Present and Future Challenges Concerning DoS-attacks against PSAPs in VoIP Networks

Nils Aschenbruck, Matthias Frank, Peter Martini
University of Bonn, Institute of Computer Science IV
Roemerstr. 164, D-53117 Bonn, Germany
{aschenbruck, matthew, martini}@cs.uni-bonn.de

Jens Tölle
FGAN - FKIE/KOM
Neuenahrer Strasse 20, D-53343 Wachtberg, Germany
toelle@fgan.de

Roland Legat, Heinz-Dieter Richmann
Stadt Köln, Berufsfeuerwehr
Scheibenstr. 13, D-50737 Cologne, Germany
{roland.legat, dieter.richmann}@stadt-koeln.de

Abstract

Nowadays, voice over IP (VoIP) telephony networks are connected to classic public switched telephony networks (PSTNs). Emergency calls from VoIP peers to PSTN public service answering points (PSAPs) are possible. Through the connection of IP networks and PSTNs the PSAP may be a victim of new, more powerful denial of service (DoS) attacks. This paper describes the present and future architecture of a PSAP. Based on measurements at a PSAP the challenge of attack detection at the PSAP is revealed. Furthermore, first solutions are pointed out and evaluated.

1 Introduction

In the past years Voice over IP (VoIP) telephony started to migrate from the research to the market. It is expected that in the future All-IP networks will substitute the classical Public Switched Telephony Networks (PSTNs). Nowadays, there is no All-IP network yet, but first steps have been made. There are different VoIP-providers which do not only provide telephony service between two VoIP peers, but also enable calls from VoIP to PSTNs and vice versa by providing gateway services between PSTN and VoIP networks.

When using VoIP, several challenges emerge concerning well-known services of the PSTN. One of these challenges is security in general (cf. [1]). Another is the emergency call. The challenge is to guarantee that emergency calls in VoIP networks reach the dedicated public service answering point (PSAP). For future All-IP networks, this challenge is met by the work of the Internet Engineering Task Force (IETF) Emergency Context Resolution with Internet Technologies (ECRIT) [14] working group. For present gateway services there are proprietary solutions like using one fixed PSAP for all users of one provider or the PSAP of the billing address.

Assuming that there are or will be solutions to deliver the call to the correct PSAP, the PSAP will be accessible by the IP network (e.g. the Internet). As a result of this connection there are further challenges concerning the security of the PSAP. There is especially the danger of denial of service (DoS) attacks. The aim of this paper is to point out the main threats and challenges concerning the PSAP. Furthermore, possible solutions in the area of intrusion detection and intrusion response are presented.

The rest of the paper is structured as follows. Section 2 introduces the architecture of present and future VoIP networks concerning the connection to the PSAP. Next, the threat of Denial of Service attacks in general and for the PSAP are described (section 3). After this, we describe intrusion detection in IP networks and point out some challenges for detection at the PSAP (section 4). Then, the ordinary load at a PSAP is described (section 5) to enable the evaluation of the presented solutions (section 6). Finally, we conclude the paper (section 7).

Proceedings of the Fourth IEEE International Workshop on Information Assurance (IWIA'06)
0-7695-2564-4/06 $20.00 © 2006 IEEE

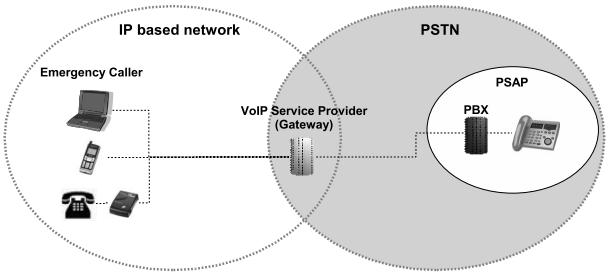

Figure 1. Present architecture from caller to PSAP

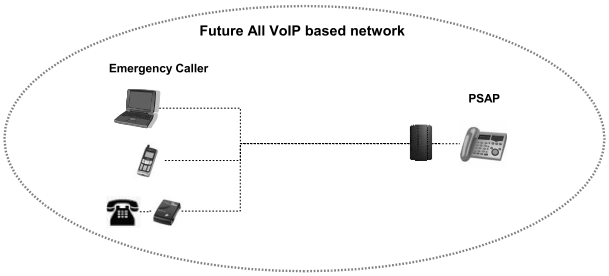

Figure 2. Future architecture from caller to PSAP

2 Architectures

This section describes the current and future network architecture from the emergency caller to the PSAP.

