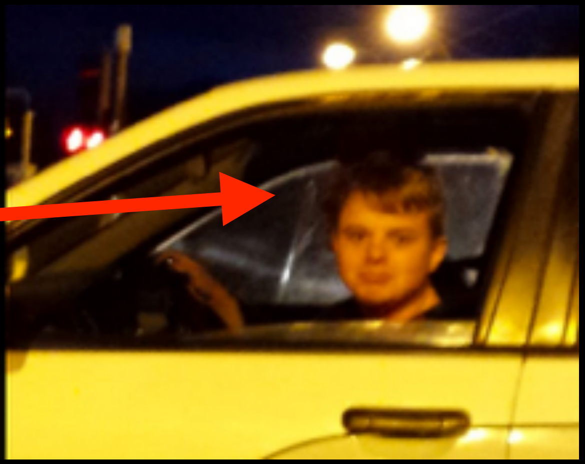
Breaking International Voicemail Security and Bypassing 2FA for fun and profit

Shubham Shah (@infosec_au) and Huey Peard (@hueypeard)

Who are we?

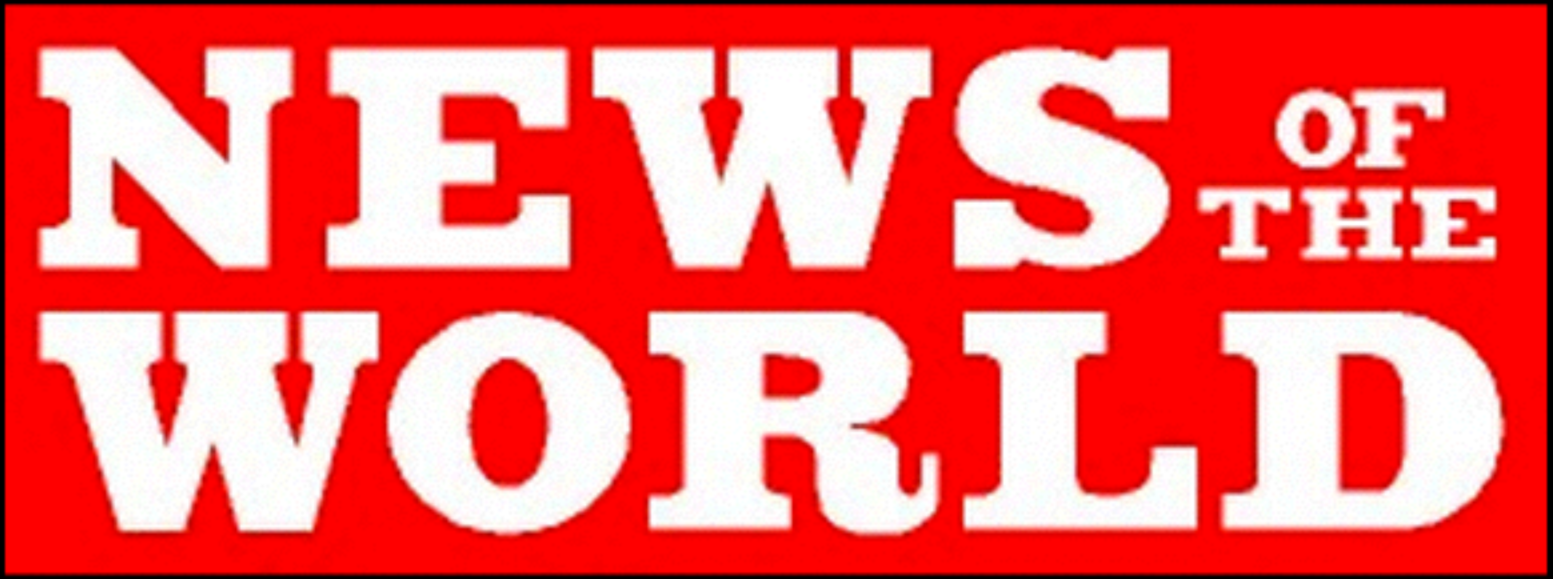
- **Shubham Shah**
  - Breaks things.
  - Security researcher, CTF’er, application developer
  - Dominating web applications since 09’
  - Makes the best butter chicken
- **Huey Peard**



  - Member of Gibson Security
  - Currently doing his HSC - Couldn’t come, English exam : (
  - Spends his time writing web apps and hacking on the JVM
  - Founding member of The Cool Crew

Remember that voicemail hacking scandal?

“Which one?”



That one.

Murdoch's “News International”, announced the closure of the newspaper following the “hacking” scandal.

Methods which were used in the News of the World Scandal (2005-2011)

Caller ID Spoofing

Pin guessing w/o lockouts

Basic Social Engineering/Default Pins

Methods which still work today

All of them

(and more!)

Caller ID Spoofing

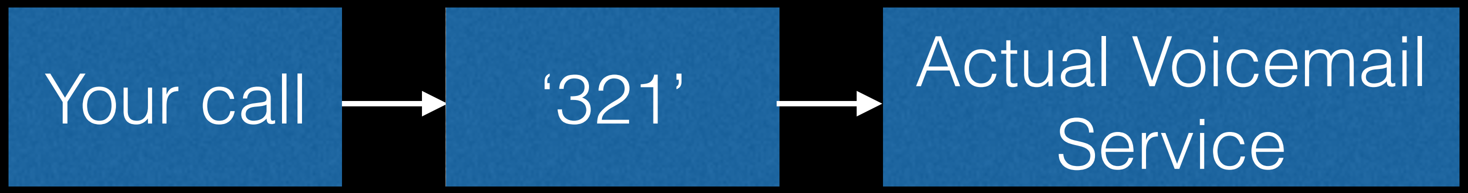
Getting access to 9.59+ million voicemail accounts (Optus)

- **What is a direct dial number (DDN)?**
  - The *actual* voicemail number, and not the proxy to the number
  - A specific, full 10 digit number which resolves to the voicemail service
  - Also known as a unique voicemail number, there can be more than one

- **Aim is to obtain the DDN, as usually they are vulnerable:**
  - e.g. call service provider and ask “How do I check my voicemail overseas?”
  - Google: “[telconame] voicemail number”, scour ISP related forums e.g. whirlpool.net.au for Australia

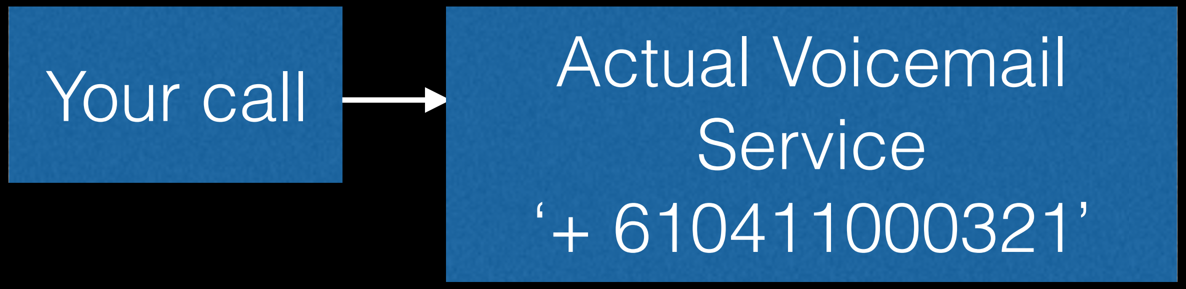
Examples of DDN’s (direct dial numbers)

