Compromising online services by cracking voicemail systems

Martin Vigo

@martin_vigo | martinvigo.com

DEFCON

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

United States Patent [19]

Matthews et al.

[11] **4,371,752**

[45] **Feb. 1, 1983**

[54] **ELECTRONIC AUDIO COMMUNICATION SYSTEM**

[75] Inventors: **Gordon H. Matthews**, Plano; **Thomas B. Tansil**; **Michael L. Fannin**, both of Dallas, all of Tex.

[73] Assignee: **ECS Telecommunications, Inc.**, Dallas, Tex.

[21] Appl. No.: **97,240**

[22] Filed: **Nov. 26, 1979**

[51] **Int. Cl.**[3] **H04M 1/66**; H04M 3/42; H04M 5/04

[52] **U.S. Cl.** ..... 179/18 BF; 179/18 DA

[58] **Field of Search** ..... 179/18 B, 18 BF, 5 P, 179/18 ES, 1 SM, 7.1 TP, 18 DA, 6.01, 6.02, 6.05, 6.2, 6.17; 360/32, 12; 370/61, 60, 94, 67, 85, 62, 86

[56] **References Cited**

U.S. PATENT DOCUMENTS

2,385,968	10/1945	Deakin	179/6 E
2,868,880	1/1959	Celetano	179/6
2,998,489	8/1961	Riesz	179/6 C
3,141,931	7/1964	Zarouni	179/6 E
3,175,039	3/1965	Wilbourn, Jr.	179/7.1 TP
3,190,961	6/1965	Fitzpatrick et al.	179/6 E
4,072,825	2/1978	McLay et al.	179/18 B
4,138,597	2/1979	Ashford	370/67
4,144,582	3/1979	Hyatt	364/900
4,160,125	7/1979	Bower et al.	179/6 D
4,188,507	2/1980	Meri et al.	179/6 D
4,229,624	10/1980	Haben et al.	179/18 E

FOREIGN PATENT DOCUMENTS

2412382	9/1975	Fed. Rep. of Germany	129/1 SM
507954	4/1976	U.S.S.R.	179/6 D

OTHER PUBLICATIONS

"Unified Communications System Serves Five Hospitals at Detroit Medical Center", Carl O. Haven, *Computerworld Version*, Oct. 29, 1973.

"IBM Voice Storage Network Described", R. A. Frank, *Communications Weekly*, 1978.

"New Custom Calling Services", Bergland et al., International Switching Symposium, Paris, May 11, 1979, pp. 1–7.

"New Custom Calling Services", Nacon and Worrall, International Conference on Communications, Boston, Mass., Jun. 1979, pp. 1–5.

"Prospectives in Voice Response from Computers", Wm. D. Chapman, *Proceedings of International Conference on Communications*, San Francisco, Jun. 1970, pp. 45–1 to 45–8.

"DMS–10 System Organization", Rushing & Totti, *Telesos* (Canada), Aug. 1978, pp. 303–308.

History: hacking voicemail systems

- When?
  - In the 80s
- What?
  - Mostly unused boxes that were part of business or cellular phone systems
- Why?
  - As an alternative to BSS
  - Used as a "home base" for communication
  - Provided a safe phone number for phreaks to give out to one another
  - http://audio.textfiles.com/conferences/PHREAKYBOYS

How?

back to ezines

“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

“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:
1234567898765432135792468642973147419336699
448855227753959637258283849181716151102620304050607080900 1
(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

Voicemail security in the 80s

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

Voicemail security today checklist time!

Voicemail security today

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

- AT&T
  - 111111
- T-Mobile
  - Last four digits of the phone number
- Sprint
  - Last 7 digit of the phone number
- Verizon
  - Last 4 digits of the phone number
    - According to verizon.com/support/smallbusiness/phone/setupphone.htm