2.1 Architecture today:

The emergency caller is using VoIP telephony either via his personal computer (PC), via special VoIP hardware, or via special VoIP terminals/adapters which support using standard (non-voip) phones in VoIP networks (confer figure 1). The VoIP service provider provides gateway functionality and routes the emergency call to a certain PSAP. One challenge is to find the right PSAP as mentioned above. Nowadays, either a fixed PSAP (specific for one provider, e.g. the PSAP of a certain city) or the PSAP belonging to the billing address is used. Similar to the classical phone, the emergency units are sent to the address that the emergency caller has told the emergency callee. Furthermore, some VoIP service providers also support (compared to the classic phone) extended features like emergency calls when the caller is not able to speak or can merely speak stertorously. In this case the emergency units are sent to the billing address.

In Germany the PSAP is connected to the PSTN via several Integrated Services Digital Network (ISDN) interfaces. Several ISDN basic rate interfaces (S0), each containing two channels, or ISDN primary rate interfaces (S2m), each (in Europe) containing 30 channels, are used. At the PSAP a private branch exchange (PBX) system is used to distribute the calls between different PSAP agents. In case there are more calls than agents available the call is queued and the caller gets the call connected signal. In case there are more calls than ISDN channels no connection is possible and the caller gets a busy signal. In addition to the amount of channels a second bottleneck may be the PBX system. The number of calls per second of the used PBX system is limited. Thus, if there are too many calls at the same time the caller gets a busy signal. Pertaining to the PSTN connection and the call management a PSAP is similar to a call center.

2.2 Architecture in the future:

In the future there may be All-IP networks where the PSAP will be directly integrated in the IP network (confer figure 2). Thus, there is no gateway to the PSTN. VoIP is also used at the PSAP. This architecture, also concerning different solution and challenges especially for finding the dedicated PSAP, is the work of the IETF ECRIT working group and described in detail in [12].

3 Denial of Service attacks

In this section we give an overview on DoS attacks in IP networks before describing concrete attacks on the PSAP.

3.1 DoS in IP networks

The main goal of DoS attacks is not to gain access to networks and computers, but to deny the access to these systems for legitimate users. There are several ways to perform these kind of attacks and there are several reasons for the attackers to carry out DoS attacks.

Typical ways to carry out network DoS attacks are either the usage of (hand-) crafted network packets aimed at known vulnerabilities, or the generation of large quantities of network traffic to cause overload conditions.

An attack called *Ping of Death* is a famous early example for attacks aiming at known vulnerabilities. A crafted IP packet with a size larger than the specified maximum size was used to crash network stacks. Several versions of the operating systems MS Windows, Linux and BSD were vulnerable (see [13]).

The method of overloading networks or server hardware is commonly used by so-called *Distributed Denial of Service attacks*. Several of the large scale Internet worms seen in the last years included components to send network packets to selected IP addresses. When worm spreading was sufficiently successful, huge amounts of infected computers were available to overload network and server hardware.

Number	Description
+49	the national code for a country (here Germany)
112	the international emergency number (equal to 911)
34	further numbers - added to conceal the intension

Table 1. Possible attack promising cheap calls

Some of these worms even included the feature of a potential remote control of the infected computers to intensify the impact of the attack. An example for a worm containing a DoS component is [3].

Defense against this kind of DoS is difficult, especially if it is a distributed DoS. Packet filtering at routers as early as possible on the path to the victims to avoid overload situations is necessary. Spoofed IP source addresses makes this filtering even more difficult because there is no property of the packets left which is easy to recognize.

The are several reasons for the execution of DoS attacks, starting from base motives, revenge to harming business competitors. In business environments, published successful attacks may decrease the customer's trust. An additional reason for executing DoS is to cover or to allow advanced attacks. Security systems may break down under the load of the DoS attack enabling further attacks, or huge amounts of warning messages for the local security personnel may blind them to messages indicating the network or system intrusion.

