Compromising online accounts by cracking voicemail systems

Martin Vigo

@martin_vigo | martinvigo.com

Amstrad CPC 6128

Captured while playing "La Abadía del crímen"

Martin Vigo

Product Security Lead

From Galicia, Spain

Research | Scuba | Gin tonics

@martin_vigo - martinvigo.com

History

back to ezines

“You can just enter all 2-digit combinations until you get the right one”

…

“A more sophisticated and fast way to do this is to take advantage of the fact that such machines typically do not read two numbers at a time, and discard them, but just look for the correct sequence”

Hacking Telephone Answering Machines by Doctor Pizz and Cybersperm

“Quickly Enter the following string:
123456789876543213579246864297314741933669944885522775395
963725828384918171615110262030405060708090 01
(this is the shortest string for entering every possible 2-digit combo.)”

Hacking AT&T Answering Machines Quick and Dirty by oleBuzzard

“Defaults For ASPEN Are:
(E.G. Box is 888)
....
Use Normal Hacking Techniques:
---
i.e.
1111
|
\|/
9999
1234
4321”

A Tutorial of Aspen Voice Mailbox Systems, by Slycath

“There is also the old "change the message" secret to make it say something to the effect of this line accepts all toll charges so you can bill third party calls to that number”

Hacking Answering Machines 1990 by Predat0r

Voicemail security in the ‘80s

- Default PINs
- Common PINs
- Bruteforceable PINs
- Efficient bruteforcing sending multiple PINs at once
- The greeting message is an attack vector

Voicemail security today

checklist time!

Voicemail security today

- ✓ Default PINs
- Common PINs
- Bruteforceable PINs
- Efficient bruteforcing by entering multiple PINs at once
- The greeting message is an attack vector

- AT&T
  - 111111
- T-Mobile
  - Last 4 digits of the phone number
- Sprint
  - Last 7 digit of the phone number
- Verizon
  - Last 4 digits of the phone number

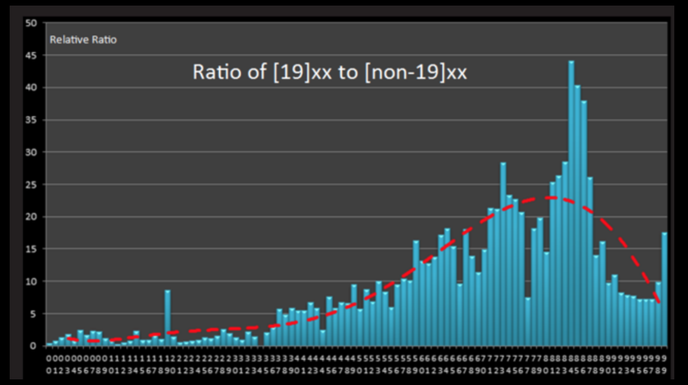
- Vodafone
  - 4 last digits of client number
  - 4 last digits of PUK for CallYa
- Telekom
  - 4 last digits of card number
- O2
  - Random PIN delivered over SMS

Voicemail security today

- ✓ Default PINs
- ✓ Common PINs
- Bruteforceable PINs
- Efficient bruteforcing by entering multiple PINs at once
- The greeting message is an attack vector

