International Visual Voicemail Security

43 messages

Shubham Shah <> Sun, Jul 6, 2014 at 10:39 PM
To: jmoran@gsma.com
Cc: Ben Grubb <bgrubb@fairfaxmedia.com.au>,

Hi James,

In the last few months, I have been on an investigative path to breaking voicemail security. Whilst complying, co-operating and assisting mobile service providers to get any issues fixed, I was recommended to inform you to see if we could work together to help get this issue patched globally.

In May 2014, I started taking a look through the visual voicemail protocol and how many major providers handle the implementation of visual voicemail. This specification, itself, is found on the GSMA website: http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpvvmspecification12.pdf.

Whilst there are multiple ways to implement authentication on visual voicemail services, it seems that there is a pattern of insecurity when using a particular method of authentication.

Most providers which seem to implement visual voicemail authentication through a pin based password method are most likely vulnerable to bruteforce attacks.

I was able to find, that at least in Australia for Vodafone, they were vulnerable to such bruteforce attacks, effectively proving it extremely easy to obtain any numbers voicemail pin.

I can confirm that Vodafone has now rolled out patches for this issue in at least Australia and I hope globally also if other countries were affected.

Below is a short technical write up relating to the vulnerability, which is made possible thanks to visual voicemail and Vodafone's implementation of it and lack of bruteforce protection.

Pre-requisites:
- Python 3 (Obtainable from here: https://www.python.org/download/releases/)
- Python futures library: install via pip3 install futures
- PoC Script (Attached)

Description of vulnerability:

Vodafone's visual voicemail system is susceptible to bruteforce attacks as it does not enforce any rate limiting or password policy rules. Due to this, all Vodafone customers are currently vulnerable to their voicemails being broken into. If Vodafone does not remediate this issue, it may lead to the taking over of voicemail accounts.

A single prerequisite is required for the execution of this vulnerability, being that the computer which runs the exploit (sends the requests to the voicemail IMAP server) is on the service providers 3G/4G network internet. This can be achieved by tethering internet from the phone, to a computer.

Steps to reproduce the vulnerability (no longer working now):

1. Obtain a Vodafone prepaid SIM card and activate the SIM.
2. After activation, purchase a $5 Internet Essentials Pack and a $10 General Prepaid Recharge.
3. Once completed, call 121 to set up regular voicemail.
4. Once regular voicemail is setup (a PIN is set for your voicemail), you must dial '1217' to activate visual voicemail.
Note: Step 4, may take 30 minutes to 1 hour for the phone to actually be activated for visual voicemail.
5. Tether the internet connection present through the Vodafone SIM to your computer.
6. Run the proof of concept script attached via Python 3 to see the attack in progress.
7. A file called oput.txt is made containing the PIN of the targeted mobile number. In this case, the script targets only a single number which I own, where the pin should be 1337.

Note: the python script will no longer work as the vulnerability is now patched in Australia.

I plan to do a presentation on international voicemail security later this year at a security conference called Ruxcon, and would really appreciate it if you could assist in helping get this issue fixed on other service providers.

Additionally, I would also be very appreciative if the information about the exploitation of visual voicemail servers and PoC scripts is not shared until we can come up and agree with a way of best fixing this issue around the world.

Thanks,
Shubham

Shubham Shah <>

International Visual Voicemail Security

43 messages

Shubham Shah <> Sun, Jul 6, 2014 at 10:39 PM
To: jmoran@gsma.com
Cc: Ben Grubb <bgrubb@fairfaxmedia.com.au>,

Hi James,

In the last few months, I have been on an investigative path to breaking voicemail

security. Whilst complying, co-operating and assisting mobile service providers to get any issues fixed, I was recommended to inform you to see if we could work together to help get this issue patched globally.

In May 2014, I started taking a look through the visual voicemail protocol and how many major providers handle the implementation of visual voicemail. This specification, itself, is found on the GSMA website: http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpvvmspecification12.pdf.

Whilst there are multiple ways to implement authentication on visual voicemail services, it seems that there is a pattern of insecurity when using a particular method of authentication.