3.2 DoS at the PSAP

The aim of a DoS attack on a PSAP may be to halt the operation of an entire emergency architecture [15]. The crucial danger of a denial of service attack on an emergency system is that it blocks victims of an emergency situation from any access to help, and such may cost life.

By using VoIP with emergency call support PCs are connected to the PSTN. Thus, it is possible to perform an attack with one or more PCs. Even without VoIP DoS on PSAP was possible. For example there could be an attack triggered by an SMS promising cheap calls when dialing "+4911234" (or similar numbers) before each number. Table 1 shows the details concerning this example. When calling the international emergency number the national code is ignored. Thus, all calls using such a number are routed to the next PSAP. The result would be overload at that PSAP caused by too many calls. The PSAP would not be able to answer real emergency calls due to the overload.

There is no conceptual difference between attacks like this one and new ones using VoIP - both try to attack by producing overload. The only difference is the power of the attack. While it was necessary to have enough wires or (in the wireless case) GSM-phones to perform such an attack without VoIP, one PC with the right software using VoIP can generate a huge amount of calls at once. Furthermore, several PCs (bot-networks [6]) may be used to reinforce the power of such an attack. Another scenario might be malware (malicious software e.g. a virus or worm) with an impact that causes a call to a PSAP at a certain time. This would be a synchronized distributed denial of service attack. Thus, by using VoIP it is a lot easier to perform a DoS attack on a PSAP.

Furthermore, in the future All-VoIP telephony networks there may be other attacks, e.g. SYN-Flooding, Replay-attacks, etc. [2] attacking the network connection of the PSAP. Even though these attacks are well known from other IP networks (cf. also the section before) and may be detected by network intrusion detection system, it is necessary to discuss the response when having detected an attack.

In general, the question is whether an overload DoS attack on a PSAP can be detected, and, in case it can be detected, whether there is there a possible response to keep the service alive.

4 Intrusion Detection

In the former sections the need of an attack detection was described. Due to the apparent similarity to the known DoS attacks in networks, it appears that applying classical Network Intrusion Detection and Intrusion Response techniques is a suitable approach. A more thorough analysis of the scenarios, however, reveals new challenges.

4.1 IDS basics

Basically, there are two main classes of Intrusion Detection Systems (IDSs). *Misuse Detection Systems* include a database of known attack methods and unwanted behavior. Pattern matching techniques are used to supervise network traffic and system usage. Whenever network usage or system usage as defined in the misuse database is seen, a warning message is generated and (if needed and configured) additional countermeasures may be initiated.

Anomaly Detection Systems rely on a pattern of *normal* system behavior. This pattern may be manually configured or learnt during normal system usage. Derivations from this normal pattern are regarded as an anomaly and a warning message is issued. Potentially, this method is the only Intrusion Detection approach which is capable of detecting new kinds of attacks and attacks not (yet) coded in attack databases.

The latter method seems to be the method of choice in the scenario described in this paper, but a closer look reveals some challenges.