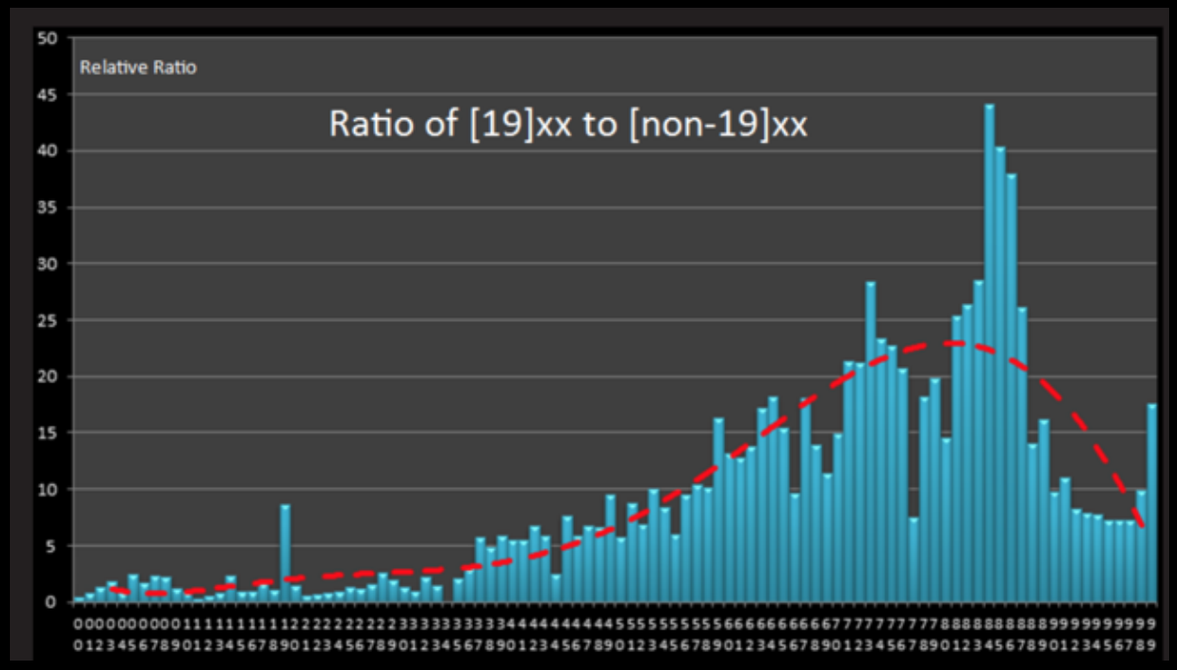
Voicemail security today

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

2012 Research study by Data Genetics

http://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 passwords
- ✓ Common passwords
- ✓ Bruteforceable passwords

- Efficient bruteforcing by entering multiple passwords 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

Voicemail security today

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

- Can try 3 pins at a time
- Without waiting for prompt or error message

voicemailcracker.py

bruteforcing voicemails fast, cheap, easy, efficiently and undetected

voicemailcracker.py

- Fast
  - Uses Twilio's services 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
    - HLR Records
        - Queryable global GSM database
        - Provides mobile device information including connection status
- **Use backdoor voicemail numbers**
    - No need to dial victim's number!
        - AT&T: 408-307-5049
        - Verizon: 301-802-6245
        - T-Mobile: 805-637-7243
        - Sprint: 513-225-6245

