# Analysis of a VoIP Attack

**Klaus Darilion, IPCom GmbH, klaus.darilion@ipcom.at**

**Abstract:** Recently, several IT news websites reported VoIP attacks against home users, containing lots of myths and incorrect statements. Unfortunately, they also give wrong security advices. This article analyzes the attacks and describes the motivations behind. Further, it shows simple workarounds how “insecure” software can be used in a secure way.

## 1 The Attack

### 1.1 Analysis

On 23.09.2008, heise.de reported an attack against VoIP devices of German VoIP users [heise]. This article references a thread in the IP-Phone-Forum [ipphone] in which people report that their VoIP phones started ringing in the middle of the night and displayed incoming calls from the phone number 5199362832664. One of the users presented a log file of a Patton SIP device which captured the suspect INVITE request:

```
02:12:42 SIP_TR> [GW] < Stack: from 213.130.74.70:3808
INVITE sip:810525551690000@1.2.3.4;transport=udp SIP/2.0
Via: SIP/2.0/UDP 213.130.74.70:3808;branch=100100101101011111101110
00100213.130.74.701.2.3.41863480914;rport
Max-Forwards: 100
From: <sip:5199362832664@1.2.3.4>;tag=21671132663-
 49852691621671132663216711326632l3.130.74.70
To: <sip:810525551690000@1.2.3.4>
Call-ID: 8376481110001110111001001011010110110011100100l011
 0101111110111000100213.130.74.701.2.3.41863480914f
 df238810525551690000021671132663-
 4509759162167113266321671132663213.130.74.70174046 6380
CSeq: 1 INVITE
Contact: <sip:fdf238@213.130.74.70:3808;transport=udp>
Content-Type: application/sdp
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK,
 REFER, REGISTER, SUBSCRIBE, UPDATE, PUBLISH
User-Agent: X-Lite release 1006e stamp 34025
Content-Length: 394
```

Let’s have a look at this SIP message. The funny thing is that absolutely nothing in this SIP message is trustworthy: Probably the SIP message has been received via UDP and the source IP address could be easily spoofed. Further, every data in the SIP message is user generated (in this case by the attacker) and does not necessarily reflect real data. Nevertheless, let us try to analyze the message:

- Source IP address 213.130.74.70 and source port 3808: Although the IP address could be easily spoofed, in this case it may be the real address of the attacker as the IP address is also present in the Via: header (used for sending back responses). Further, if the attacker wants to know the result of the attack, he has to receive the SIP responses meaning that he has to provide his real IP address.
- The Call-ID looks like a random string and contains the source IP address. As the Call-ID is invalid (per RFC 3261 the Call-ID must not contain spaces), it can be assumed that the attacker did not use a full-fledged SIP stack, but some scripts to generate the request.
- The User-Agent header displays “X-Lite” as client. However, if you compare the above request with an INVITE request sent by X-Lite you will find out that the random strings (call-id, tags, branch

parameter) do have a different style. Thus, this message for sure was not generated by X-Lite and this user agent header was probably used for obfuscation.

- The caller identity is sip:5199362832664@1.2.3.4. Fur sure the domain part is faked (1.2.3.4 is in a reserved IP address block), and the user part probably too – why should the attacker reveal its real identity? Often, the user part of SIP URIs is used to signal telephone numbers. If the user part is considered as phone number it may be seen as an international phone number without the international access code: 51 would indicate Peru, and according to the Peruvian numbering plane [ITU] this would be an invalid mobile phone number in the area of Lima (invalid as it exceeds the fixed length of 9 digits).

So what would be the intention behind such an attack? The news reports made the following presumptions:

> [cio] "…Der Angriff zielte offenkundig direkt auf die Hardware der Kunden, um kostenpflichtige Rückrufe zu provozieren. Bei fehlerhaften Konfigurationen von Asterisk-Anlagen sollen diese aber automatisch erfolgt sein…."
> which means: "The attackers intention was to trigger costly callbacks. In case of misconfigured Asterisk installations, the callback may be performed automatically."