- The default voicemail number provided to Optus customers was ‘321’ - accessible only when on Optus network in Aus.
- This is a network specific number and is most likely, a proxy to the actual voicemail service number.
- Here’s how it looks like, visually:



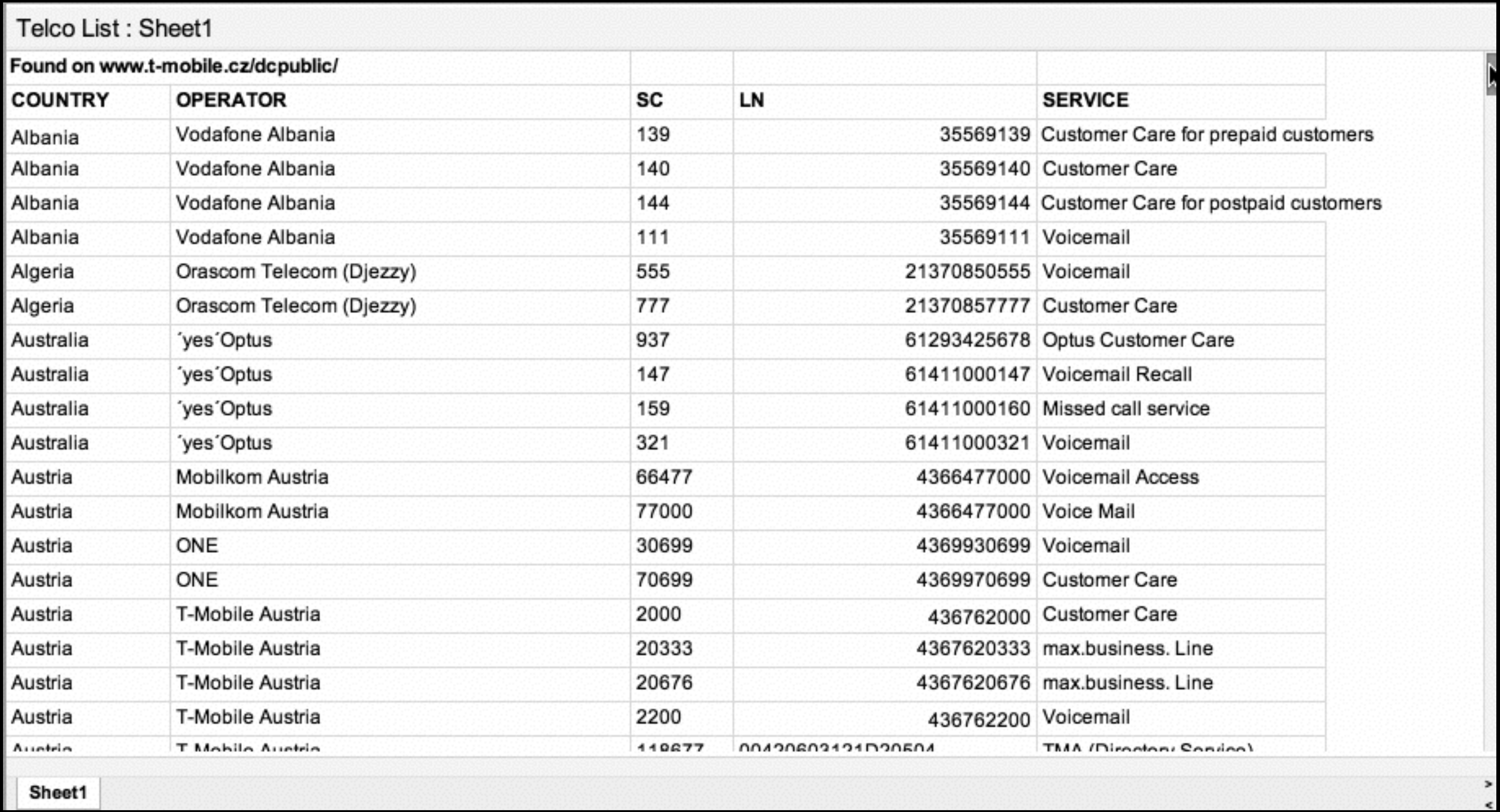
Your call → ‘321’ → Actual Voicemail Service

- However, when using direct dial numbers, the number is 10 digits, accessible anywhere and does not consist of a proxy like system.



Your call → Actual Voicemail Service ‘+ 610411000321’

List of DDNs



Telco List : Sheet1

Found on www.t-mobile.cz/dcpublic/				
COUNTRY	OPERATOR	SC	LN	SERVICE
Albania	Vodafone Albania	139	35569139	Customer Care for prepaid customers
Albania	Vodafone Albania	140	35569140	Customer Care
Albania	Vodafone Albania	144	35569144	Customer Care for postpaid customers
Albania	Vodafone Albania	111	35569111	Voicemail
Algeria	Orascom Telecom (Djezzy)	555	21370850555	Voicemail
Algeria	Orascom Telecom (Djezzy)	777	21370857777	Customer Care
Australia	´yes´Optus	937	61293425678	Optus Customer Care
Australia	´yes´Optus	147	61411000147	Voicemail Recall
Australia	´yes´Optus	159	61411000160	Missed call service
Australia	´yes´Optus	321	61411000321	Voicemail
Austria	Mobilkom Austria	66477	4366477000	Voicemail Access
Austria	Mobilkom Austria	77000	4366477000	Voice Mail
Austria	ONE	30699	4369930699	Voicemail
Austria	ONE	70699	4369970699	Customer Care
Austria	T-Mobile Austria	2000	436762000	Customer Care
Austria	T-Mobile Austria	20333	4367620333	max.business. Line
Austria	T-Mobile Austria	20676	4367620676	max.business. Line
Austria	T-Mobile Austria	2200	436762200	Voicemail
Austria	T-Mobile Austria	118677	00420603121D20504	TMA (Directory Service)

