevent brute force attempts. Kamailio 3.0.x version has inbuilt capabilities to block brute force as well as flooding.

[2] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel- sg-en-4/s1-wstation-pass.html

3.3 Ways to mitigate DoS and DDoS

In [4] the following are mentioned as system security mechanisms examples:

1. Applications that download and install security patches
2. Firewall systems
3. Intrusion detection systems
4. Worm defence systems

The above mentioned mechanisms should enable the victim to endure attack attempts without denying service to legitimate clients. This is done either by enforcing policies for resource consumption or by ensuring that abundant resources exist so that legitimate clients will not be affected by the attack.

3.4 Ways to mitigate toll fraud

Blake's paper [1] mentioned that checking VoIP logs can bring to light irregularities such as international calls made at odd hours.

3.5 Ways to mitigate eavesdropping

Virtual Local Area Network (VLAN) can be used to protect conversations from being eavesdropped [1]. This is because a VLAN is a closed loop of servers or computers that does not allow any other computer access to its network or facilities.

3.6 Ways to mitigate Spam over the Internet

The following are SPIT countermeasures and their weaknesses [10]:

3.6.1 Device Fingerprinting

The technique of active and passive fingerprinting works on the assumption that having knowledge about the type of User Agent that initiates a call, it helps finding out whether a session initiation attempt can be classified as SPIT or not. Comparing the header layout and order or the response behaviour of a SIP User Agent with a typical User Agent, it can determined if the initiated session establishment is an attack or a normal call.

- Weaknesses in device fingerprinting

If the attacker can order the field header in the same way as one standard client then passive fingerprinting mechanism can not detect the attack. The second weakness is that more and more phones are released and they have different Session Initiation Protocol (SIP) stack. This means that the attacker has to keep up to date with firmware upgrades.

3.6.2 White Lists, Black Lists, Grey Lists

1. White Lists - each user has a list that he accepts calls from and any caller who is not present in the list is blocked.
2. Black Lists - any call from a caller whose identity is present in the callee's Black List is blocked.
3. Grey Lists - on initial request of an unknown user (no in White List) the call is rejected and the identity is put in the Grey List. If the caller tries calling back within a short time period, the call will be accepted.

- Weaknesses of White Lists, Black Lists, Grey Lists

In White Lists mechanism an attacker can simply try out all existing accounts with a brute force attack until he finds out which identities are not blocked. Black Lists are bypassed by Direct IP Spitting. Grey Listing have the same weakness as the White Lists.

3.6.3 Reputation Systems

After receiving a call, the callee can set a reputation value for the caller, that marks this caller a Spitter or not. This reputation value is assigned to the identity of the caller and can be used for future requests. The assumption behind this assumption is that the reputation value will differ much between normal users and spitters.

- Weakness in Reputation Systems

The reputation has the same weaknesses as the Black Lists. The attacker can simply change the values in the header, when he uses Direct IP Spitting.

3.6.4 Turing tests

Turing tests or Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) are tests where the caller is given a challenge, that a human can solve easily and that is hard to solve for a machine. On initial call establishment attempt, the caller is transferred to an interactive system where he is challenged with a task, for instance, dialling 5 digits that he is hearing.

- Weakness in Turing tests

An attacker who can detect CAPTCHA and relay it to human solvers is able to bypass Turing tests.

3.6.5 Payments at risk

Payments at risk mechanisms can be used in order to demand payment from an unknown caller. The technique is described as follows: If user A wants to call user B, he must first send a small amount of money to user B. When user B accepts the call and confirms that the call is not a SPIT call, then the amount will be charged back.

- Weakness in Payments at Risk

This method requires high administrative overhead and more costs on service providers.

3.6.6 Intrusion Detection Mechanisms, Honey phones

Intrusion Detection Systems (IDS) are used to detect any kind of abnormal behaviour within a network. In the case of VoIP systems, it is used to monitor VoIP specific traffic. The IDS is designed as a defence mechanism against different VoIP specific attacks including scan attacks and SPIT attacks.