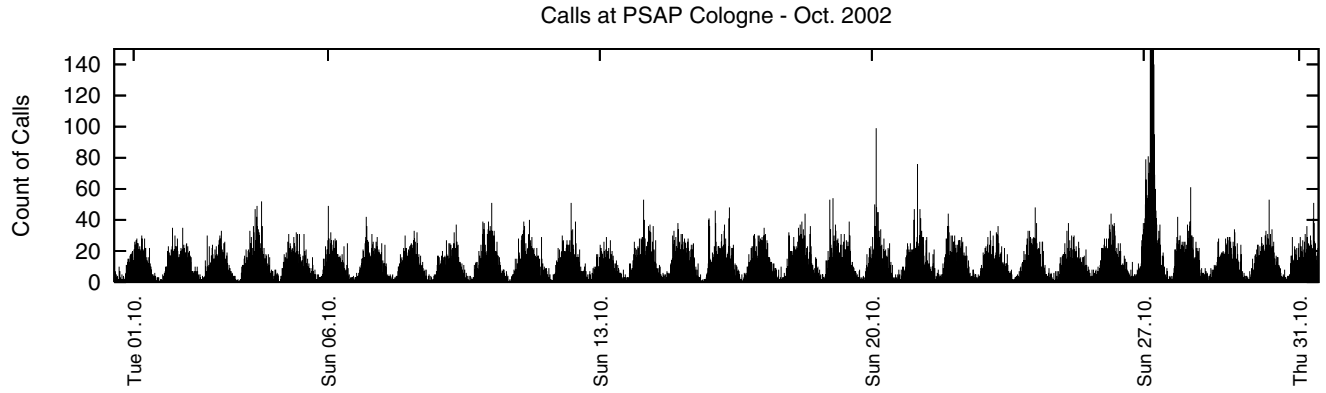

Figure 3. Calls at PSAP Cologne - Oct. 2002

4.2 Challenges

Since the first description of an anomaly detection approach was presented (see [4]), lots of enhancements were proposed and published, but main drawbacks are still not solved.

- Distinguishing between normal and abnormal system behavior is often not exactly possible.
- Unwanted user behavior does not necessarily lead to abnormal system behavior, while abnormal system behavior is not necessarily caused by unwanted user behavior.

  In the first case, an anomaly detection system stays silent and does not warn the security personnel. This is called a *false negative*. In the second case, an erroneous warning message is created and perhaps counter measures are triggered. This is called *false positive*. Depending on the configuration, this can even cause a self initiated DoS. A system causing false positives is not suitable for the supervision of incoming calls to PSAPs. In reverse, this means that suitable systems will imply the danger of considerable amounts of false negatives, because decreasing either number without fundamental change in methodology often leads to an increase in the other number. In general, the parameterization of an intrusion detection system is a trade-off between false negatives and false positives.

  At network intrusion detection some false positives are tolerated, because it is more important to minimize the false negatives. At a PSAP, when doing any kind of response (e.g. discarding calls), it is really important that no real emergency call is regarded as a failure. Thus, false positives can not be tolerated at PSAPs, because they may cost life.
- Some kinds of anomaly detection systems are just able to detect a general abnormal system state. It is not possible to identify the true reason for this anomaly warning. This feature makes a substantiated evaluation of incoming warning messages hard.

The major problem is that it is hard to estimate whether future DoS attacks show statistical properties which differ significantly from abnormal system behavior caused by masses of people calling a PSAP after a widely recognizable emergency. Thus, in the next section we will take a closer look at the load at one PSAP.

5 The ordinary Overload at a PSAP

To recognize the load at a PSAP, we examined several measurements of the Cologne fire department. It is one of the largest PSAPs in Germany and responding on emergency calls of about one million citizens. The measurements were taken at the PBX system with a granularity of 15 minutes. Figures 3 and 4 each show the calls for one month. Each difference between day and night is envisioned clearly by the periodical rises. Figure 3 was chosen because of a hurricane at the 27.10.2002 [5]. The hurricane can be figured out clearly by a large peak.

Figure 4 was chosen because of the World Youth Day which took place in Cologne in August 2005 and caused a significantly higher (more than 10%) amount of citizens in Cologne. The last few days (rises) of the figure show the calls during this event. It can be seen that the larger amount of citizens had only small impact on the amount of emergency calls.