Sheet1

- These DDNs are available @: http://bit.ly/1tvZtWS

Breaking Optus's voicemail

the facts

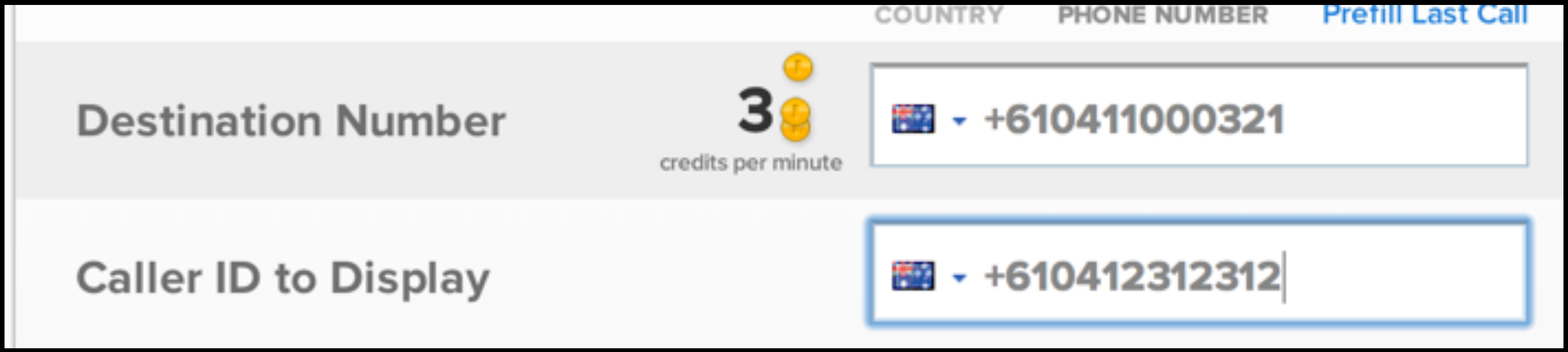
- Optus acknowledged that they: "are looking at multiple options to address this emerging industry-wide threat (spoofing), including technical solutions and customer education."- 22 Jul, 2011, http://www.ausbt.com.au/is-your-voicemail-hackable-optus-telstra-and-vodafone-respond
- Hundreds of threads on Whirlpool (Australian ISP discussion forum) on numbers to call voicemail directly - very valuable information.
- DDN numbers are needed if you want to access voicemail when overseas and hence are disclosed freely.

Spoofing Numbers

- Spoof to ‘+61321’? ✗ Unless we can spoof whilst ON the Optus network, this is not possible.

- Spoof to ‘+610411000321’ DDN? ✓ We can spoof from any PBX system. Even easier, due to spoofcard.com. Spoof victim number to the DDN.