Most providers which seem to implement visual voicemail authentication through a pin based password method are most likely vulnerable to bruteforce attacks.

I was able to find, that at least in Australia for Vodafone, they were vulnerable to such bruteforce attacks, effectively proving it extremely easy to obtain any numbers voicemail pin.

I can confirm that Vodafone has now rolled out patches for this issue in at least Australia and I hope globally also if other countries were affected.

Below is a short technical write up relating to the vulnerability, which is made possible thanks to visual voicemail and Vodafone's implementation of it and lack of bruteforce protection.

Pre-requisites:
- Python 3 (Obtainable from here: https://www.python.org/download/releases/)
- Python futures library: install via pip3 install futures
- PoC Script (Attached)

Description of vulnerability:

Vodafone's visual voicemail system is susceptible to bruteforce attacks as it does not enforce any rate limiting or password policy rules. Due to this, all Vodafone customers are currently vulnerable to their voicemails being broken into. If Vodafone does not remediate this issue, it may lead to the taking over of voicemail accounts.

A single prerequisite is required for the execution of this vulnerability, being that the computer which runs the exploit (sends the requests to the voicemail IMAP server) is on the service providers 3G/4G network internet. This can be achieved by tethering internet from the phone, to a computer.

Steps to reproduce the vulnerability (no longer working now):

1. Obtain a Vodafone prepaid SIM card and activate the SIM.
2. After activation, purchase a $5 Internet Essentials Pack and a $10 General Prepaid Recharge.

3. Once completed, call 121 to set up regular voicemail.
4. Once regular voicemail is setup (a PIN is set for your voicemail), you must dial '1217' to activate visual voicemail.
Note: Step 4, may take 30 minutes to 1 hour for the phone to actually be activated for visual voicemail.
5. Tether the internet connection present through the Vodafone SIM to your computer.
6. Run the proof of concept script attached via Python 3 to see the attack in progress.
7. A file called oput.txt is made containing the PIN of the targeted mobile number. In this case, the script targets only a single number which I own, where the pin should be 1337.

Note: the python script will no longer work as the vulnerability is now patched in Australia.

I plan to do a presentation on international voicemail security later this year at a security conference called Ruxcon, and would really appreciate it if you could assist in helping get this issue fixed on other service providers.

Additionally, I would also be very appreciative if the information about the exploitation of visual voicemail servers and PoC scripts is not shared until we can come up and agree with a way of best fixing this issue around the world.

Thanks,
Shubham

06 July 2014 13:40
To: James Moran
Cc: Ben Grubb;
Subject: International Visual Voicemail Security
[Quoted text hidden]

GSMA SWAP-001-13 Template.doc
132K

James Moran <jmoran@gsma.com> Mon, Jul 21, 2014 at 11:27 PM

To: Shubham Shah <>

Hi Shubham,

I look forward to hearing from you when you get a chance to reply to my earlier email as we have received an inquiry from Ben Grubb at the Sydney Morning Herald in which he informed us of his plans to publicise your research well in advance of your presentation later this year. My understanding is that he will most likely publish an article in the coming days and he has asked us if operators other than Vodafone Australia are vulnerable. Regrettably, we are never likely to be in a position to answer that question as security deployments on individual networks are a matter for the operators of those networks and they do not share details pertaining to their configurations with GSMA. That said, we are anxious to alert our members to the possible vulnerability and to encourage them to check their configurations.

In order to progress I would be grateful if you could provide more details that we can share our members and clarification on how you wish us to proceed.

Many thanks,

James.

P.S. Will you be at the upcoming Black Hat event in Las Vegas?

From: James Moran
Sent: 15 July 2014 09:04
To: 'Shubham Shah'
Subject: RE: International Visual Voicemail Security

Hi Shubham,

Thank you very much for approaching us at the GSMA about this matter and apologies for the delay in getting back to you as I have been out of the office.

I have been in contact with Vodafone regarding this matter and await their response.

It appears from the information you have provided that the vulnerability specifically affects the OMTP defined visual voicemail interface protocol rather than anything defined by GSMA. Is that correct?