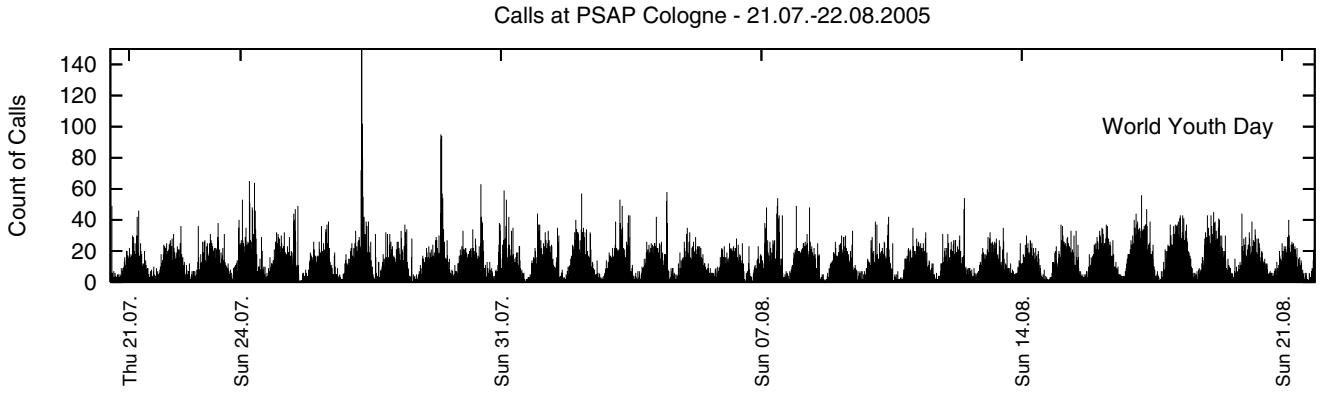

Figure 4. Calls at PSAP Cologne - 21.07.-22.08.2005

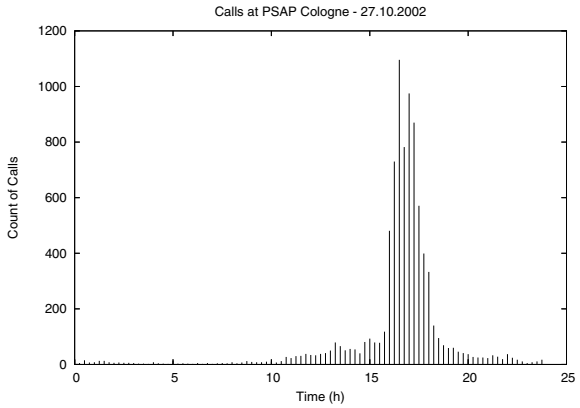

Figure 5. Calls at PSAP Cologne - 27.10.2002

Apart from this, there are small peaks at several days. The reason for these peaks are smaller emergencies. This shows that even relatively small emergencies may cause spontaneous strong rises. However, these arisings cause no overload at the PSAP.

In general, the figures show that the amount of calls is quite periodical. Anyway, in case of larger emergencies the amount of calls strongly varies as it can be clearly seen in figure 3. Such an overload occurs is ordinary at a PSAP. Figure 5 shows the calls for 24 hours containing the hours where the impact of the hurricane can be seen. The slope of the graph is exponential. This strong rise is reinforced by user behavior. When a user gets a busy signal he uses the re-dialing function and thus reinforces the peaks.

One indication to detect an abnormal state by anomaly detection systems is an exponential/heavy slope of load. Thus, larger emergencies may be detected as false positives. As mentioned before, false positives at a PSAP can not be tolerated. Thus, attack or intrusion detection at a PSAP is a fundamental challenge. The load at the PSAP strongly varies and it will be hard to distinguish between an attack and the "ordinary" emergency.

6 Possible solutions and further challenges

After having pointed out the challenge of attack detection and attack response for the PSAP, we will point out possible solutions and further challenges that evolve from the solutions.

6.1 Attack Detection

It seems to be impossible to distinguish between an emergency and an overload caused by a denial of service attack using only one agent. A solution may be to use two agents: the first sensing only calls that are performed by non-VoIP (classic PSTN, GSM, or UMTS) callers; the second sensing the calls that are performed by VoIP peers. In case of a real emergency similar to the hurricane in the figure above, both PSTN and VoIP calls will arise suddenly. In case only VoIP shows strong peaks, the probability of an attack seems significantly larger. It is implausible that there is a large emergency which only concerns VoIP users. An assumption for this solution is that one can distinguish between VoIP and non-VoIP calls. However, this is an administrative rather than a technical challenge.

In general this approach of using different agents for attack detection is similar to intrusion detection in coalition environments (cf. [11], [9], [10], [7]). The detection results of other agents are used to rate the detection results of a single one.

6.2 Attack Response

In case it is possible to detect attacks, what can be done in case there is an attack - what is the response? The solution of IP-Networks shutting down everything is definitely not possible, because no one will be able to use the PSAP anymore. It may be a solution to ignore all VoIP calls in case of an attack. However, one would victimize other callers and through this the attacker would have partially achieved its aim.

Another solution may be to use special queueing technologies. Non-VoIP calls could be prioritized against VoIP calls. Furthermore, if the location (geo-information) of the caller is also transmitted, new locations could be prioritized against already known ones. The probability that two callers of the same house or street will call because of the same emergency is high. Thus, a caller from another district should be prioritized. However, it is a technical challenge to include geographic information into the emergency calls. Anyway, this challenge has parallels with the one of finding the next PSAP automatically in case of using VoIP not at home (billing address).