2012 Research study by Data Genetics
https://www.datagenetics.com/blog/september32012

#	5		6		7		8		9		10	
	PSWD	%	PSWD	%	PSWD	%	PSWD	%	PSWD	%	PSWD	%
#1	12345	22.802%	123456	11.684%	1234567	3.440%	12345678	11.825%	123456789	35.259%	1234567890	20.431%
#2	11111	4.484%	123123	1.370%	7777777	1.721%	11111111	1.326%	987654321	3.661%	0123456789	2.323%
#3	55555	1.769%	111111	1.296%	1111111	0.637%	88888888	0.959%	123123123	1.587%	0987654321	2.271%
#4	00000	1.258%	121212	0.623%	8675309	0.465%	87654321	0.815%	789456123	1.183%	1111111111	2.087%
#5	54321	1.196%	123321	0.591%	1234321	0.220%	00000000	0.675%	999999999	0.825%	1029384756	1.293%
#6	13579	1.112%	666666	0.577%	0000000	0.188%	12341234	0.569%	147258369	0.591%	9876543210	0.971%
#7	77777	0.618%	000000	0.521%	4830033	0.158%	69696969	0.348%	741852963	0.455%	0000000000	0.942%
#8	22222	0.454%	654321	0.506%	7654321	0.154%	12121212	0.320%	111111111	0.425%	1357924680	0.479%
#9	12321	0.412%	696969	0.454%	5201314	0.128%	11223344	0.293%	123454321	0.413%	1122334455	0.441%
#10	99999	0.397%	112233	0.417%	0123456	0.124%	12344321	0.275%	123654789	0.378%	1234512345	0.402%
#11	33333	0.338%	159753	0.283%	2848048	0.124%	77777777	0.262%	147852369	0.356%	1234554321	0.380%
#12	00700	0.261%	292513	0.250%	7005425	0.120%	99999999	0.223%	111222333	0.304%	5555555555	0.259%
#13	90210	0.244%	131313	0.235%	1080413	0.111%	22222222	0.219%	963852741	0.255%	1212121212	0.244%
#14	88888	0.217%	123654	0.228%	7895123	0.107%	55555555	0.205%	321654987	0.253%	9999999999	0.231%
#15	38317	0.216%	222222	0.212%	1869510	0.102%	33333333	0.176%	420420420	0.241%	2222222222	0.219%
#16	09876	0.185%	789456	0.209%	3223326	0.100%	44444444	0.165%	007007007	0.227%	7777777777	0.206%
#17	44444	0.179%	999999	0.194%	1212123	0.096%	66666666	0.160%	135792468	0.164%	3141592654	0.195%
#18	98765	0.169%	101010	0.190%	1478963	0.088%	11112222	0.140%	397029049	0.158%	3333333333	0.186%
#19	01234	0.160%	777777	0.188%	2222222	0.085%	13131313	0.131%	012345678	0.154%	7894561230	0.165%
#20	42069	0.154%	007007	0.186%	5555555	0.082%	10041004	0.127%	123698745	0.152%	1234567891	0.161%



Voicemail security today

- ✓ Default PINs
- ✓ Common PINs
- ✓ Bruteforceable PINs
- Efficient bruteforcing by entering multiple PINs at once
- The greeting message is an attack vector

- AT&T
  - 4 to 10 digits
- T-Mobile
  - 4 to 7 digits
- Sprint
  - 4 to 10 digits
- Verizon
  - 4 to 6 digits

- Vodafone
  - 4 to 7 digits
- Telekom
  - 4 to 10 digits
- O2
  - 4 to 10 digits

Voicemail security today

- ✓ Default PINs
- ✓ Common PINs
- ✓ Bruteforceable PINs
- ✓ Efficient bruteforcing by entering multiple PINs at once
- The greeting message is an attack vector

- Supports multiple pins at a time
  - 0000#1111#2222#
- Without waiting for prompt
  - or error messages

voicemailcracker.py

bruteforcing voicemails fast, cheap, easy, efficiently and undetected

voicemailcracker.py

- Fast
  - Uses Twilio's APIs to make hundreds of calls at a time
- Cheap
  - Entire 4 digits keyspace for $40
  - A 50% chance of correctly guessing a 4 digit PIN for $5
  - Check 1000 phone numbers for default PIN for $13
- Easy
  - Fully automated
  - Configured with specific payloads for major carriers
- Efficient
  - Optimizes bruteforcing
  - Tries multiple PINs in the same call
  - Uses existing research to prioritize default PINs, common PINs, patterns, etc.

Undetected

Straight to voicemail

- Multiple calls at the same time
  - It's how *slydial* service works in reality
- Call when phone is offline
  - OSINT
    - Airplane, movie theater, remote trip, Do Not Disturb
  - Query HLR database
  - Online services like realphonevalidation.com
- Class 0 SMS
  - Reports back if it was displayed

- Use backdoor voicemail numbers
  - No need to call the victim!

AT&T: 408-307-5049

Verizon: 301-802-6245

T-Mobile: 805-637-7243

Sprint: 513-225-6245

Vodafone: XXX-55-XXXXXXXX

Telekom: XXX-13-XXXXXXXX

O2: XXX-33-XXXXXXXX

voicemailcracker.py

- Fast
  - Uses Twilio's APIs to make hundreds of calls at a time
- Cheap
  - Entire 4 digits keyspace for $40
  - A 50% chance of correctly guessing a 4 digit PIN for $5
  - Check 1000 phone numbers for default PIN for $13
- Easy
  - Fully automated
  - Configured with specific payloads for major carriers
- Efficient
  - Optimizes bruteforcing
  - Tries multiple PINs in the same call
  - Uses existing research to prioritize default PINs, common PINs, patterns, etc.
- **Undetected**
  - **Supports backdoor voicemail numbers**