↓



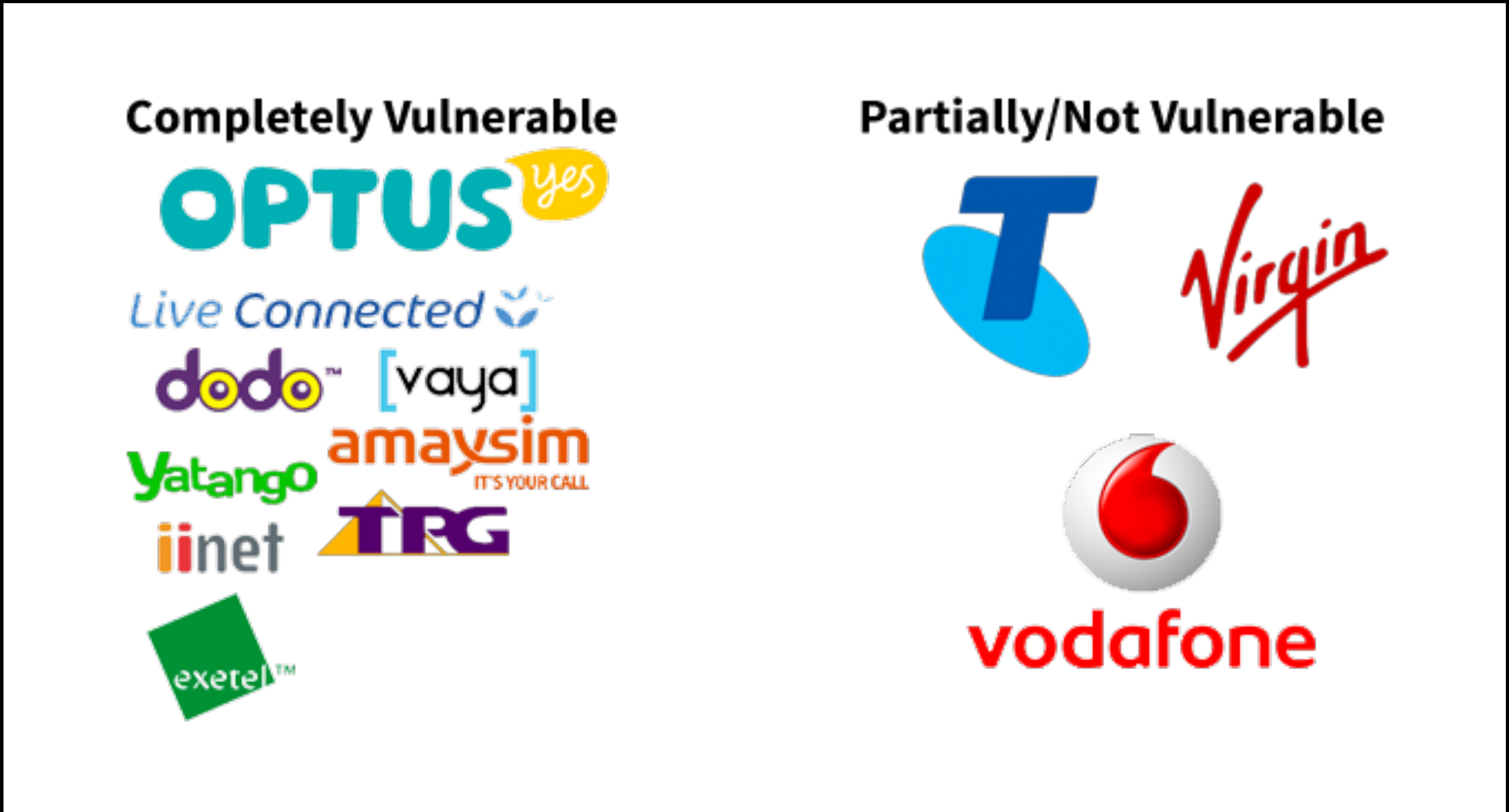
COUNTRY PHONE NUMBER Prefill Last Call

Destination Number 3 credits per minute +610411000321

Caller ID to Display +610412312312

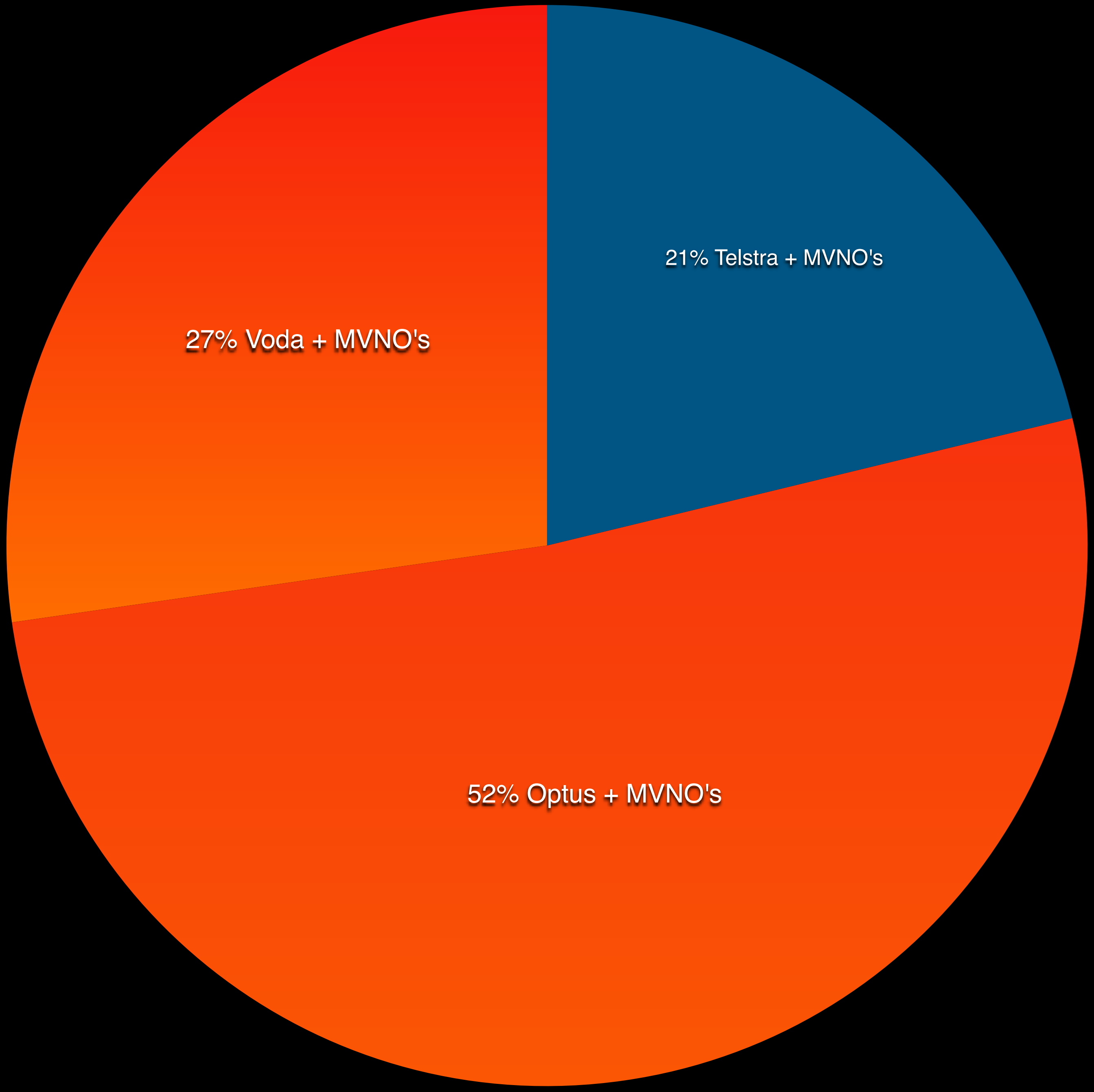
Congratulations

- You now have access to all mobile voicemail accounts from 9.59 million Australian Optus accounts.



Providers Vulnerable

Percentage of providers and Mobile Virtual Network Operators vulnerable,
grouped by provider (red means vuln ;))



Why did this work?

- It’s likely that Optus had protections set up for the number “+61 321” but did not have any protection set up when calling “+61 0411000321”.

- Optus’s authentication system assumed that your mobile number was a valid form of ID and used it to decide whether or not you need to enter a pin to access your account.

- The CID should never be used as a form of authentication as it has been designed so that it could be spoofed.

Why did this work?

- Issue got overlooked? Someone forgot to update multiple other ‘endpoints’ i.e. DDN’s to disallow CID authentication?

- Regardless, for a long period of time (>6 months), the entire Optus customer base whom had voicemail accounts, were wide open.

- This is a silly mistake, with potentially critical after effects. It is not known whether or not the attack was used in the wild for Optus customers.

Facts

- Optus took approximately a week or so until it was patched on a single DDN.

- Before the news article about the flaw was released, I was able to bypass Optus's patch on the first DDN by discovering a second DDN within an hour- also vulnerable.

- I disclosed this ASAP, and Optus fixed in approx. 1 day.

- News article released, all DDN's I could find/fuzz were patched. Very possible that there are more DDN's out there which are still vulnerable.

Facts

- Based off the list of DDN’s mentioned earlier - I am very very sure that this vulnerability is around in many countries, still not fixed.

- I’ve had emails from multiple people, stating that their country was vulnerable to the very same attack (surprise, surprise) - however, taking action on this has been a challenge.

- Either, we have two options.

  - 1) Seriously, do not rely on voicemail at all to be secure.

  - 2) Attempt to fix as many carriers voicemail security around the world.

What’s was new in this finding?

- nothing lol. It’s the same hack from 09’.

Is that all? The only way to breach voicemail?

- No.

- Being able to get into Optus's voicemail using age-old tricks was a good find, however nothing new.

- What is new? Voicemail wise? What technologies have emerged in the last few years, relating to voicemail?

- Most importantly, a recent development called Visual Voicemail, and the frameworks and implementations related to it.

Visual Voicemail 101

- Visual Voicemail was first introduced and publicised with the release of the first iPhone from Apple in **2007**.

- Visual voicemail allows for the access of voicemail through an interface, where messages can be replayed and general voicemail actions can be accessed via a GUI.