voicemailcracker.py

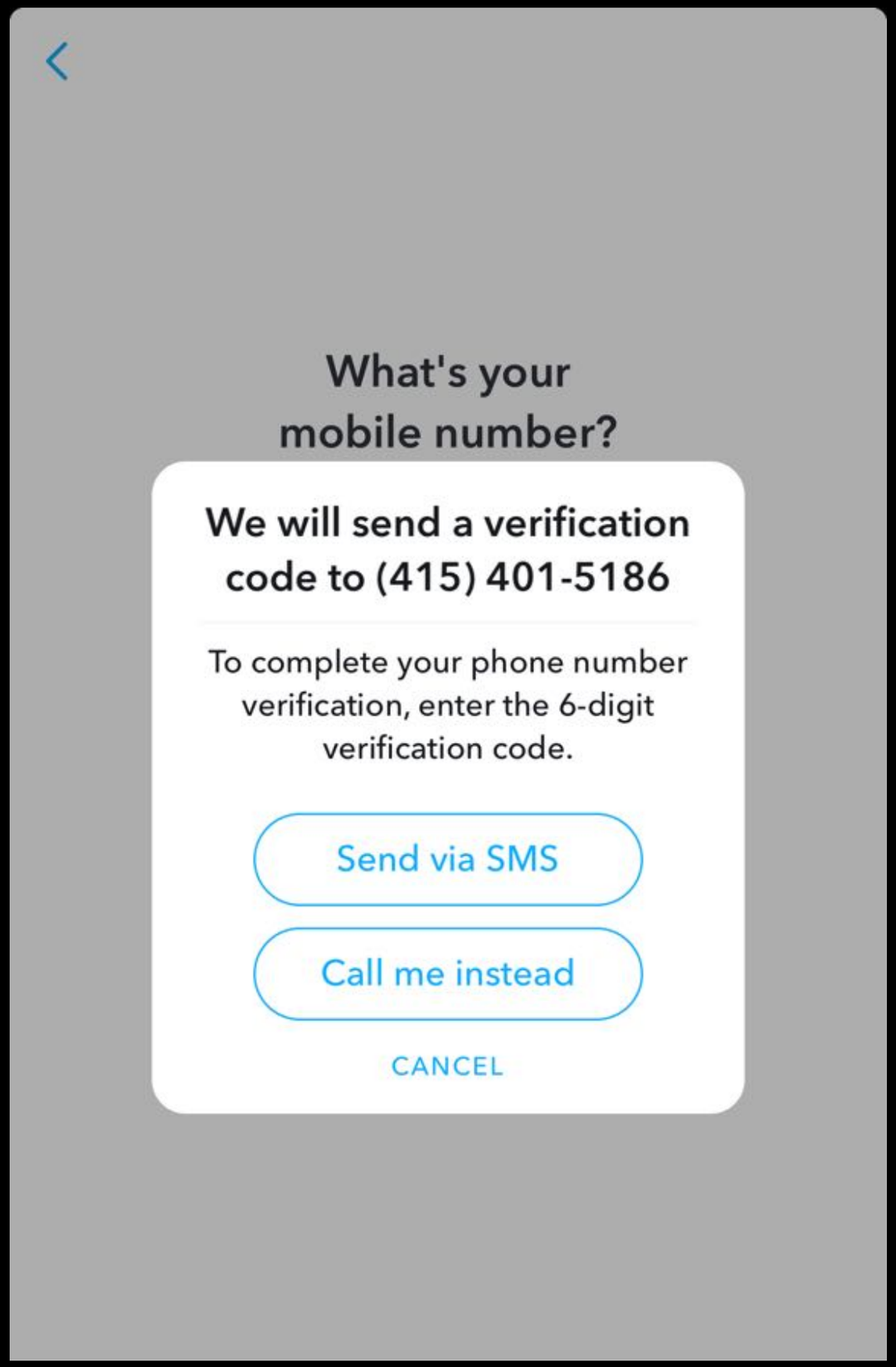
- Fast
    - Uses Twilio’s services to make hundreds of calls at a time
- Cheap
    - All 4 digits keyspace under $10
- Easy
    - Enter victim’s phone number and wait for the PIN
    - Configured with specific payloads for major carriers
- Efficient
    - Optimizes bruteforcing
    - Tries multiple PINs in the same call
    - Uses existing research to prioritize default PINs, common PINs, patterns, etc.
- **Undetected**
    - **Supports backdoor voicemail numbers**