I note in your email your intention to make public the vulnerability in October and that gives us ample time to bring this matter to the attention of our members. However, I also note that you do not want us to provide certain information pertaining to the exploit to our members despite the fact that you have copied your correspondence to the media. The request to withhold information already provided to the media, months ahead of your planned announcement, seems to be inconsistent and I really need your clear guidance on how we can proceed.

In that regard, I have attached a simple report template that we can use to bring this issue to the attention of our members and I invite you to complete it as best you can with the information you deem appropriate. Once I receive it back I will do any minor editing that may be required and will promptly issue it to our members.

Best regards and thanks again for bringing this matter to our attention.

Best regards,

James.

From: Shubham Shah [mailto:]
Sent: 06 July 2014 13:40
To: James Moran
Cc: Ben Grubb;
Subject: International Visual Voicemail Security

Hi James,

[Quoted text hidden]
[Quoted text hidden]

Shubham Shah <> Tue, Jul 22, 2014 at 12:50 AM
To: James Moran <jmoran@gsma.com>

Hey James,

Thanks so much for replying. You're correct in saying that Ben Grubb will be disclosing that Vodafone's misconfiguration left its customers open for a long period of time. However, he will not be mentioning any part of the methodology of techniques used to gain access to Vodafone customers visual voicemail accounts.

In my understanding, the article will be more of a notification to the general public that such a vulnerability was present, for a period of time and not much more.

It's so unfortunate that we are unable to determine which telco's are vulnerable globally, however as far as I know, most telco's seem to be lacking in security for visual voicemail - unless they are using the STATUS sms method which sets a relatively random password as their visual voicemail configuration password. Even then, there are flaws in that process but none big enough to gain access arbitrarily to others voicemail accounts.

I am interested in disclosing this issue to your members, but am requesting some more time to finalise whatever current research I have and to test configurations from other countries. I do not wish to raise unwarranted panic if this is an isolated case (even though it is unlikely). At the moment, I am finding great difficulty to test services in America and New Zealand due to a total lack of access to equipment and sim cards from that region.

I shall attempt to answer your questions now:

It appears from the information you have provided that the vulnerability specifically affects the OMTP defined visual voicemail interface protocol rather than anything defined by GSMA. Is that correct?

Not quite, what is quite peculiar is that OMTP explain a way of setting a lengthy and randomised password for visual voicemail via the STATUS message. However, with the way that Apple has implemented it, operators can also allow for a the visual voicemail password to be a pin. This pin is usually set to be less than 8 numbers long and hence, enumerable. Due to this fact and also the fact that there is usually a total lack of rate limiting and bruteforce protection on IMAP based authentication services - the ability to extract visual voicemail pins, is quite possible.

As for Blackhat, it is something I am definitely interested in - however I have not booked any accommodation nor have tickets to the conference since I was originally not planning to go this year. This may change in the next two weeks or so and if it does, I'll let you know.

I am currently in dire need of being able to test my methods and techniques, with my partner in another country. This is mainly to validate my ideas since Apple's visual voicemail implementation is very undocumented. A lot of guesswork has been done and whilst Vodafone was at one stage defeated via my exploitation techniques, I need to discover if this is true in other telco's. If you could somehow arrange a way where my partner and I can perform research on a visual voicemail account somewhere else in the world - we would be very grateful.

Thanks,
Shubham

P.S. I shall be filling out the security reporting form sometime in the coming month, or as soon as I have done sufficient research to document the

vulnerability.
[Quoted text hidden]

James Moran <jmoran@gsma.com> Tue, Jul 22, 2014 at 9:28 AM
To: Shubham Shah <>

Hi Shubham,

Many thanks for your prompt reply and for your constructive and responsible engagement with us on this matter.

I note your request for more time to complete your research and that is perfectly reasonable and understandable. I also note the difficulties you have experienced with your testing and although this is not something GSMA can directly assist as we do not control or have access to any test SIMs issued by our member networks we could ask our members to support your efforts by initially highlighting the issue to them, asking them to check their local configurations and report findings back, possibly to us and then to you.

To make that ask we will need to issue the report alerting them to the problem and providing to them precise details of the tests they need to perform and the results they need to return to us. Does that approach sound like something you want to do?