Bruteforce protections

Different flavors in Germany

Vodafone

Resets to a 6 digit PIN
and sends it over SMS

Telekom

Blocks the Caller ID from
accessing mailbox
or even leaving messages

O2

Blocks the Caller ID from
accessing mailbox
or even leaving messages

Caller IDs are cheap

Vodafone

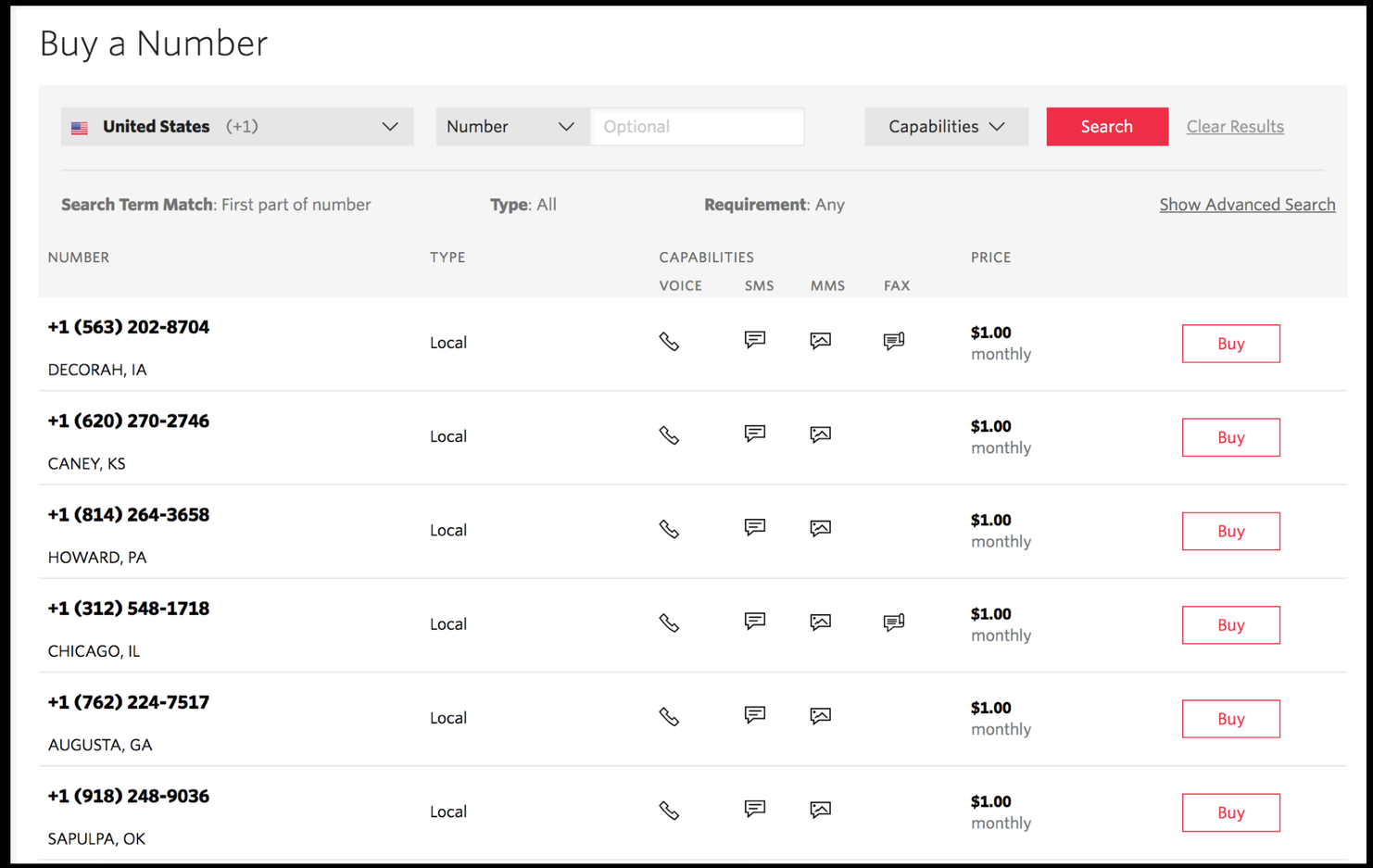
Resets to a 6 digit PIN and sends it over SMS

Telekom

Blocks the Caller ID from accessing mailbox or even leaving messages

O2

Blocks the Caller ID from accessing mailbox or even leaving messages



voicemailcracker.py

- Fast
  - Uses Twilio's APIs to make hundreds of calls at a time
- Cheap
  - Entire 4 digits keyspace for $40
  - A 50% chance of correctly guessing a 4 digit PIN for $5
  - Check 1000 phone numbers for default PIN for $13