7 Conclusion and Future Work

In this paper we described present and future architectures connecting the emergency caller with the PSAP. By using VoIP several new security challenges arise. It is not possible to use classical intrusion detection mechanisms due to the varying load at the PSAP. Large emergencies show similar characteristics as DoS attacks. Nevertheless, we pointed out first solutions to overcome these challenges. The idea is to use different agents for different network technologies to distinguish between an attack and an emergency. Attack response may be performed by implementing advanced queueing technologies at the PSAP. In the future, the ideas presented should be evaluated by simulation and test bed implementation. Furthermore, it should be evaluated whether the assumption pointed out for the different solutions can be satisfied. Besides, other potential security challenges for the PSAP like malware on mobiles (like [8]) should be analyzed.

References

[1] A. Adelsbach, A. Alkassar, K.-H. Garbe, M. Luzaic, M. Manulis, E. Scherer, J. Schwenk, and E. Siemens. VoIPSEC Studie zur Sicherheit von Voice over Internet Protocol. *Bundesamt für Sicherheit in der Informationstechnik*, 2005. `http://www.bsi.de/literat/studien/VoIP/`, [in German].

[2] C. Busch and S. Wolthusen. *Netzwerksicherheit*. Spektrum Akademischer Verlag, 2002. [in German].

[3] Carnegie Mellon Software Engineering Institute CERT Advisory. Code Red Worm. `http://www.cert.org/advisories/CA-2001-19.html`, 2002.

[4] D. E. Denning. An Intrusion Detection Model. *IEEE Transactions on Software Engineering, Vol. 13, p. 222*, 1987.

[5] Deutscher Wetterdienst. Jeanett, the first strong storm of autumn 2002. `http://www.dwd.de/en/FundE/Klima/KLIS/prod/spezial/sturm/index.htm`, 2002.

[6] T. Fischer. Botnetze. *12. DFN-CERT Workshop, "Sicherheit in vernetzten Systemen"*, 2005. [in German].

[7] N. gentschen Felde. Einsatz der graphbasierten Meldungsstrukturanalyse in domänenübergreifenden Meta-IDS. *Proc. of the GI Informatik 2005 - Workshop Sicherheit in komplexen, vernetzen Umgebungen*, 2005. [in German].

[8] Heise Security. Handy-Virus "in the wild" in Kalifornien gesichtet. `http://www.heise.de/security/news/meldung/56662`, 2005. [in German].

[9] M. Jahnke, S. Henkel, M. Bussmann, and J. Tölle. Components for Cooperative Intrusion Detection in Dynamic Coalition Environments. *Proc. RTO IST-041 Adaptive Defence in Unclassified Networks*, 2004.

[10] M. Jahnke, M. Lies, S. Henkel, M. Bussmann, and J. Tölle. Komponenten für kooperative Intrusion-Detection in dynamischen Koalitionsumgebungen. *Proc. of the GI Workshop on Detection of Intrusions and Malware a. Vulnerability Assessment (DIMVA)*, 2004. [in German].

[11] M. Lies, M. Jahnke, M. Bussmann, S. Henkel, and J. Tölle. Ein Intrusion-Warning-System für dynamische Koalitionsumgebungen. *11. DFN-CERT Workshop, "Sicherheit in vernetzten Systemen"*, 2004. [in German].

[12] H. Schulzrinne and R. Marshall. Requirements for Emergency Context Resolution with Internet Technologies. *IETF ECRIT Draft draft-schulzrinne-ecrit-requirements-01.txt*, 5 2005.

[13] Security Focus. Example for Vulnerability Warning: Ping of Death. `http://www.securityfocus.com/advisories/1457`, 1996.

[14] H. Tschofenig and M. Linsner. Emergency Context Resolution with Internet Technologies (ecrit) Charter. *`http://www.ietf.org/html.charters/ecrit-charter.html`*, 6 2005.

[15] H. Tschofenig, H. Schulzrinne, and M. Shanmugam. Security Threats and Requirements for Emergency Calling. *IETF ECRIT Draft draft-tschofenig-ecrit-security-threats-01.txt*, 7 2005.