Steve Jobs showing off Visual Voicemail
@ WWDC 2010 Keynote

Visual Voicemail 101

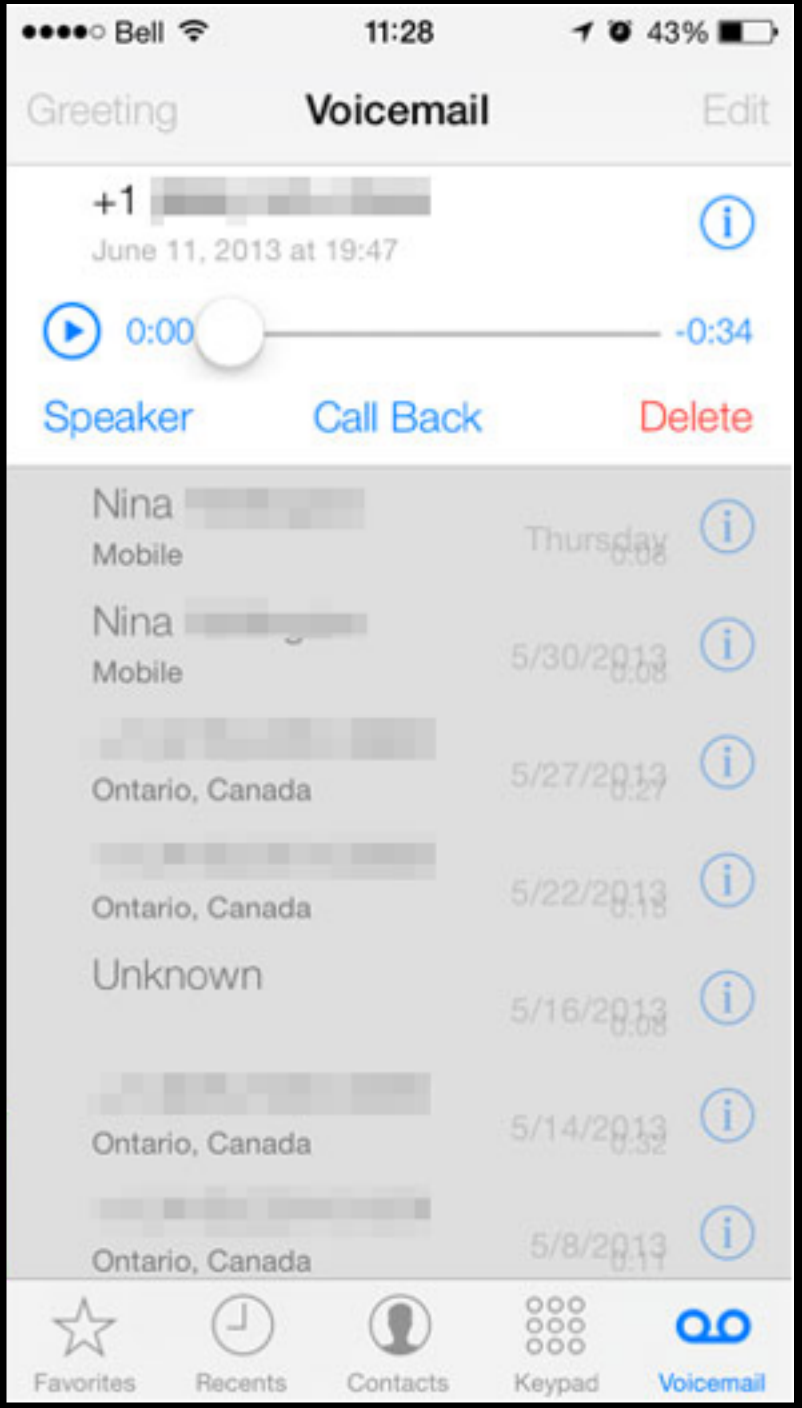
- IMAP4 server as the back bone (authentication and data storage)

- For most service providers, your voicemail pin, is your Visual Voicemail password.

- Some service providers set a generated password, via STATUS SMS 0 Type Messages

- To connect to a visual voicemail IMAP server, **you** **MUST** **be on the corresponding service providers internet (3g/4g/_) on the mobile network.** (we have not found providers so far that are accessible from the internet)

- Very detailed specification made by the OMTP: http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtpvvmspecification12.pdf



+1 [redacted]
June 11, 2013 at 19:47

Nina [redacted]
Mobile
Thursday

Nina [redacted]
Mobile
5/30/2013

[redacted]
Ontario, Canada
5/27/2013

[redacted]
Ontario, Canada
5/22/2013

Unknown
5/16/2013

[redacted]
Ontario, Canada
5/14/2013

[redacted]
Ontario, Canada
5/8/2013

iOS7 Visual Voicemail

Visual Voicemail 101

Observations

- Visual Voicemail servers which are running IMAP on port 943 (IMAP w/ SSL), tend to use the PLAIN authentication mechanism (which predictably uses plain-text).
- Visual Voicemail servers which are running IMAP on port 143 (Non-SSL IMAP), tend to use the DIGEST-MD5 mechanism (which is now obsolete as of RFC6331 due to a variety of issues with the standard and the cryptography used).
- DIGEST-MD5 is described in RFC2831

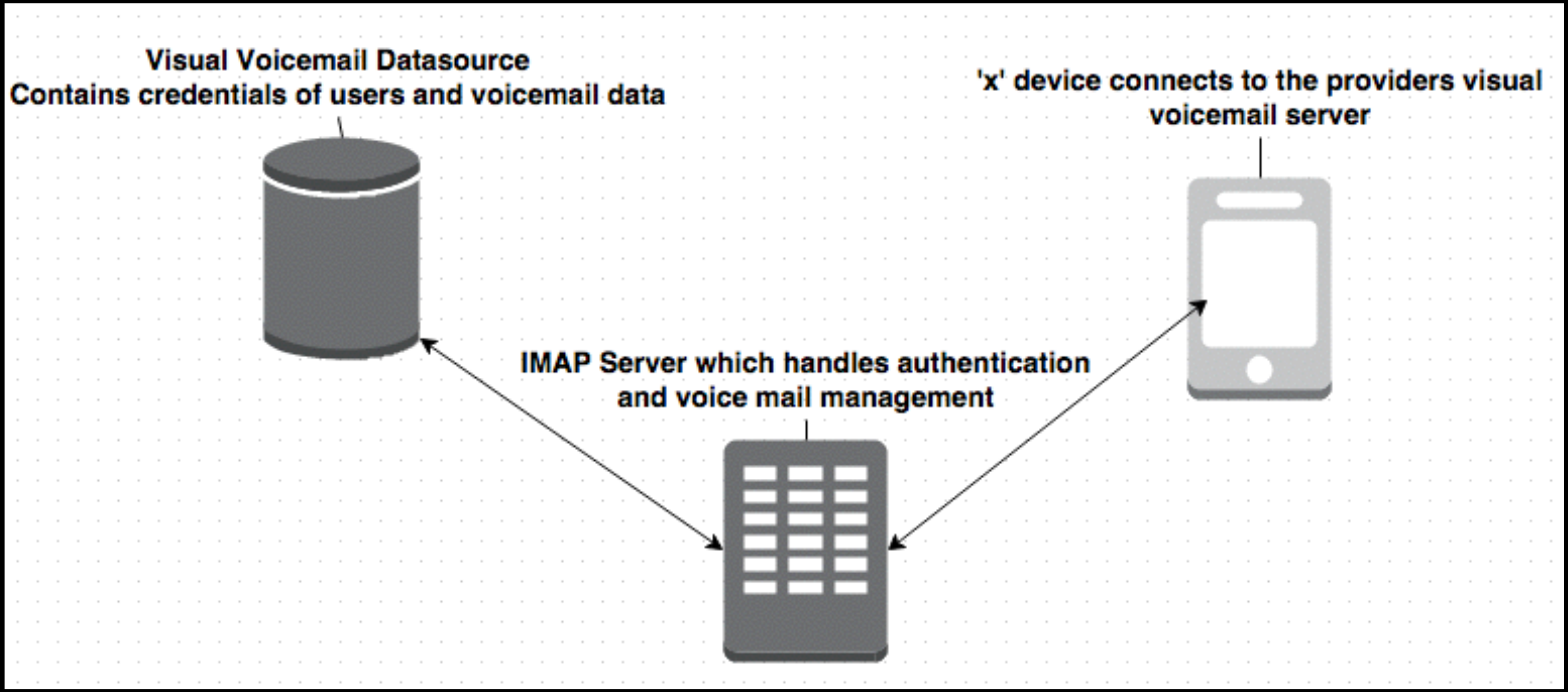
Visual Voicemail 101

Observations

- Most service providers require you to SMS a number or call a specific number to enable visual voicemail, but through tests we have found that authentication can be done without “activating” visual voicemail services.