- Easy
  - Fully automated
  - Configured with specific payloads for major carriers
- Efficient
  - Optimizes bruteforcing
  - Tries multiple PINs in the same call
  - Uses existing research to prioritize default PINs, common PINs, patterns, etc.
- **Undetected**
  - **Supports backdoor voicemail numbers**
- **Bruteforce protection bypass**
  - **Supports Caller ID randomization**

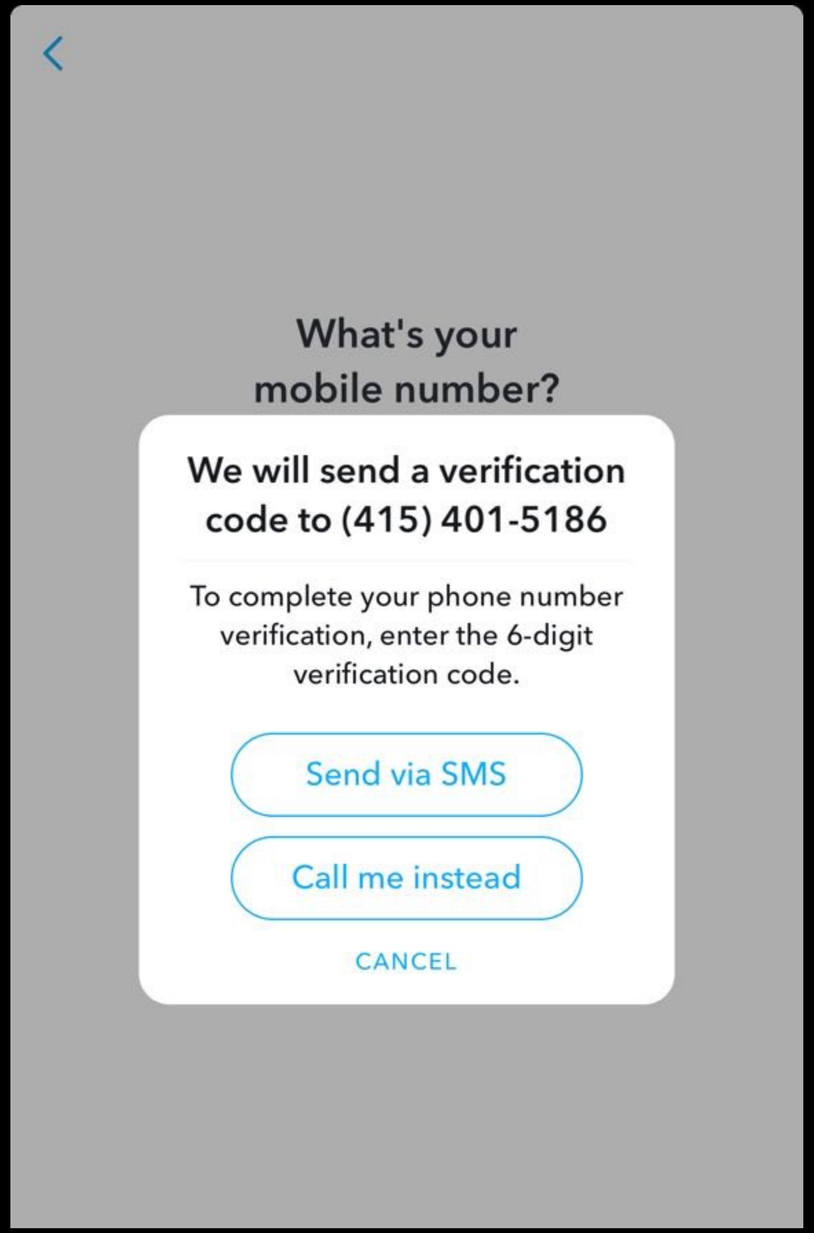
Demo

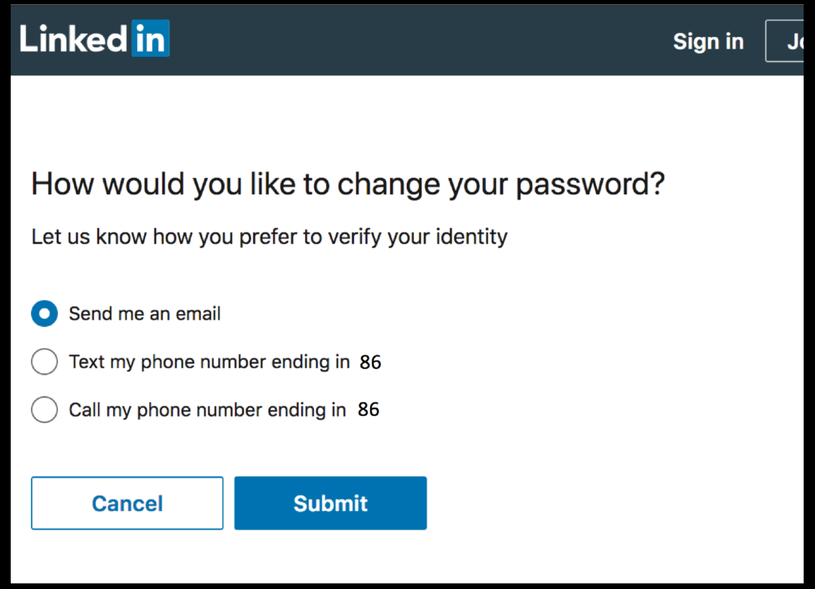
bruteforcing voicemail systems with voicemailcracker.py

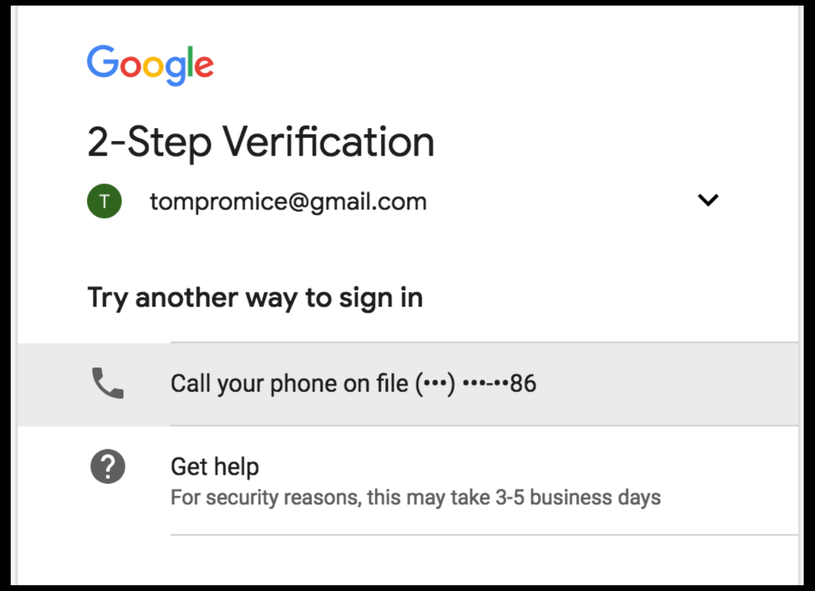

Terminal Shell Edit View Window Help
00:56
100%
Tue 5:34 PM
09:41
100%
Mail
Tuesday
26
Calendar
Photos
Camera
Maps
Clock
Weather
News
Home
Notes
Stocks
Reminders
6
App Store
iTunes Store
iBooks
Health
Wallet
Google Maps
WiFi Map
Files
Extras
FaceTime
Podcasts
voicemail cracking — bash — 83×37
~/Google Drive/Research/voicemail cracking — node /usr/local/bin/lt --port 8080
~/Google Drive/Research/voicemail cracking — bash
bash-3.2$ python voicemailcracker.py bruteforce --victimnumber 4154015186 --carrier
tmobile --callerid 4153048826 --backdoornumber 8056377243 --toppins

Impact

so what?


What's your mobile number?
We will send a verification code to (415) 401-5186
To complete your phone number verification, enter the 6-digit verification code.
Send via SMS
Call me instead
CANCEL


LinkedIn
Sign in
How would you like to change your password?
Let us know how you prefer to verify your identity
Send me an email
Text my phone number ending in 86
Call my phone number ending in 86
Cancel
Submit


Google
2-Step Verification
tompromice@gmail.com
Try another way to sign in
Call your phone on file (•••) •••-••86
Get help
For security reasons, this may take 3-5 business days

What happens if you don’t pick up?

Voicemail takes the
call and records it!