I note you do not currently plan to attend Blackhat and that is not a problem. I asked merely because I will be there and if you were too we could catch up but we can continue our dialogue in this manner.

Best regards,

James.

From: Shubham Shah [mailto:]
Sent: 21 July 2014 15:50
To: James Moran
Subject: Re: International Visual Voicemail Security

[Quoted text hidden]
[Quoted text hidden]

Shubham Shah <> Mon, Aug 4, 2014 at 6:28 PM
To: James Moran <jmoran@gsma.com>
Cc: Ben Grubb <bgrubb@fairfaxmedia.com.au>
Bcc: Huey Peard <>

Hey James,

Thanks so much for the reply. Please excuse my delay in responding, as I have been busy documenting the flaw and have been trying to work out a way to have a standard test for this vulnerability.

Unfortunately, there is no single way of testing the flaw. As of yet, I have constructed each of my exploits on a vendor basis, due to the differences in how everyone seems to perform visual voicemail authentication. Here are the variables that come into play:

- Whether or not they use Digest-MD5 or Plain AUTH
- Whether or not their IMAP server is accessible only when on their 3G/4G network or externally accessible
- How they do the visual voicemail authentication (either via STATUS messages or Plain Text Auth)
- The location of their IMAP server and it's corresponding port

The **best** test for this vulnerability, is merely the question: "**Does our visual voicemail IMAP server have sufficient rate limiting and lockout procedures to prevent bruteforce attacks**". If the answer is no, then simply the question "**Do we use the PIN as the visual voicemail password, or do we issue a random password via the STATUS SMS Message?**".

If the answer is no and no, the vendor is very, very likely to be vulnerable.

I have filled out the form and have attached it to this email. It has some more detail of how to reproduce it, but I think my initial email to you with the PoC attachments will help assist you in the testing phase.

Please do not hesitate to contact me, I'm always available to assist and answer questions.

Thanks,
Shubham
[Quoted text hidden]

GSMA SWAP-001-13 Template.doc
140K

Shubham Shah <> Tue, Aug 5, 2014 at 8:45 PM
To: James Moran <jmoran@gsma.com>

Hey James,

Out of curiosity, will you be able to disclose which organisations could potentially have been vulnerable to the attack I documented above, once they have identified and patched the issue?

If so, it will assist me greatly.

Thanks,
Shubham
[Quoted text hidden]

James Moran <jmoran@gsma.com> Thu, Aug 7, 2014 at 3:03 PM
To: Shubham Shah <>

Hi Shubham,

Thank you very much for submitting the competed alert, which I am about to issue but I have just one question and it relates to the fact that the "Manufacturer Comments/Action" section is blank. Have you raised this issue with Apple and have they provided any response that is worthy of inclusion in the alert?

In response to your question, yes, I will be happy to share with you details of any operators that provide feedback to me.

Many thanks,

James.

From: Shubham Shah [mailto:]
Sent: 05 August 2014 11:45

[Quoted text hidden]
[Quoted text hidden]
[Quoted text hidden]

Shubham Shah <> Thu, Aug 7, 2014 at 4:47 PM
To: James Moran <jmoran@gsma.com>

Hey James,

It's indefinite whether or not Apple have put out standards on how to implement visual voicemail. The reason why I have placed apple in there, is because I had suspected that Apple has some sort of guideline for telco's on how to implement visual voicemail so it works with their native Apple visual voicemail application itself.

I have notified Apple about the issue, however I do not think it is entirely their fault. They have not taken responsibility or given me any more details, but have however said that they appreciated a heads up on the research I was doing.

It's very difficult to figure out, externally with hardly any resources, how the visual voicemail system works and if there is a set default. From external testing, I've recognised that Apple has a wide range of support for visual voicemail implementations: whether they be visual voicemail implementations using DIGEST-MD5 auth or Plain Text auth and whether they are using the STATUS method, or are connecting with the password as the actual voicemail pin number.

In short: the vulnerable implementation of visual voicemail does not originate from Apple but instead from telco to telco. I however had notified all parties whom I think are involved in making visual voicemail available.