A Honeyport represents a part of a network that is not accessible by “normal” users and therefore any access to the honeyport can be viewed as an attack.

- Weakness in Intrusion Detection Mechanisms, Honey phones

The attacker can align his behaviour with the behaviour of normal user users, for example, adjust the call rate to 5 calls per hour. Additionally, an attacker can use, for instance, 100 different valid user accounts. In such a case it it harder for a monitoring system to detect attacks that originate from different sources. The practical problem with IDS in general is, that they base on statical assumptions, that are not verified. Where would be the borderline between normal usage and abrnomal usage? Honeypots have a disadvantage that they only detect access to invalid or unassigned accounts, this means that an attacker who only accesses valid accounts won’t be handled by a honeypot.

4 Linux security

4.1 Secure Shell (SSH) authentication

According to Ubuntu documentation[3] it recommends the use of public key authentication instead of passwords especially for SSH servers that are visible on Internet. With public key authentication, every computer has a public and a private key. Key-based authentication has several advantages over password authentication, for example the key values are significantly more difficult to brute force attack. SSH can use either Rivest-Shamir-Adleman (RSA) or Digital Signature Algorithm (DSA) keys. Both of these were considered state-of-the-art algorithms when SSH was invented. RSA is recommended over DSA because DSA has been seen as less secure in recent years.

[3] https://help.ubuntu.com/community/SSH/OpenSSH/Keys

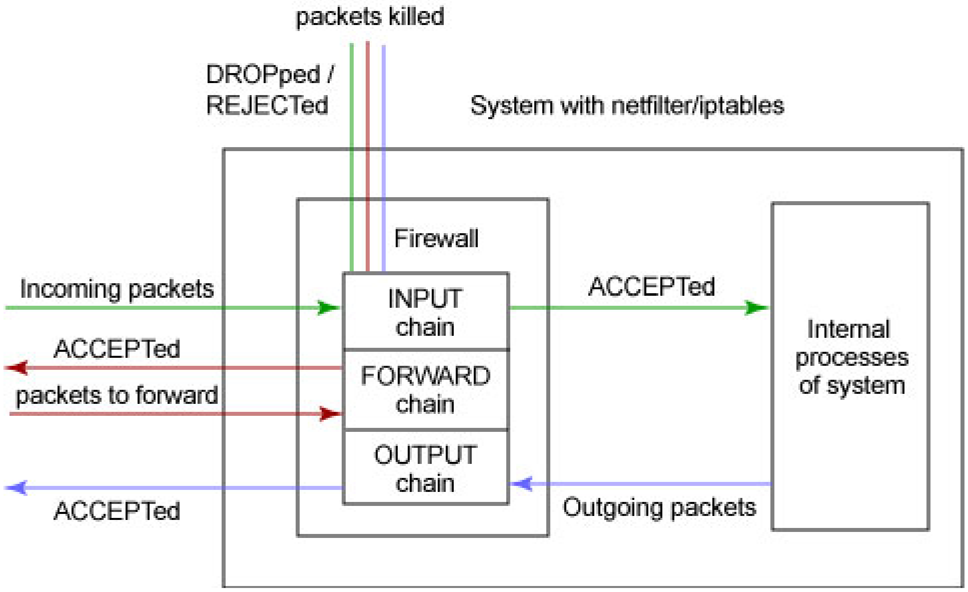

Figure 1: Packet filtering process.

4.2 Firewall

By instituting a firewall, you can prevent unauthorised access to services at the network level before an attacker is given the chance to exploit them. [11] Netfilter and IPtables are integrated in the Linux kernel since 2.4.x series and later series of kernels.

The netfilter/iptables IP filtering system is a powerful tool that is used to add, edit and remove the rules that a firewall follows while making packet filtering decisions. The rules are are grouped together into chains. The kernel defines three chains by default (INPUT, FORWARD, OUTPUT chains), but new chains can be specified and linked to the predefined chains [11]. Figure 1 shows the packet filtering process.