- A majority of telco’s worldwide now offer visual voicemail as a default, or for free. Of course, with the exception of Telstra. lol. (you have to pay a monthly fee to use the service).

Visual Voicemail 101



Visual Voicemail Datasource
Contains credentials of users and voicemail data

'x' device connects to the providers visual voicemail server

IMAP Server which handles authentication and voice mail management

Flash SMS

- Class 0 or Flash SMS is a type of SMS that is typically used to show messages to the user that are not stored in their inbox.

- For example, due to their temporary nature, Flash SMS have been used to send users one time passwords, as well as alert them of the latest information in an emergency

- Most phones only show the latest Flash SMS, and removing it once read.

STATUS Messages
Authenticating to Visual Voicemail

- One definitive and documented way of authenticating to visual voicemail, is through the use of Visual Voicemail STATUS messages.

- These messages contain a single string which contains all the credentials required for a users visual voicemail account to be registered on the phone.

- For example, on T-Mobile, the STATUS message looks something like this:

- **VVM:STATUS:st=R;rc=0;srv=vvm.tmomail.net;ipt=143;u=0000000000@vms.eng.t-mobile.com;pw=BOQ8CAzzNcu;lang=1l2l3l4;g_len=180;vs_len=10;pw_len=4-9**

STATUS Messages: continued

- These VVM messages are sent as, you guessed it, Flash 0 SMS messages. The difference in this case, is that the message is hidden from the user altogether and only viewable by phone internals.

- Some older phones that do not implement the spec can be used to view these messages.

- Spoofing of Flash 0 SMS messages with bogus STATUS SMS messages could even lead to the de-anonymisation of any individual with an iPhone iOS 6 and above.

Connection Credentials

- The first step to pentesting your a visual voicemail service, is obtaining the connection details from your phone to the visual voicemail server.

- These details can be obtained via network packet dumps or via iPhone plist/db analysis.

Dumping pcap via tcpdump (OSX only)

Note: Xcode is required, the iPhone UDID should be in lowercase and obtainable via XCode

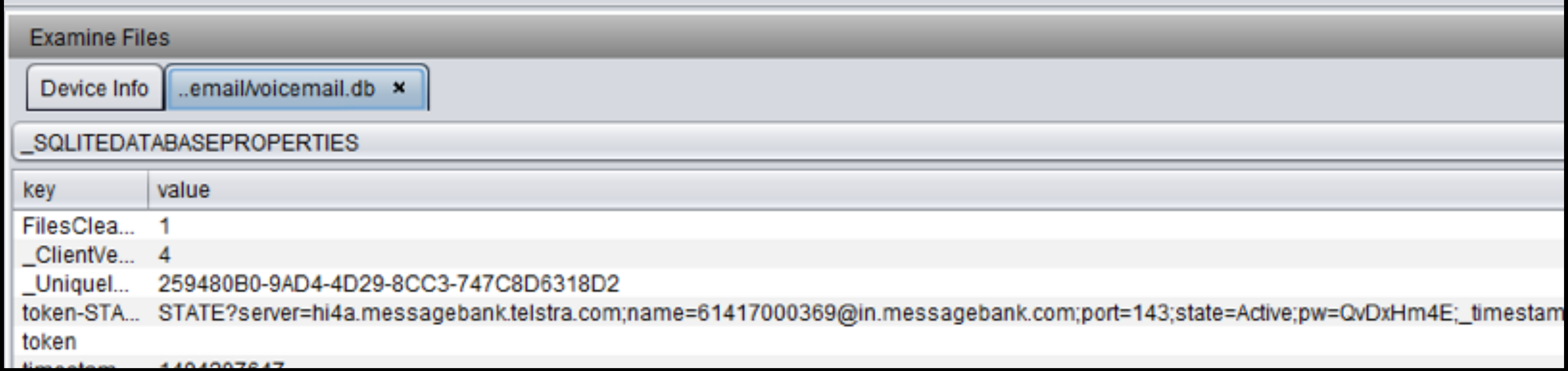
rvictl -s <iPhone UDID>;sudo launchctl list com.apple.rpmuxd;sudo tcpdump -n -t -i rvi0 -w dump.pcap

iPhone Backup Analysis (requires phone backup)

Download iPhone Analyser
http://goo.gl/9FGS1Z

Navigate to /Library/Voicemail and then select Voicemail.db. The SQLite field `token-STATE` will contain full plain text credentials to the VVM server.

Example of Telstra's visual voicemail connection string



key	value
FilesClea...	1
_ClientVe...	4
_Uniquel...	259480B0-9AD4-4D29-8CC3-747C8D6318D2
token-STA...	STATE?server=hi4a.messagebank.telstra.com;name=61417000369@in.messagebank.com;port=143;state=Active;pw=QvDxHm4E;_timestam
token	

- Server name, port, username and password. Basically, all you need to connect to the IMAP server yourself.

- Telstra uses a pre-generated password (which is seemingly random) sent via the STATUS message. However, there are no limits to brute forcing via the Telstra IMAP connection. (Tested mid to late August)

- Due to the security of the pre-generated password, brute forcing a Telstra VVM account password is sadly near-impossible.

VVM for Pentesters and Forensic Analysts

- VVM is quite a verbose voicemail system.
- After logging into the IMAP server with any given VVM credentials, you'll find that everything is well logged, documented and stamped. This can help for data collection, forensics and preciseness.
- Having any iPhone in an unlocked state, if a successful backup is made, you now have their visual voicemail account - and can access their voicemail.

VVM for Pentesters and Forensic Analysts

- Sometimes, in fact, most of the times, the VVM password is different to the pin code chosen by the user. In this case, when the user changes their pin code for voicemail, their VVM password remains the same.

- Problem!

- This means, that even a single breach of VVM password, could lead to long term access to ones voicemail account.