Thanks,

Shubham
[Quoted text hidden]

James Moran <jmoran@gsma.com> Thu, Aug 7, 2014 at 5:12 PM
To: Shubham Shah <>

Hi Shubham,

Many thanks for this additional clarification. I will remove Apple's name from the alert and ensure operators understand the issue is likely to be with their implementations.

Best regards,

James.

From: Shubham Shah [mailto:]
Sent: 07 August 2014 07:47

[Quoted text hidden]
[Quoted text hidden]
[Quoted text hidden]

Shubham Shah <> Thu, Aug 7, 2014 at 5:12 PM
To: James Moran <jmoran@gsma.com>

Thanks James,

Please do keep me updated.

Thanks,
Shubham
[Quoted text hidden]

James Moran <jmoran@gsma.com> Fri, Aug 15, 2014 at 1:44 AM

To: "Shubham Shah ()" <>

Hi Shubham,

I hope this email finds you well.

I have been in contact with Vodafone regarding the proposed SWAP (see attached) and they are very happy with it to be released. The only request they have is that the Vodafone Australia login details are removed from the script to avoid Vodafone encountering lots of false positive brute forcing attempts from GSMA members that run the script without modification!

Could you possibly amend the script to use example login details instead like 12345678@vm.example.com? If so, you can either embed an updated script in the SWAP or simply send the file to me and I will embed it.

Many thanks,

James.

From: James Moran
Sent: 07 August 2014 08:10
To: 'Shubham Shah'
Subject: RE: International Visual Voicemail Security

Hi Shubham,

Many thanks for this additional clarification. I will remove Apple's name from the alert and ensure operators understand the issue is likely to be with their implementations.

Best regards,

James.

From: Shubham Shah [mailto:]
Sent: 07 August 2014 07:47

[Quoted text hidden]
[Quoted text hidden]
[Quoted text hidden]

GSMA SWAP-002-14 Visual Voicemail Security.doc
149K

Shubham Shah <> Fri, Aug 15, 2014 at 1:14 PM
To: James Moran <jmoran@gsma.com>

Hey James,

No worries.

That's great news! I'll be presenting the visual voicemail attack later this year at Ruxcon in Melbourne.

In there I will also redact or obfuscate Vodafone's IMAP server details.

As for the script, I have attached the redacted version below.

Thanks so much,
Shubham

[Quoted text hidden]

example.py
2K

James Moran <jmoran@gsma.com> Sat, Aug 16, 2014 at 9:35 PM
To: Shubham Shah <>

Many thanks Shubham.

This has now been issued to our Security Group and I have invited member feedback on whether they find and fix the vulnerability within their own deployments. I will let you know what I get back.

Best regards,

James.

From: Shubham Shah [mailto:]
Sent: 15 August 2014 04:15
To: James Moran
Subject: Re: FW: International Visual Voicemail Security

[Quoted text hidden]
[Quoted text hidden]

Shubham Shah <> Mon, Sep 8, 2014 at 10:57 PM
To: James Moran <jmoran@gsma.com>
Cc: Ben Grubb <bgrubb@fairfaxmedia.com.au>

Hey James,

I was just wondering whether or not there have been any reports of successful exploitation using this technique?

Additionally, I thought I would update you with more details of my presentation later next month:

https://ruxcon.org.au/speakers/#Shubham Shah

Thanks,
Shubham
[Quoted text hidden]

James Moran <jmoran@gsma.com> Wed, Sep 10, 2014 at 8:42 AM
To: Shubham Shah <>
Cc: Ben Grubb <bgrubb@fairfaxmedia.com.au>

Hi Shubham,

Your email is timely indeed as earlier today I emailed our Security Group members to ascertain if any of them had identified the reported problem. I had not heard anything since I circulated the notification hence the reason for my follow up and I will let you know as soon as I receive anything.

Best regards,

James.

From: Shubham Shah [mailto:]
Sent: 08 September 2014 13:58
To: James Moran
Cc: Ben Grubb

[Quoted text hidden]
[Quoted text hidden]
[Quoted text hidden]