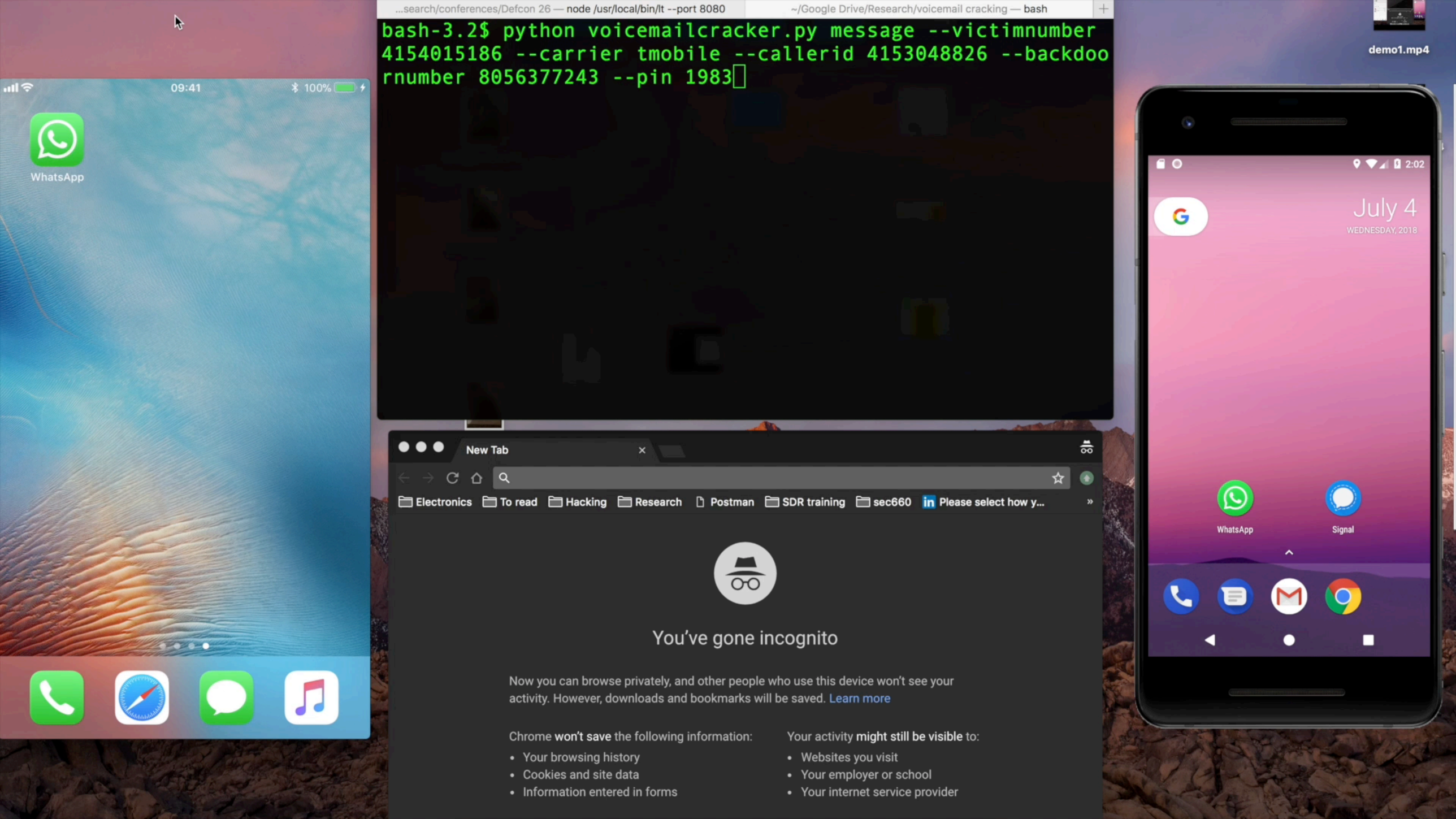
Attack vector

1. Bruteforce voicemail system, ideally using backdoor numbers
2. Ensure calls go straight to voicemail (call flooding, OSINT, etc.)
3. Start password reset process using “Call me” feature
4. Listen to the recorded message containing the secret code
5. Profit!

voicemailcracker.py can do all this automatically

Demo

compromising WhatsApp


...search/conferences/Defcon 26 — node /usr/local/bin/lt --port 8080
~/Google Drive/Research/voicemail cracking — bash
bash-3.2$ python voicemailcracker.py message --victimnumber 4154015186 --carrier tmobile --callerid 4153048826 --backdoornumber 8056377243 --pin 1983
demo1.mp4
09:41
100%
WhatsApp
New Tab
Electronics
To read
Hacking
Research
Postman
SDR training
sec660
Please select how y...
You've gone incognito
Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more
Chrome won't save the following information:
Your browsing history
Cookies and site data
Information entered in forms
Your activity might still be visible to:
Websites you visit
Your employer or school
Your internet service provider
2:02
July 4
WEDNESDAY, 2018
WhatsApp
Signal

We done? Not yet…

User interaction based protection

Please press any key to hear the code…

Please press [ARANDOMKEY] to hear the code…

Please enter the code…

Can we beat this
recommended protection?