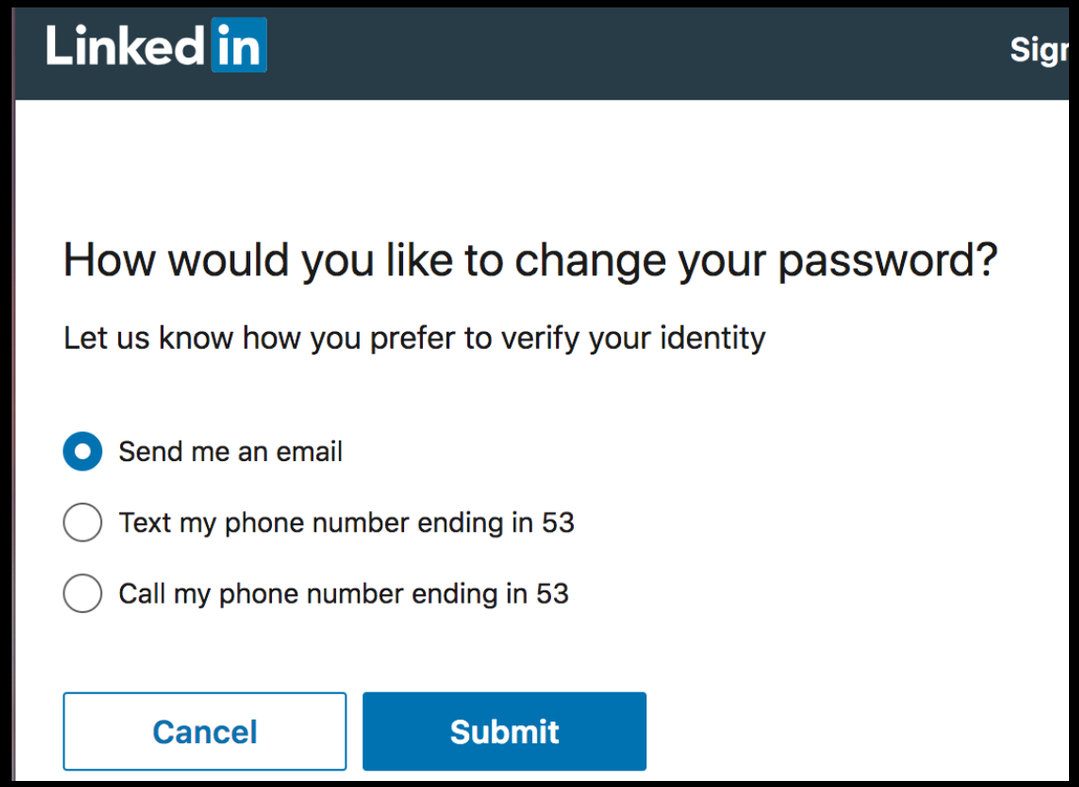
Demo

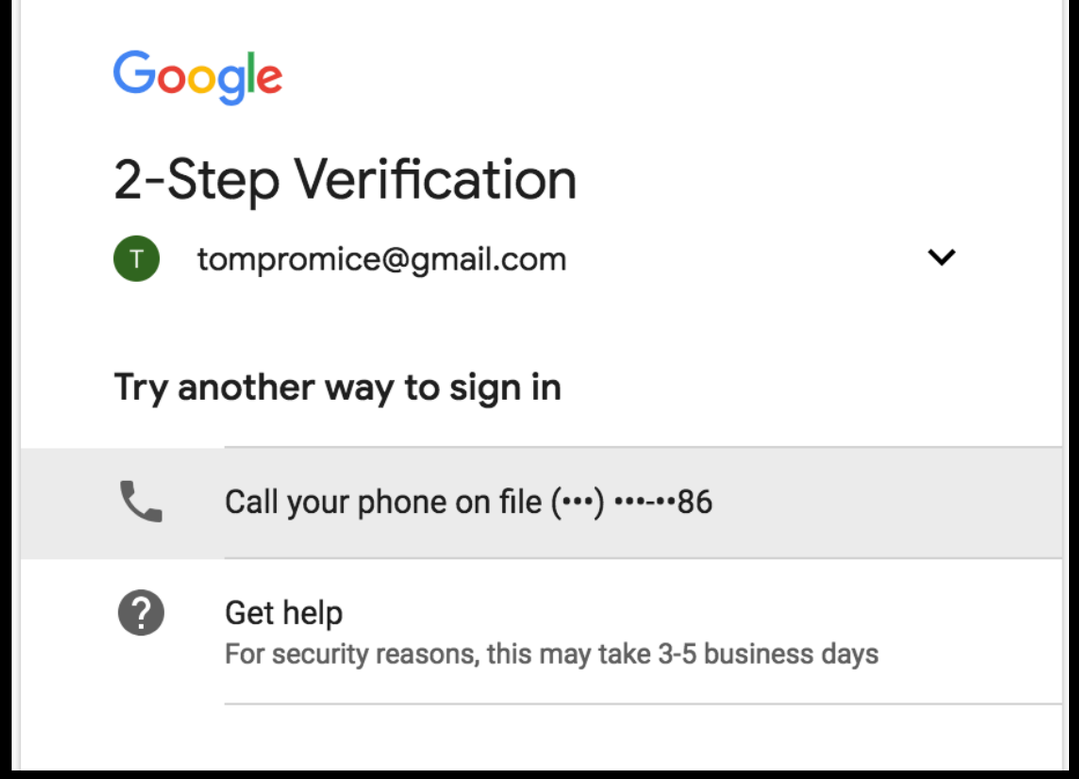
bruteforcing voicemail systems with voicemailcracker.py

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


Linked in
Sign
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 53
Call my phone number ending in 53
Cancel
Submit


Google
2-Step Verification
T
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, HLR records)

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 for you!

Demo

compromising WhatsApp

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 currently recommended protection?

Hint

Another hint

- ✓ Default passwords
- ✓ Common passwords
- ✓ Bruteforceable passwords
- ✓ Efficient bruteforcing by entering multiple passwords 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, HLR records)
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 for you!

Demo

compromising Paypal

Vulnerable services

small subset

Password reset

2FA

Google

Microsoft

YAHOO!

Verification

WhatsApp

Signal
Secure Messaging App

twilio

Google Voice

Open source

voicemailcracker.py limited edition

- Support for 1 carrier only
- No bruteforcing
- Change greeting message with specially crafted payloads
- Retrieve messages containing the secret temp codes

Git repo: https://github.com/martinvigo

Recommendations

Recommendations for online services

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

Recommendations for carriers

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

Recommendations for you

- Disable voicemail
  - or use longest possible, random PIN
- Don’t provide phone number to online services unless strictly required
- Use only 2FA apps

TL;DR

Automated phone calls are a common solution for password reset, 2FA and verification 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 over phone call

THANK YOU!

@martin_vigo

martinvigo.com

martinvigo@gmail.com

linkedin.com/in/martinvigo

github.com/martinvigo

youtube.com/martinvigo