How to exploit the SIP Digest Leak vulnerability

(By using VOIPPACK)

By: Sandro Gauci (sandro@enablesecurity.com)

Date: 26 March 2009

Last updated: 01 April 2009

Introduction

The SIP Digest Leak is a vulnerability that affects a large number of SIP Phones, including both hardware and software IP Phones as well as phone adapters (VoIP to analogue). The vulnerability allows leakage of the Digest authentication response, which is computed from the password. An offline password attack is then possible and can recover most passwords based on the challenge response.

By making use of sipdigestleak.py which is included in VOIPPACK, one can automate the process of getting the phone to ring, obtaining a challenge response and performing a bruteforce attack. In this tutorial we shall be looking at how this module makes the whole process an easy task.

Basic Requirements

- Gizmo5
- VOIPPACK March edition

Optional

- A hardware IP Phone or phone adapter (using a Linksys SPA2102 in our case)

After following this tutorial you will be able to:

- Understand how the SIP Digest Leak attack works
- Be able to get an IP Phone to ring
- Get the IP Phone to leak the challenge response
- Recover the password

Need to know:

- SIP is a protocol used for signaling that looks like HTTP
- Each SIP entity sends out SIP messages that could be anything from INVITE, BYE, CANCEL and so on
- INVITE SIP messages initiate a phone call, i.e. they get a phone to ring

Understanding the attack

Vulnerability scenario:

1. An IP Phone (victim) is listening on port 5060, accepting phone calls
2. The attacker sends an INVITE to the IP Phone
3. The victim phone starts ringing and someone picks up and hangs up (because no one answers the phone at the other end)
4. When the phone is hung up, the victim phone sends a BYE to the attacker
5. The attacker issues a 407 response that asks for authentication and issues an authentication challenge
6. The victim phone provides a response to the authentication challenge in a second BYE
7. The attacker can then issue a brute-force attack on the challenge response on his local machine (or distributed network etc) and guess the password

More details will be at the EnableSecurity Research page:

http://enablesecurity.com/research

Therefore the attack has the following requirements:

- We need to know how to ring the phone
- The victim needs to hang up

Setting up the IP Phone

Making use of Gizmo5

Installation of Gizmo5 is very straightforward especially since it does not require a PBX but instead makes use of SIPphone's PBX servers. Unlike other SIP phones, Gizmo5 listens on UDP port 64064 instead of 5060 or some random high port.

Upon installation, Gizmo5 will ask you to create a new account. Set the password to an easy pattern such as "2323", so that the offline password cracker will have no problem cracking it.

Getting an IP Phone to ring

Gizmo5

In the case of Gizmo5, the IP Phone does not discriminate INVITE messages based on any specific extension to be specified when it is called. This means that this software phone will happily ring on any extension as long as another SIP phone sends it an “INVITE” message on port 64064. This makes this phone an easy target for our demonstration.

To test this make use of the “sipphonecall” module:

- From the classic node view make sure that the IP address of the host where you installed Gizmo5 is the current target
- Also make sure that the correct interface is set as the callback interface
- Double click on “sipphonecall” under the Tools
- Change the “Port” field to 64064 instead of 5060
- Click on OK