- Benefits of a firewall

  1. It is configured as a stateful firewall. A stateful firewall is capable of assigning and remembering the state of connections made for sending and receiving packets.
  2. Help understand where the threats to your system are coming from
  3. It gives administrator total control over firewall configuration and packet filtering.
  4. Administrator can make own rules that will suit specific needs
  5. It is an open source tool.

4.3 Hardening

A very important step in securing a Linux system is to determine the primary function or role of the server. You should have detailed knowledge of what is on your system. It is therefore critical to look at the default list of software packages and remove unneeded packages. For example you do no need to have Samba or Apache installed on your system if you do not need them.

- Benefits for removing unnecessary software packages;
  1. Fewer packages to update when security alerts are released.
  2. Unnecessary packages can be potential vectors for attackers.
- Drawbacks for removing unnecessary software packages:
  1. The process is time consuming.

5 Asterisk security

5.1 Basic security steps

As described in [9] there are seven basic steps to securing Asterisk. There are other complex and reactive methods which are also described in the advanced steps section 5.2 .

- The seven basic steps to secure asterisk.
  1. Don't accept SIP authentication from all IP addresses. In sip.conf file, there is an option to allow a reasonable subset of IP address to reach each user within this file.
  2. Set "alwaysauthreject=yes" in the sip.conf file. The default option is "alwaysauthreject=no" which causes information leakage. Setting it to "yes" will deny remote attackers to detect existing extensions with brute force guessing attacks.
  3. Use STRONG passwords for SIP entities. This is the most important step for a secure entity. A strong or secure password should have attributes mentioned in section 3.1
  4. Block your AMI manager ports. Use "permit=" and "deny=" lines in manager.conf to reduce inbound connections to known hosts only. Strong passwords are recommended here again.
  5. Allow only one or two calls at a time for SIP entities. This option limits your exposure to toll free calls.
  6. Make sure your SIP username are different from your extensions. While it is convenient to have extension "1000″ map to SIP entry "1000″ which is also SIP user "1000″, this is an easy target for attackers to guess SIP authentication names.

7. Ensure your [default] context is secure. Don't allow unauthenticated callers to reach any contexts that allow toll calls. Permit only a limited number of active calls through your default context (use the "GROUP" function as a counter.) Prohibit unauthenticated calls entirely (if you don't want them) by setting "allowguest=no" in the [general] part of sip.conf.

5.2 Advanced security steps

1. Asterisk hardening (slimming)

   Server hardening is very critcal because the elimination of anything not required will reduce the chance that the exploited vulnerability in the operating system can be used to gain access to the server and launch an attack [12] . The initial installation of Asterisk results in many dynamically loaded modules, providing the full suite of channel types, codecs, file formats, application commands, and accounting/database interfaces. Eliminating unneeded dynamic modules will lower the risk of security exploits[4] .

   - Benefits of slimming
     (a) Reduce the risk of security exploits.
     (b) Reduce memory clutter.
     (c) Improves performance.

2. Using fail2ban

   fail2ban is a tool to block unwanted IP addresses from accessing your server . It works along with iptables (linux firewall). The tool secures against unwanted SIP registration attempts, which is the most common type of attack on Asterisk servers. It checks the logs files for predefined patterns, and on finding a matching pattern blocks, the IP address which is responsible for generating that pattern.

- Benefits of using fail2ban

  1. The flexibility and integration with iptables/netfilter is a major benefit of fail2ban
     (a) Filtering is performed at the kernel-level.
     (b) Can handle more than one service: sshd (default), apache, vsftpd/proftpd, etc.
     (c) Can send e-mail notifications.
     (d) Can ban IPs for a limited amount of time and since 0.6.1 can also permanently ban hosts.