Hint

Another hint

- ✓ Default PINs
- ✓ Common PINs
- ✓ Bruteforceable PINs
- ✓ Efficient bruteforcing by entering multiple PINs at once
- ☐ The greeting message is an attack vector

We can record DTMF tones as the greeting message!

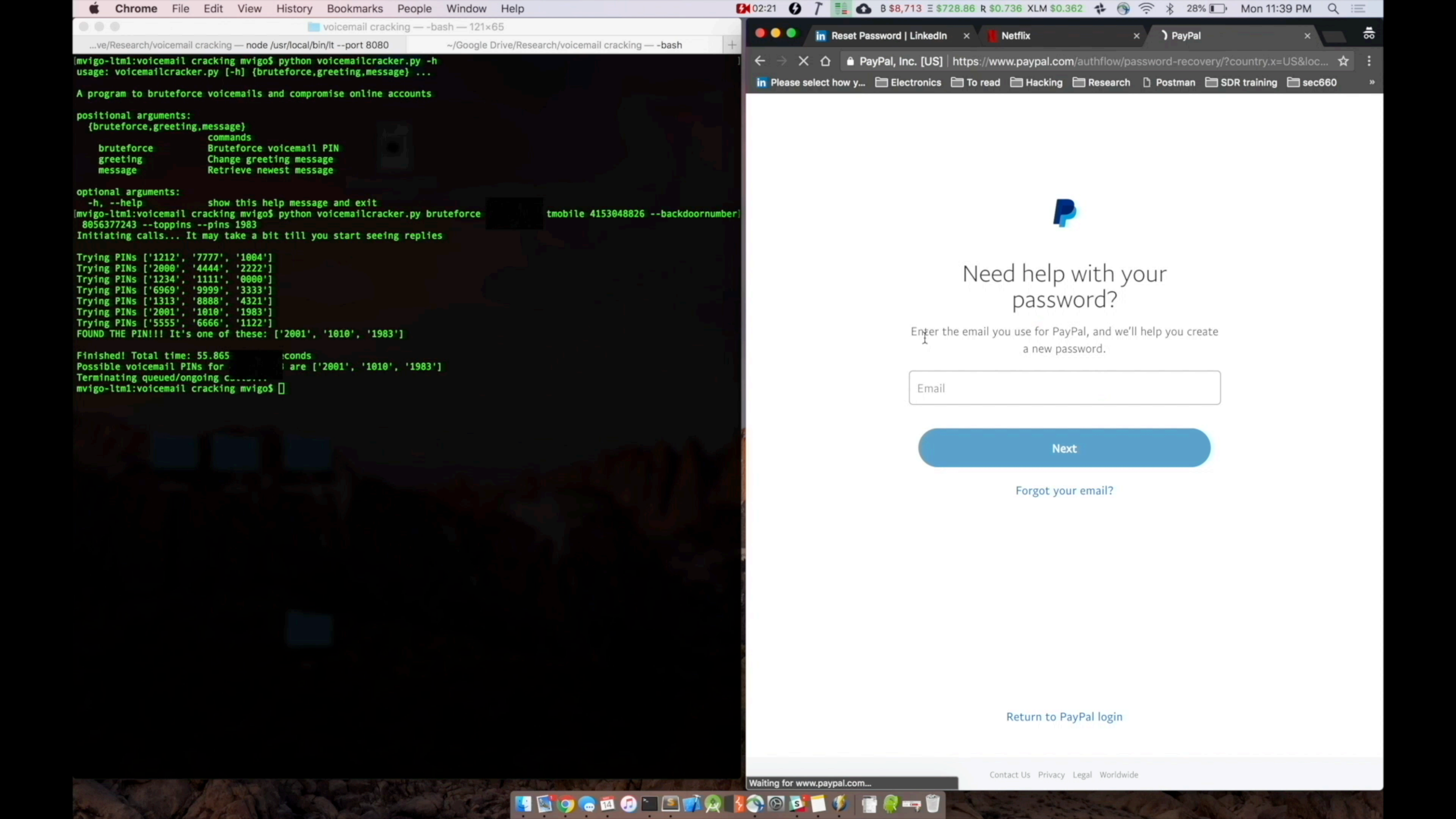
Attack vector

1. Bruteforce voicemail system, ideally using backdoor numbers
2. Update greeting message according to the account to be hacked
3. Ensure calls go straight to voicemail (call flooding, OSINT, etc.)
4. Start password reset process using “Call me” feature
5. Listen to the recorded message containing the secret code
6. Profit!