The attack was targeted against German VoIP users. For those, usually the German dialing plan is used. Thus, the number 5199362832664 would be interpreted as local number, which may be invalid at all. Even if the user's telephony provider had accepted this number as international phone number (without the usual '+' or '00' prefix), then, according to the quoted report, the attack would have triggered a phone call to an invalid Peruvian mobile number. This may cause costs to the caller, but has no benefit for the attacker.

Further, configuring automatic callbacks with Asterisk is a complicated task. Thus, it is unlikely to achieve automatic callbacks due to misconfiguration.

So, what could have been the real intention of this attack? To find out the hackers intention it is useful to analyze the impact of this attack. The impact may differ whether the attack's victim is a SIP phone or a SIP server[1].

## 1.2 Impact on SIP Phones

If the above INVITE request is sent to a SIP phone, and the SIP phone accepts the request, the SIP phone will probably start ringing and inform the user about an incoming SIP call. As caller identity, the SIP phone should display 5199362832664@1.2.3.4. Unfortunately, as some SIP phones only have limited display capabilities, or are implemented to just replace PSTN features, such phones will display only the digits of the user part, e.g.: 5199362832664.

The effect is that the user gets disturbed by an unknown calling party. Further, if the user has configured call forwarding, the call gets forwarded and may cause costs to the user (there is no difference to the PSTN – if you configure call forwarding on your mobile phone you have to pay for the forwarding).

## 1.3 Impact on SIP Servers

The impact on SIP servers may be much more substantial. Usually the SIP server will analyze the requested target and forward the request depending on this target. The requested target is identified by the request URI – in the above example this is "sip:810525551690000@1.2.3.4".

If the receiver is a PBX, it usually tries to find a local extension that matches the user part of the request URI (810525551690000). If there is no such local extension, the call will either be forwarded to a default extension or rejected.

[1] The term "SIP server" is an undefined term, but often used to describe SIP elements other than SIP phones. In this article, the term "SIP server" will be used to describe proxies, gateways or PBXs.

If the receiver is a SIP proxy, it should reject the call, as the proxy is not authoritative for the domain 1.2.3.4. Unfortunately, many SIP proxy setups ignore the domain part and just analyze the user part of the request URI, and if it is similar to a phone number it will be forwarded  to a gateway.

If the receiver is a SIP/PSTN gateway that accepts SIP requests from everywhere and the number in the request URI matches the dialing plan at the gateway, then the gateway will forward the call into the PSTN.

In the SIP proxy or SIP gateway scenario, if the call is accepted and forwarded into the PSTN, there is massive potential for fraud. Of course, if the PBX has an included gateway (or a SIP trunk to a gateway provider) and does not control access to this resource, then there is also fraud potential for PBX users (e.g. Asterisk installations). In order for the attacker to find out if the call attempt is successful, it will analyze the SIP responses, e.g. a 180 or 183 response message indicates that the request will be handled somewhere.

## 1.4 Real Intention of the Attack

Based on the previous impact analysis there are two possible intentions of the attacker:

- disturbing users
- detection of insecure gateways for illegal PSTN termination

Unless the attacker just wanted to disturb VoIP users, the real motivation is to find insecure gateways for terminating calls into the PSTN via these gateways. The attacker can sell PSTN termination to VoIP service providers using the detected insecure gateways. It may even happen that the VoIP provider does not know that it is routing PSTN traffic via a “hacked” gateway. Finally, the attacker gets money from the VoIP provider (or is a VoIP provider itself) for terminating the calls, but the termination costs will be charged to the owner of the gateway.

[honey] also reported about similar attacks against two Norway companies, coming to the same conclusion, that the attack is targeted to find insecure gateways.

## 1.5 Useless Proposed Solutions

In [ipphone] some users recommended to block incoming phone calls from the number 5199362832664. This of course will help to reject INVITEs that have this phone number in the From URI, but it does not solve the problem generally. As soon as the attacker uses another From-URI (which might be a random number used by the attacker), the filter list does not match anymore and the user gets disturbed again.