- Disadvantages of using fail2ban:

[4] http://www.voip-info.org/wiki/view/Asterisk+Slimming

1. An attacker can cause all users to be blocked by trying wrong passwords causing denial of service.
   (a) A Botnet can be used with many computers.

6 MySQL security

According to MySQL general security guidelines [13] , it emphasize the necessity for protecting the entire server host against all several types of applicable attacks such as eavesdropping, altering, playback, and denial of service. MySQL supports Secure Socket Layer (SSL) encrypted connections. It uses security based Access Control Lists (ACLs) for all connections, queries etc.

6.1 Guidelines when running MySQL

- The following should be considered:

  1. Only root accounts should be used to gain access to the user table in the mysql database.
  2. Do not grant more privileges than necessary. Use the GRANT and REVOKE statements for controlling access to MySQL.
  3. Do not store any plain text passwords in your database. Instead use MD5 or SHA1 or some other one-way hashing function and store the hash value.
  4. Use strong password. Password should not be from dictionary, easy to remember, alphanumeric, etc.
  5. Put MySQL behind a firewall.
  6. Do not transmit plain (unencrypted) data over the Internet. Use an encrypted protocol such as Secure Socket Layer (SSL) or Secure Shell (SSH).
  7. Use tcpdump to check whether MySQL data streams are unencrypted.

Access to the mysql.user table should never be granted to any non-administrative accounts. Log files should be located in a directory that restricts access only to the server and database administrator to prevent unwarranted exposure. Database backups that include tables or log files containing passwords should be protected using a restricted access mode.

6.2 Securing the initial MySQL accounts

On Linux systems there are different types of users namely: root and anonymous.

- Root account identification.

  User name is root.

- Root user capability.

  Each root account permits connections from the local host. Connections can be made by specifying the host-name and IP address.

- Anonymous account identification.

  They have empty user name. They have empty password.

- Anonymous user capability.

  Anyone can connect to MySQL server using this account. Connections can be made by specifying host-name and IP address

6.2.1 User accounts

The mysql.user grant table defines the initial MySQL user accounts and their access privileges. MySQL installation is insecure unless you do the following :

1. You should assign a password to each MySQL root account.
2. Assign password to anonymous accounts or rather remove them.

7 Kamailio security

7.1 Kamailio definition

Kamailio is an Open Source Server with the ability to handle thousands of call setups per second [14] . It can be used to build VoIP servicing platforms or to scale up SIP-to-PSTN gateways, Private Branch Exchange (PBX) systems and media servers like Asterisk.

7.1.1 Kamailio features

1. SIP routing capabilities
   - Serial and parallel forking
   - Stateless and transactional stateful proxy functions
   - Load balancing with many distribution algorithms and failover support
   - NAT traversal support for SIP
2. Secure communication
   - Digest SIP User authentication
   - TLS support for SIP signalling
   - Transparent handling of SRTP for secure audio
   - Authentication and authorization against database(MySQL database)

3. Interconnectivity

   - Straightforward interconnection with PSTN gateways
   - Interoperability with SIP-enabled devices and applications such as SIP phones

4. IP and DNS

   - It hides the topology of the network by hiding IP addresses in SIP headers to protect your network architecture.
   - IP level blacklists

7.1.2 Improvements in Kamailio 3.0.x version

- According to Mierla [15] there are improvements added to Kamailio 3.0.x configuration compared to previous versions.

  1. IP authentication can be enabled with the WITH_IPAUTH setting.
  2. TLS support can be enabled with the WITH_TLS setting.
  3. Detection of DoS attacks, it can be enabled with the WITH_ANTIFLOOD setting.
  4. Banning traffic from attacker IP addresses for a specific time interval.
  5. Better modularity and highlighting of functionalities such as registrar, location server, within-dialog request routing

7.1.3 Security benefits for using Kamailio 3.0.x version

- Kamailio handles Session initiation Protocol (SIP) signalling only.

- It can handle flood attacks and protect Asterisk, therefore it has increased security.