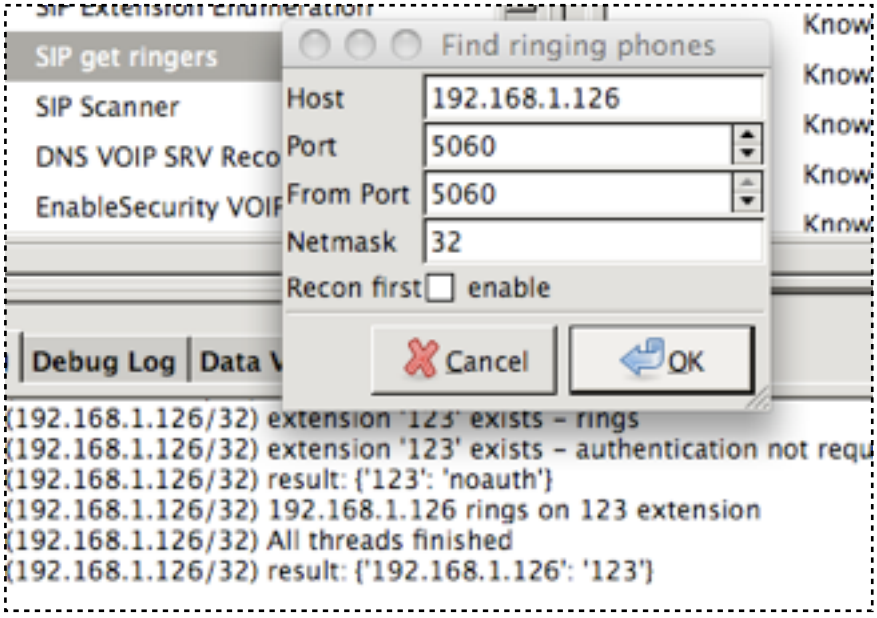
Linksys SPA2102

In the case of a Linksys phone adapter, we need to know the extension of the phone to be able to call it. This can be done by intelligent brute-force when the range of extensions is known and pattern guessing. A script is included in the March edition of VOIPPACK called sipgetringers.py that automates this process. This is also used by sipdigestleak.py during the initial / reconnaissance stage. A number of hardphones and embedded SIP devices will also only ring on the extension that they are configured to work with.

In our case we set the user id to “123” as can be seen from the screenshot of the HTTP interface:

To test this make use of the “sipgetringers” module:

- From the classic node view make sure that the IP address of the target SIP phone
- Also make sure that the correct interface is set as the callback interface
- Double click on “sipgetringers” under the Recon
- Make sure that the “Port” is 5060 (or the correct port on your device)
- Click on OK



Leaking out the Challenge Response

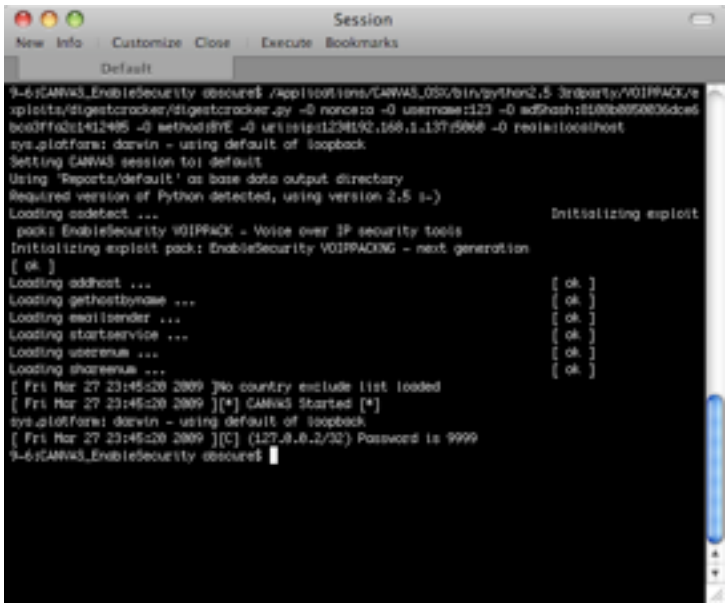
Once you know how to get the target phone to ring, it is time to get down to business:

- From tools double click on sipdigestleak
- The phone will start ringing
- Pick it up and hang up
- SIP Digest Leak tool will receive the hash and mount a short offline bruteforce attack which breaks most short pin codes / passwords

```
(192.168.1.126/32) Proxy auth: ['Digest username="123",realm="localhos
te6bca3ffa2c1412405"']
(192.168.1.126/32) The phone rings on extension 123
(192.168.1.126/32) Launching the password cracker
(192.168.1.126/32) Password is 9999
(192.168.1.126/32) username: 123
(192.168.1.126/32) nonce: a
(192.168.1.126/32) realm: localhost
(192.168.1.126/32) passwd: 9999
(192.168.1.126/32) uri: sip:123@192.168.1.137:5060
(192.168.1.126/32) method: BYE
(192.168.1.126/32) response: 8108b0850036dce6bca3ffa2c1412405
```

There will be times when the password is not easy to crack. For that reason is it best to make use of the DigestCracker tool that is included with VOIPPACK. To run this tool from the command line provide the details obtained through sipdigestleak. For example:

python2.5 3rdparty/VOIPPACK/exploits/digestcracker/digestcracker.py -O nonce:a -O username:123 -O md5hash:8108b0850036dce6bca3ffa2c1412405 -O method:BYE -O uri:sip:123@192.168.1.137:5060 -O realm:localhost



Conclusion

That is all for this tutorial. If you have any comments or additional content please email me sandro@enablesecurity.com.

About EnableSecurity:

EnableSecurity is dedicated to providing high quality Information Security Consultancy, Research and Development. EnableSecurity develops security tools such as VOIPPACK (for Immunity CANVAS) and SIPVicious. EnableSecurity is focused on analysis of security challenges and providing solutions to such threats. EnableSecurity works on developing custom targeted security solutions, as well as working with existing off the shelf security tools to provide the best results for their customers. More info at enablesecurity.com