VVM for Pentesters and Forensic Analysts

- Forensics wise, voicemails may be something which need to be accessed. The process of extracting voicemails via the phone is not pleasant.

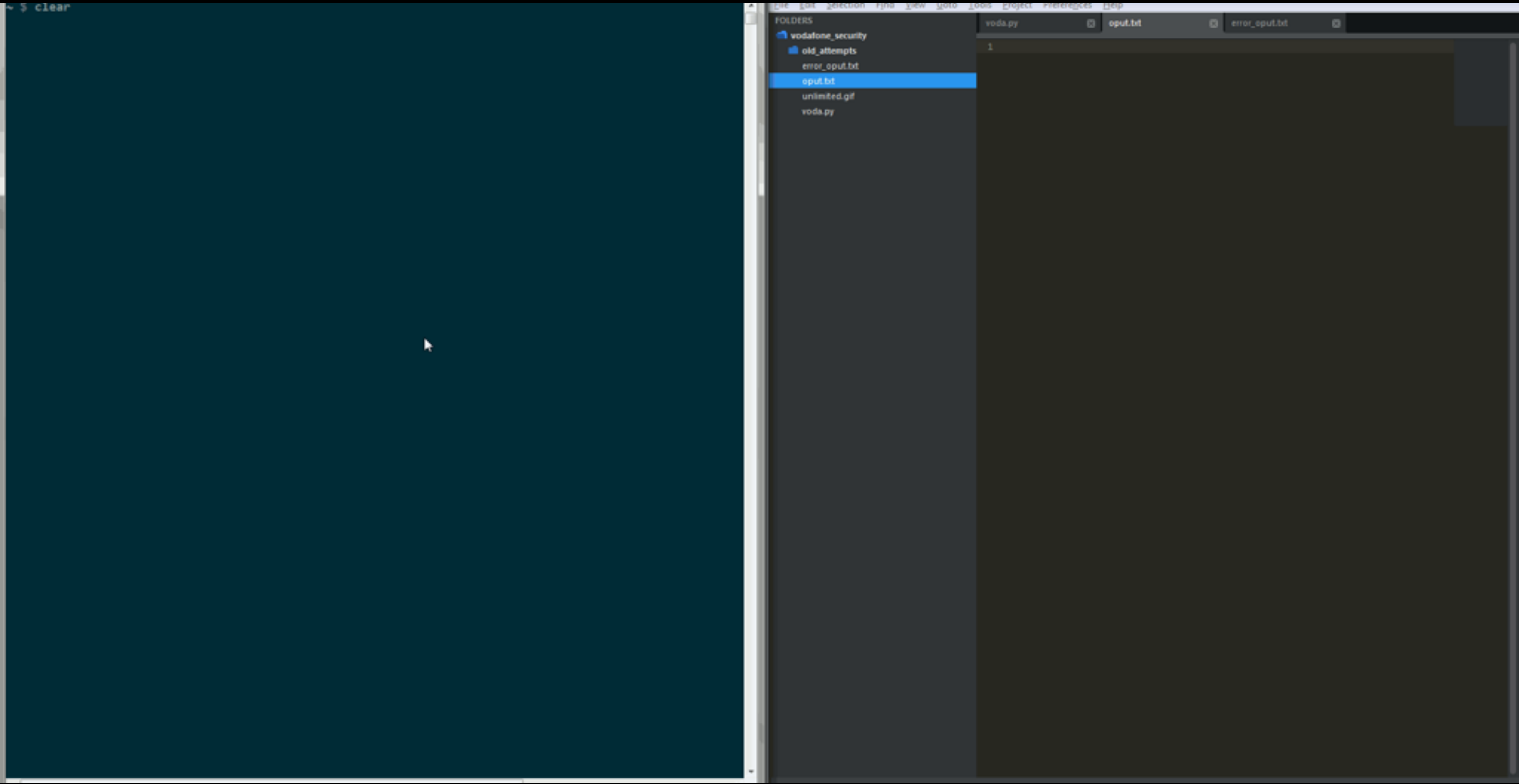
- If you have the VVM connection details, connecting to the VVM server and extracting raw audio files, is very useful.

- Timestamps and more can also be extracted from the mail headers.

Times when you can own visual voicemail

- It’s a simple criteria really.
- If your visual voicemail provider, uses pins instead of randomly generated pass phrases - you will most likely be able to completely pwn the visual voicemail service.
- If they have rate limiting, you’ll need to look at other options.
- If they lock out accounts, it may even be a DoS exploit. However, bruteforcing is the most applicable vulnerability class for VVM.

Demo



```
~ $ clear
```

File Edit Selection Find View Goto Tools Project Preferences Help
FOLDERS
vodafone_security
old_attempts
error_oput.txt
oput.txt
unlimited.gif
voda.py
voda.py
oput.txt
error_oput.txt
1

Larger Scope?

- Once you know the VVM server location, multiple attacks can be performed - without the strong focus on JUST breaking pins.

- Port scans, directory bruteforce, general recon tactics and more. If applications/services are found, owning these services could lead to higher access.

- Basically, if one has a high level of access on a VVM server - a very very big breach could occur.

Malware?

- is your iPhone backed up via iTunes?
- If so, imagine the attacker having persistent access to your voicemail account.

NOTE: as long as he/she can get internet connection relative to your mobile service provider

Why do voicemails even matter that much?

- 2 Factor Authentication Bypass via Voicemail Flaws
- Embarrassing voicemails from your mother
- ID Theft and could contain sensitive info (insider information)
- Account recovery via Voicemail

Facts about the 2FA Bypass

- Multiple online services provide soft-2FA (especially via Text or Phone Call):
  - i.e. Google, LinkedIn, Yahoo, Facebook.. etc.
- Usually, soft-2FA is a big issue for attackers (especially fraudsters).
- If the attacker has access to your voicemail, he/she will most likely be able to bypass such soft-2FA systems.

Practical Example

- For more than 6 months, the flaw mentioned earlier in the slides about CID spoofing - allowed access to the voicemail of Optus Customers.
- This means:
    - IF you were an Optus customer &&
        - IF you had soft-2FA on almost any online service

The attacker could have quite easily bypassed your protection.

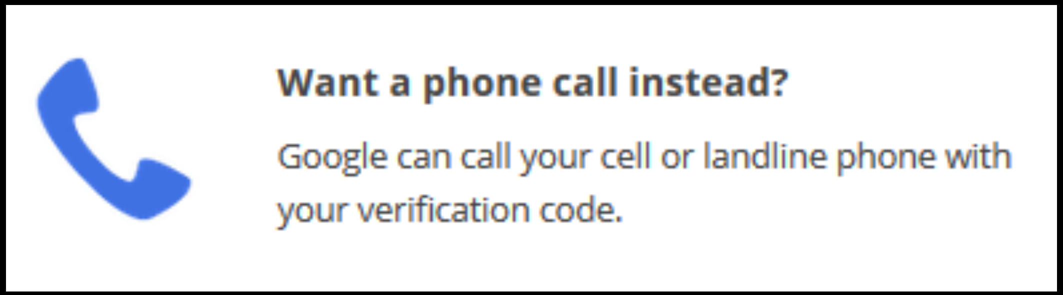
Executing the attack

- What do you need?
  - The victim's username/email & password.
  - The victims's attached mobile number to the 2FA service.
  - A mobile number spoofing service
  - The mobile networks voicemail number for remote access.