- Its load balancing properties enables it to handle several instances of Asterisk.

7.1.4 Other benefits for using Kamailio 3.0.x version

- Kamailio can act as a transport layer gateway because of its mature implementations for UDP, TCP, TLS and SCTP. It can therefore be used in front of Asterisk to translate between these protocols.

- In a distributed architecture, Kamailio can be configured to re-route the call if the Asterisk box does not react in a specified time.

8 Conclusion

This literature review described the main attacks that iLanga is likely to suffer when deployed. It described how certain attacks are achieved and possible ways to mitigate them. These attacks include brute force attacks, DoS and DDoS, eavesdropping and SPIT. The ways to mitigate have been discussed as preventive and reactive measures. Preventive measures ensures that the system is secure by server hardening, use of strong passwords, use of public key authentication for servers, use of firewall, etc. Reactive measures include the use of Intrusion Detection Systems, use of fail2ban to block attempted scans etc. It is important to note that a system's security is an incremental process, so the discussed countermeasures are the foundation. Finally, if these countermeasures are applied to iLanga, they will add protection to the system from attackers.

References

[1] Errol A. Blake. Network security: Voip security on data network–a guide. In *Proceedings of the 4th annual conference on Information security curriculum development*, InfoSecCD '07, pages 27:1–27:7, New York, NY, USA, 2007. ACM.

[2] Ilker Korkmaz and Mehmet Emin Dalkilic. The weak and the strong password preferences: a case study on turkish users. In *Proceedings of the 3rd international conference on Security of information and networks*, SIN '10, pages 56–61, New York, NY, USA, 2010. ACM.

[3] Kamaljit Singh. On improvements to password security. *SIGOPS Oper. Syst. Rev.*, 19:53–60, January 1985.

[4] Jelena Mirkovic and Peter Reiher. A taxonomy of ddos attack and ddos defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34:39–53, April 2004.

[5] Peter Steinbacher, Florian Fankhauser, Christian Schanes, and Thomas Grechenig. Black-box approach for testing quality of service in case of security incidents on the example of a sip-based voip service: work in progress. In *Principles, Systems and Applications of IP Telecommunications*, IPTComm '10, pages 101–110, New York, NY, USA, 2010. ACM.

[6] Nils Aschenbruck, Matthias Frank, Peter Martini, Jens Tolle, and Heinz dieter Richmann. Present and future challenges concerning dos-attacks against psaps in voip networks.

[7] M Theoharidou G F Marias D Gritzalis S Dritsas, J Mallios. Threat analysis of the session initiation protocol regarding spam, 2007.

[8] Vincent M. Quinten, Remco Meent van de, and Aiko Pras. Analysis of techniques for protection against spam over internet telephony. In Aiko Pras

and Marten Sinderen van, editors, *Dependable and Adaptable Networks and Services*, volume 4606 of *Lecture Notes in Computer Science*, pages 70–77, Berlin, July 2007. Springer Verlag.

[9] John Todd. Seven steps to better sip security with asterisk. http://blogs.digium.com/2009/03/28/sip-security/, March 2009.

[10] Dr. Andreas, U. Schmidt, Nicolai Kuntze, and Rachid El Khayari. Spam over internet telephony and how to deal with it.

[11] A. Lockhart. *Network security hacks*. Hacks series. O'Reilly, 2007.

[12] Jared Smith Jim Van Meggelen, Leif Madsen. *Asterisk: the future of telephony*. 2011.

[13] MySQL. Securing the initial mysql accounts. http://dev.mysql.com/doc/refman/5.0/en/default-privileges.html, 2011.

[14] Kamailio. Kamailio sip server project. http://www.kamailio.org/w/, 2010.

[15] Daniel-Constantin Mierla. Kamailio 3.1.x and asterisk 1.6.2 realtime integration using asterisk database. http://kb.asipto.com/asterisk:realtime:kamailio-3.1.x-asterisk-1.6.2-astdb, 2011.