![KnowBe4 - Human error. Conquered.]

Many Ways to Hack Multi-Factor Authentication

Roger Grimes
Data-Driven Defense Evangelist,
KnowBe4, Inc.
rogerg@knowbe4.com

Roger A. Grimes
**Data-Driven Defense Evangelist**
KnowBe4, Inc.

About Roger

- 30-years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- PKI, smartcards, MFA, biometrics, since 1998
- Consultant to world's largest and smallest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1000 magazine articles
- InfoWorld and CSO weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certifications passed include:

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada
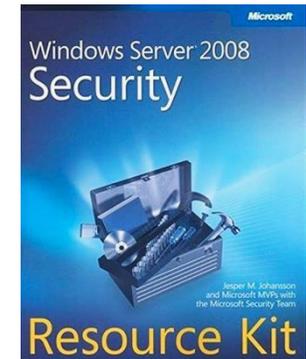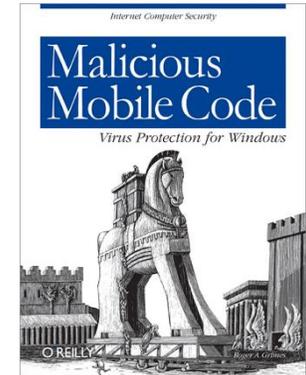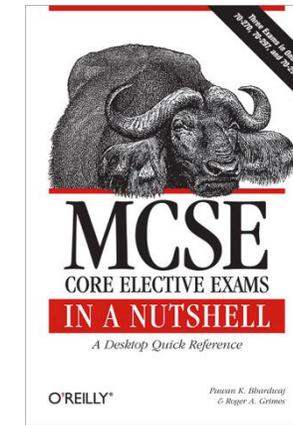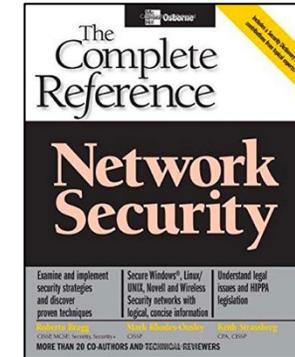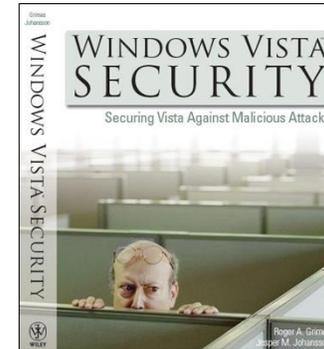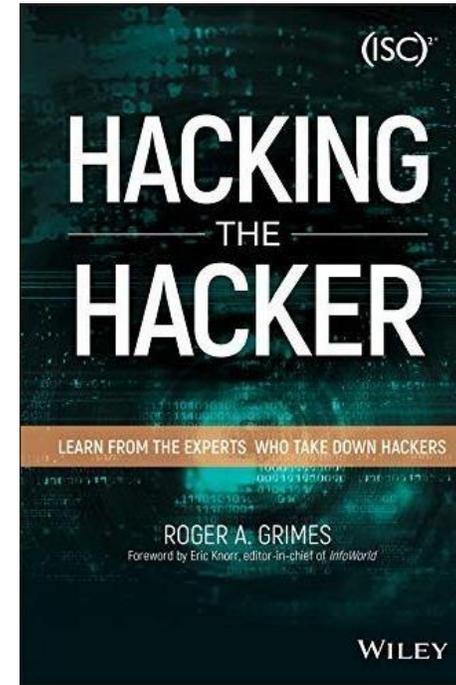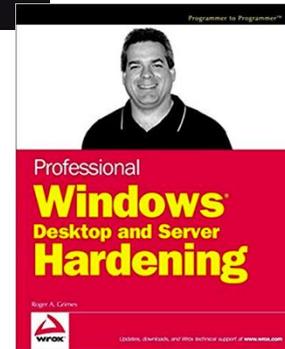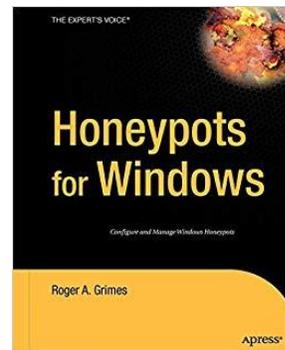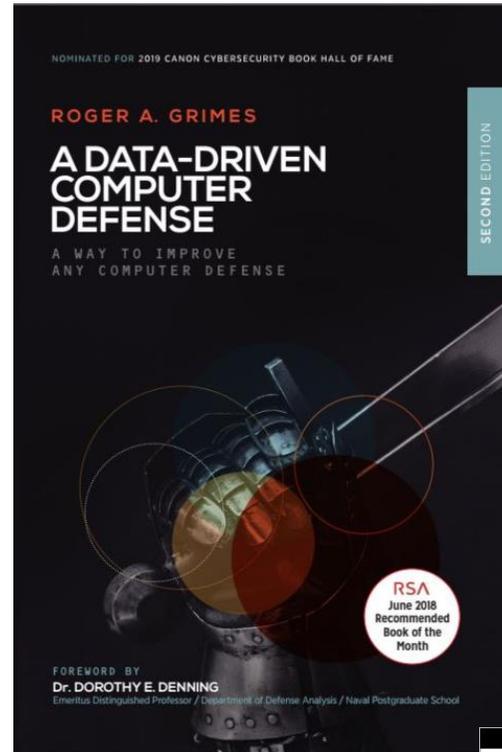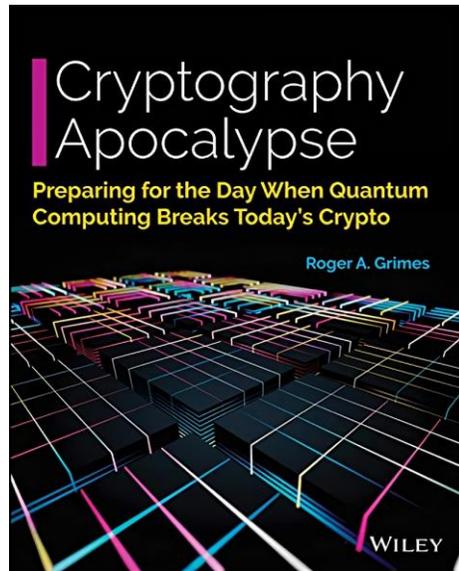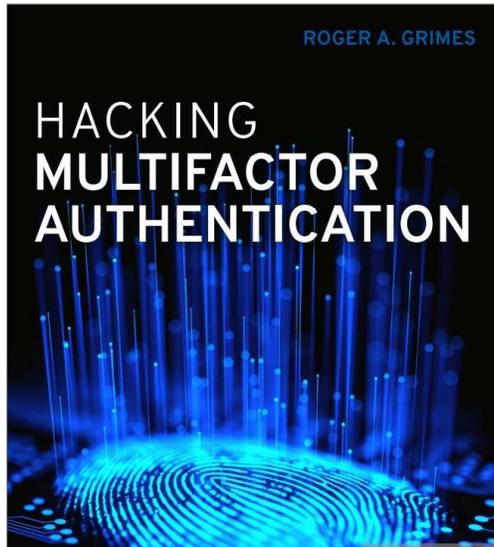
Roger's Books