General Recon Techniques

Executing the attack

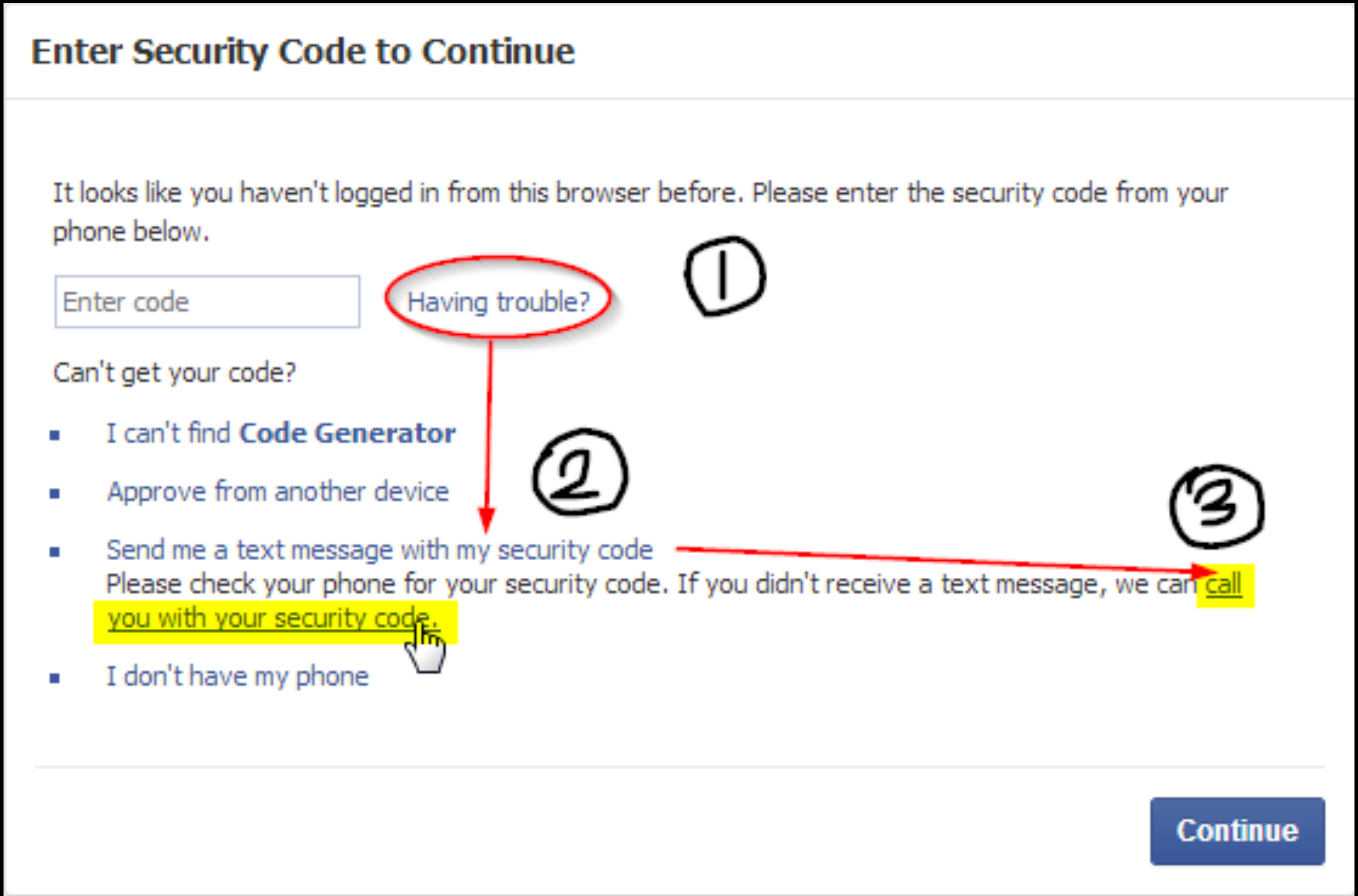
- Attacker initiates the login procedure, to the victims account.
- The victim receives a text-message or something similar, with a 2FA code.
- The attacker then engages the victim, by calling his/her mobile number.
- Whilst calling, the attacker chooses the option to receive the 2FA code **via Phone Call rather than a txt msg.**



Want a phone call instead?

Google can call your cell or landline phone with your verification code.

E.g. Facebook (Pre June-2014)



Enter Security Code to Continue

It looks like you haven't logged in from this browser before. Please enter the security code from your phone below.

Can't get your code?

- I can't find **Code Generator**
- Approve from another device
- Send me a text message with my security code
  Please check your phone for your security code. If you didn't receive a text message, we can call you with your security code.
- I don't have my phone

Executing the attack

- When the 2FA system tries to send the 2FA OTP/Token via a phone call - it gets redirected to voicemail.

- This is because the attacker has engaged the victims mobile number.

- As an attacker, this is a big win. The vectors to get that OTP/token have now increased greatly.

- Social engineering, mobile number porting and so on.

Executing the attack

- Attacker quickly breaches the victims voicemail account and gains access to the 2FA OTP/Token.
- Finally, then is able to fully authenticate into the victims account.
- Success!
- When discovering this attack (late May, 2014) - this attack worked on Google, LinkedIn, Facebook, Yahoo, Zoho and many more.

Important Notes

- Pentesters and attackers now have a very wide surface area to go after voicemails.

- If there is one thing that I have learnt out of all of this - the way voicemails are handled, regardless of provider, is that you should **NEVER** assume that your voicemails are ‘secure’ / only accessible by you.

- **Test your service provider.**

Responsible Disclosure

- GSMA: “The GSM Association is an association of mobile operators and related companies devoted to supporting the standardising, deployment and promotion of the GSM mobile telephone system. The GSM Association was formed in 1995.” (Wikipedia)
- via a middle man: Contacts in media can assist with responsible disclosure to the right people of an organisation.
- Persistent effort to contact relevant infosec teams @ telco’s.

Concluding

- All of this would not have been possible without the help from the Optus, Vodafone and Ben Grubb from SMH for co-ordinating all responsible disclosure in Australia.

- A big thanks to Nathan Wakelam, Chris Carter and Anshuman Bhartiya with their assistance in performing the research with VVM exploitation.

- Hope you enjoyed the pres :)

Welcome to SuperBank! Press any key on your phone to authenticate.