[honey] proposes some solutions which do not help in this scenario, like:

> “Use VPN tunnels to protect the VoIP traffic going over the Internet”

This helps you to protect the VoIP traffic, but as long as the SIP server is reachable from the Internet, the SIP server itself must be secured too.

> “Use SIP TLS and SRTP if possible (we are waiting on hardware manufacturers here as well)”

Using TLS and SRTP allows you to encrypt your VoIP traffic, but it does not prevent attacks against your SIP servers. Usually only the SIP server provides a certificate, client certificates are rarely use. Thus. the attackers can use TLS and SRTP too.

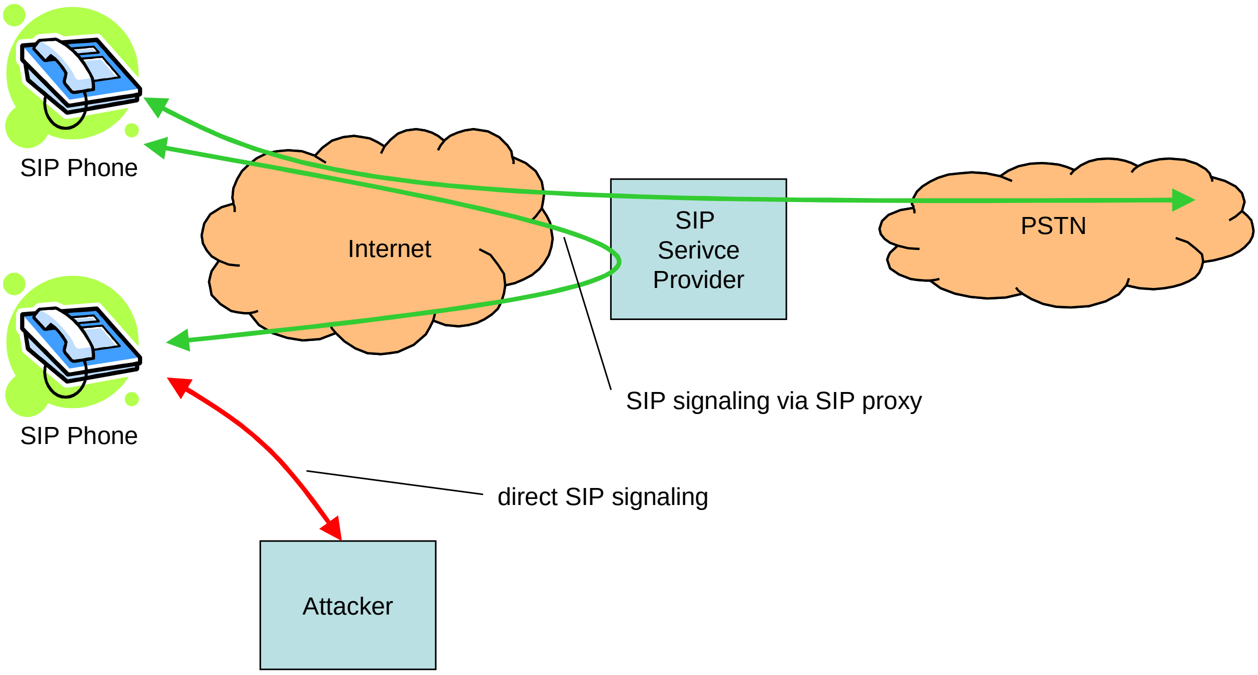
The following sections will discuss the cause of the problems.

# 2 Cause Analysis

Again, it is useful to differ between SIP phones and SIP server software as attack target.

## 2.1 SIP Phones

The SIP protocol as defined in RFC 3261 allows the direct communication between SIP clients – without any server software in-between. Therefore SIP phones should allow incoming SIP messages from any source IP addresses. However, in most scenarios this is not necessary. Usually the SIP phone registers its SIP address[2] to the SIP Proxy (Registrar) of its domain. Further, the SIP proxies usually perform record-routing to relay between the caller and callee for the whole duration of the dialog (this is for example necessary for NAT traversal and accounting). Thus, the whole SIP traffic is usually exchanged between the SIP phone and the SIP proxy (there can be multiple SIP proxies if there are multiple NAPTR, SRV or A records for the respective domain) and the SIP phone should ignore SIP messages from sources different to the SIP proxy it registers with.