voicemailcracker.py can do all this automatically

Demo

compromising Paypal


Chrome File Edit View History Bookmarks People Window Help
02:21
Mon 11:39 PM
voicemail cracking — -bash — 121×65
...ve/Research/voicemail cracking — node /usr/local/bin/lt --port 8080
~/Google Drive/Research/voicemail cracking — -bash
mvigo-ltm1:voicemail cracking mvigo$ python voicemailcracker.py -h
usage: voicemailcracker.py [-h] {bruteforce,greeting,message} ...
A program to bruteforce voicemails and compromise online accounts
positional arguments:
{bruteforce,greeting,message}
commands
bruteforce Bruteforce voicemail PIN
greeting Change greeting message
message Retrieve newest message
optional arguments:
-h, --help show this help message and exit
mvigo-ltm1:voicemail cracking mvigo$ python voicemailcracker.py bruteforce tmobile 4153048826 --backdoornumber
8056377243 --toppins --pins 1983
Initiating calls... It may take a bit till you start seeing replies
Trying PINs ['1212', '7777', '1004']
Trying PINs ['2000', '4444', '2222']
Trying PINs ['1234', '1111', '0000']
Trying PINs ['6969', '9999', '3333']
Trying PINs ['1313', '8888', '4321']
Trying PINs ['2001', '1010', '1983']
Trying PINs ['5555', '6666', '1122']
FOUND THE PIN!!! It's one of these: ['2001', '1010', '1983']
Finished! Total time: 55.865 conds
Possible voicemail PINs for are ['2001', '1010', '1983']
Terminating queued/ongoing c...
mvigo-ltm1:voicemail cracking mvigo$
Reset Password | LinkedIn
Netflix
PayPal
PayPal, Inc. [US] https://www.paypal.com/authflow/password-recovery/?country.x=US&loc...
Please select how y...
Electronics
To read
Hacking
Research
Postman
SDR training
sec660
Need help with your password?
Enter the email you use for PayPal, and we'll help you create a new password.
Email
Next
Forgot your email?
Return to PayPal login
Contact Us
Privacy
Legal
Worldwide
Waiting for www.paypal.com...

Vulnerable services

small subset

Password reset

2FA

Google

Microsoft

YAHOO!

Verification

Physical security

Consent

Open source

voicemailautomator.py

- No bruteforcing
- Limited to 1 carrier
- Change greeting message with specially crafted payloads
- Retrieve messages containing the secret temp codes

Git repo: github.com/martinvigo/voicemailautomator

Recommendations

Still…do I care?

```
if (carriersSetDefaultPins == TRUE)
    if (testingForDefaultPinsCheapFastUndetectedAutomatable == TRUE)
        if (updatingGreetingMessageAutomatable == TRUE)
            if (retrievingNewestMessageAutomatable == TRUE)
                if (speechToTextTranscription == TRUE)
                    if (accountCompromiseIsAutomatable == TRUE)
                        print “Yes, I should care”
```

Recommendations for online services

- Don’t use automated calls for security purposes
- If not possible, detect answering machine and fail
- Require user interaction before providing the secret
  - with the hope that carriers ban DTMF tones from greeting messages

Recommendations for carriers

- Ban DTMF tones from greeting messages
- Eliminate backdoor voicemail services
  - or at least no access to login prompt from them
- Voicemail disabled by default
  - and can only be activated from the actual phone or online
- No default PIN
- Don’t allow common PINs
- Detect and prevent bruteforce attempts
- Don’t process multiple PINs at once

Recommendations for you

- Disable voicemail
  - or use longest possible, random PIN
- Don’t provide phone number to online services unless required
  - or it’s the only way to get 2FA
  - use a virtual number to prevent OSINT and SIM swapping
- Use 2FA apps only

TL;DR

Automated phone calls are a common solution for password reset, 2FA, verification and other services. These can be compromised by leveraging old weaknesses and current technology to exploit the weakest link, voicemail systems

Strong password policy

2FA enforced

Abuse/Bruteforce prevention

A+ in OWASP Top 10 checklist

Military grade crypto end to end

Lots of cyber

Password reset | 2FA | Verification | Consent

over phone call

Danke schön!

@martin_vigo

martinvigo.com

martinvigo@gmail.com

linkedin.com/in/martinvigo

github.com/martinvigo

youtube.com/martinvigo