Today's Presentation

- Multi-Factor Authentication Intro

- Hacking MFA

- Defending Against MFA Attacks

Multi-Factor Authentication Intro

Factors

Introduction to Multi-Factor Authentication

- Something You Know

  - Password, PIN, Connect the Dots, etc.

- Something You Have

  - USB token, smartcard, RFID transmitter, dongle, etc.

- Something You Are

  - Biometrics, fingerprints, retina scan, smell

- Contextual, behavioral analytics, actions, location, etc.

Introduction to Multi-Factor Authentication

Factors

- Single Factor

- Two Factor (2FA)

- Multi-Factor (MFA)

  - 2-3 factors

- Two or more of the same factor isn't as strong as different types of factors

Introduction to Multi-Factor Authentication

Factors

- All things considered, MFA is usually better than 1FA

- We all should strive to use MFA wherever it makes sense and then whenever possible

- But MFA isn't unhackable

First, we need to understand some basic concepts to better understand hacking MFA

Hacking MFA

MFA Hacks

Network Session Hijacking

- Usually requires Man-in-the-Middle (MitM) attacker

- Attacker puts themselves inside of the communication stream between legitimate sender and receiver

- Doesn't usually care about authentication that much

- Just wants to steal resulting, legitimate access session token after successful authentication

- On web sites, session tokens are usually represented by a "cookie" (a simple text file containing information unique for the user/device and that unique session)

- Session token usually just good for session

MFA Hacks

Network Session Hijacking

Network Session Hijacking Proxy Theft

1. Bad guy convinces victim to visit rogue (usually a look-alike) web site, which proxies input to real web site

2. Prompts victim to put in MFA credentials

3. Victim puts in credentials, which bad guy relays to real web site

4. Bad guy intercepts victim's resulting access control token

5. Bad guy logs into real site, and drops legitimate user

6. Takes control over user's account

7. Changes anything user could use to take back control

MFA Hacks

Network Session Hijacking

Kevin Mitnick Hack Demo

https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedin-2-factor-auth.-see-this-kevin-mitnick-video