For example, the SNOM phones have a configuration option[3] to allow this behavior. If the SIP phone does not offer such a configuration option, as a workaround the SIP phone can be placed behind a NAT. The NAT allows incoming packets only if there was a foregoing outgoing packet to the same address. Although NAT devices may cause problems with VoIP, they can improve overall system security.

For SIP phones which are not secured by NAT, e.g. various terminal adaptors included in NAT routers like Fritz!Box Fon, a workaround is to change the default port. Many SIP phones use the local UDP port 5060 for SIP communication although there is no need for that. It would be much more secure if the SIP device chooses a random port for SIP signaling. If the device does not support random SIP ports, the port should be changed to an arbitrary selected port instead of the mostly used default setting 5060[4].

[2] SIP Address of Record (AoR), the public SIP identity, e.g. sip:klaus.darilion@ipcom.at

[3] http://wiki.snom.com/wiki/index.php/Settings/filter_registrar

[4] Random means, that the SIP client chooses a random port during startup and then use this port for sending and receiving of SIP messages as long as the SIP client is running. Further, do not confuse with the port of the SIP

Another problem is that most of the SIP phones accept any request URI on incoming calls. Usually, on incoming call the request URI matches the Contact-URI in the REGISTER request. The INVITE request shown in section 1.1 clearly contains a random identity in the request URI. Thus, it should be rejected. In difference to the previous weakness, which is actually due to the SIP standard, this behavior is in contrast to the standard:

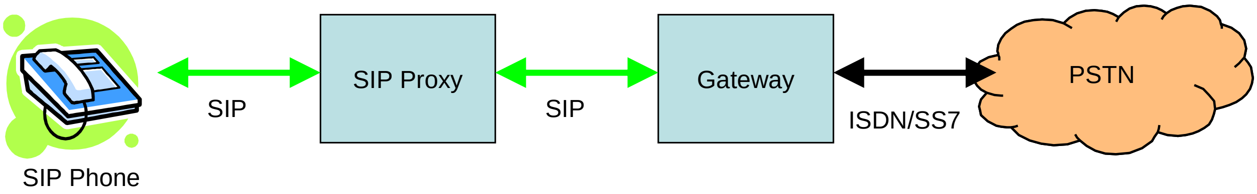
> RFC 3261 section 8.2.2.1: "…If the Request-URI does not identify an address that the UAS is willing to accept requests for, it SHOULD reject the request with a 404 (Not Found) response. Typically, a UA that uses the REGISTER method to bind its address-of-record to a specific contact address will see requests whose Request-URI equals that contact address…"

SIP phones should reject incoming calls if the request URI of the incoming request does not match the previously registered contact URI.

## *2.2 SIP Servers*

For SIP servers the situation is different, as e.g. proxies have to accept incoming SIP messages from any IP address because of user mobility. Nevertheless, they should apply restrictions before forwarding calls into the PSTN, and gateways should only accept SIP messages from trusted sources.

The following picture shows a typical SIP service provider setup:



The SIP proxy receives the call from the SIP phone, performs call processing and forwards the call to the PSTN gateway. To find out if the caller is allowed to make PSTN calls, the SIP proxy has to identify the caller – usually by requiring authentication. If a caller cannot authenticate against the SIP proxy he is not allowed to use gateway resources. Further, the gateway should only accept SIP messages from trusted sources like the SIP proxy.

The same is of course also important if an IP PBX is used. In this case, the gateway is often part of the PBX (e.g. via an ISDN interface card) or a SIP trunk to a gateway provider is used. Again, it has to be ensured that the caller is identified and gateway resources are only granted for authorized users.

# 3 Countermeasures

Fortunately, securing the SIP infrastructure is rather easy. Administrators should review the configuration of the SIP proxies and gateways to avoid unauthorized access to gateway resources. This includes for example:

- apply access restrictions for the SIP proxy, PBX or gateway depending on source IP address: Some applications allow different handling of SIP messages depending on the source address. If the software does not support this, either a dedicated firewall or internal firewall (like iptables or Cisco's IP access lists) should be used to filter directly on IP level. Actually, applying both, access lists on IP level and in the SIP software, is the preferred choice.

server. Servers do listen on the well known port 5060, but there is no need for the SIP client to locally listen on the well known port, as the SIP server will learn the local port during registration.

- authenticate users and restrict granted resources: If filtering on IP level is not possible (e.g., the SIP proxy of a SIP service provider must accept SIP messages from everywhere), the users need to be authenticated (typically using SIP's digest authentication) to apply authorization rules.
- hardened SIP proxies: There are various ways to bypass authentication (like UDP source address spoofing, loose routing …) – ask an expert to review you configuration, especially if your SIP proxy requires low-level configuration[5], which requires deep knowledge of SIP for correct configuration.
- hardened PBXs: Make sure that unauthenticated incoming calls (e.g. received via SIP or ISDN) are not allowed to access PSTN resources. How this is done depends of course on the used PBX and guidelines for all various PBXs would exceed the scope of this document. Nevertheless, as Asterisk is the most popular PBX and many people use it without really understanding it, a short description for Asterisk based PBXs follows:

  1. Configure a password for all provisioned SIP phones
  2. Apply a different context for authenticated and non-authenticated incoming SIP requests. For example use *context=default* in the *[general]* section, and use *context=authorized* in the respective SIP phone configuration settings in sip.conf.
  3. In extensions.conf, make different "service" contexts e g.:

     ```
     [toPSTN]
     exten => _00X.,1,Dial(Zap/${EXTEN})

     [toLocalExtensions]
     exten => 350,1,Dial(SIP/350)
     exten => 351,1,Dial(SIP/351)
     exten => 352,1,Dial(SIP/352)
     ```

  4. In extensions.conf include the allowed "service" contexts according to the permissions of the incoming user:

     ```
     [default]
     include => toLocalExtensions

     [authorized]
     include => toLocalExtensions
     include => toPSTN
     ```

Although the attack was not targeted against SIP phones, it is unwanted that an anonymous user disturbs you at 3am in the morning by performing SIP port scans. Hence, also end users should protect their SIP phones, for instance:

- locally, use a random SIP port for sending and receiving SIP messages, or at least configure a port other than 5060
- reject or ignore incoming SIP messages except from the SIP proxy
- if your SIP phone does not support the above workarounds, put your SIP phone behind NAT

[5] The ser family of SIP proxies – ser, Openser, Kamailio, OpenSIPS – are considered to have low-level configuration.

# 4 Conclusion

The recently detected SIP attacks were targeted to find insecure PSTN gateways. Operating an insecure gateway may cause massive costs to the operator of the gateway as the gateway can be abused for illegally terminating calls into the PSTN. These first attacks should alarm administrators to review the configuration of their SIP servers. To avoid unauthorized access to gateway resources the above described countermeasures should by applied. Further, although end users are not as exposed as providers of SIP servers, they should apply countermeasures too.

# 5 References

| | |
|---|---|
| [heise] | http://www.heise.de/newsticker/Erste-groessere-Attacke-gegen-deutsche-VoIP-Nutzer--/meldung/116335 |
| [ipphone] | http://www.ip-phone-forum.de/showthread.php?t=174567 |
| [cio] | http://www.cio.de/knowledgecenter/netzwerk/859255/index.html |
| [honey] | http://www.honeynor.no/2008/10/19/voip-attacks-are-escalating/ |
| [ITU] | http://www.itu.int/oth/T02020000A6/en |

Klaus Darilion received both, his Diploma Degree and his Dr. Degree in electrical engineering, from Vienna University of Technology. He is currently employed as systems engineer at IPCom were he provides SIP solutions to service providers, VoIP consulting, SIP security trainings and SIP security audits. Klaus Darilion is active contributor to the Kamailio SIP Proxy and Asterisk open source projects.

For information about SIP security, trainings or audits please contact Klaus Darilion: klaus.darilion@ipcom.at, +43 1 5056416 36