MFA Hacks

Network Session Hijacking
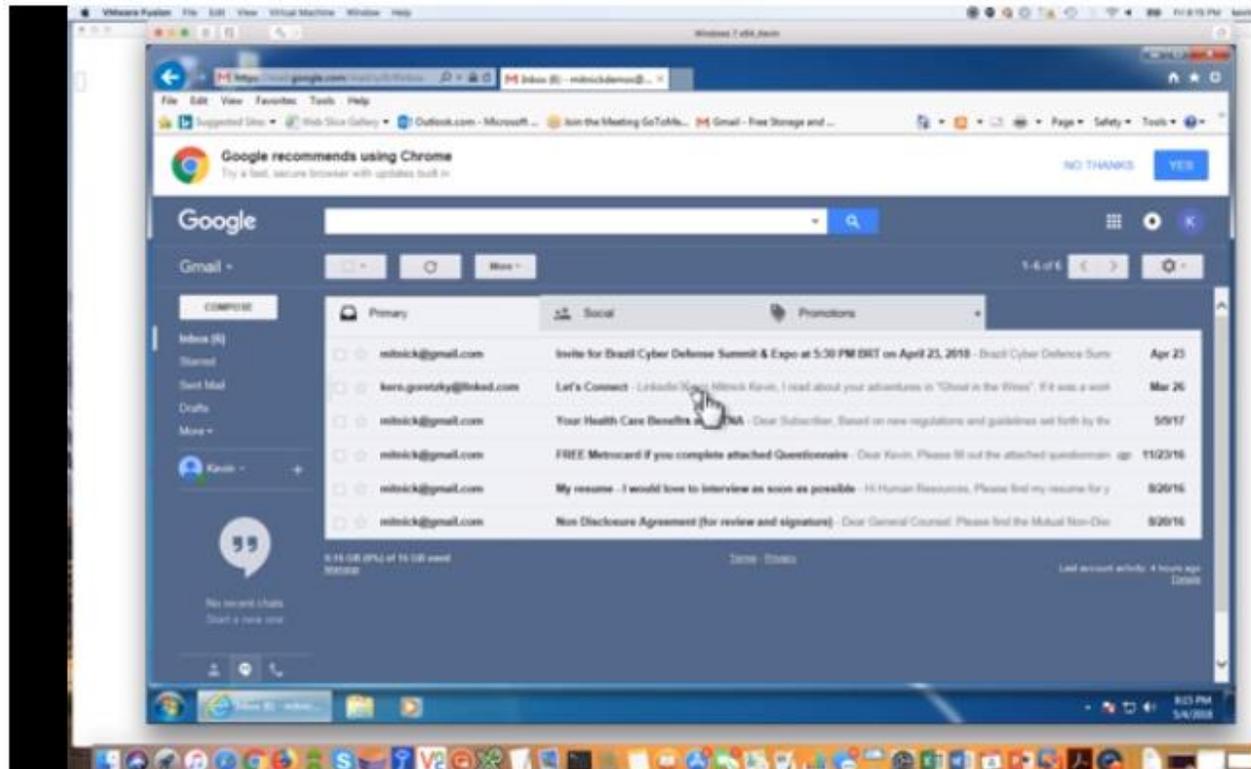
Kevin Mitnick Hack Demo

1. Kevin set up fake look-alike/sound-alike web site that was really an evil proxy

2. Tricked user into visiting evil proxy web site

3. User typed in credentials, which proxy, now pretending to be the legitimate customer, presented to legitimate web site

4. Legitimate web site sent back legitimate session token, which Kevin then stole and replayed to take over user's session

- Kevin used Evilginx (https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/)

- One example hack out of the dozens, if not hundreds of ways to do session hijacking, even if MFA is involved

MFA Hacks

Real-World Example

Is Google To Blame For The Binance Exchange API "Hack"?

March 12, 2018 by Paul Costas — Leave a Comment

This is a follow up to the article on the **Binance exchange API "hack"** based on what we now know.

Binance was quick to stress their exchange was **not hacked**, but to be honest, you would expect that to be their first reaction, to prevent a meltdown. I use the term "hack" as a very general term for any **nefarious computer activities**, which on this occasion appears to be a **very elaborate phishing scam**.

It appears that the fake Binance site that stole the login credentials also hacked the 2FA security. The fake site requested 2FA via the Google Authenticator, and then, during the 60-second timeout for this security feature, it surreptitiously logged into the real Binance site and activated API control on the affected account.

MFA Hacks

Network Session Hijacking

Real-World Example

NOT ALL 2FA WAS CREATED EQUAL. —

Iranian phishers bypass 2fa protections offered by Yahoo Mail and Gmail

Group breaches SMS-protected accounts. It's still testing attacks against 2fa apps.

DAN GOODIN - 12/13/2018, 5:20 PM

messages. When targets entered passwords into a fake Gmail or Yahoo security page, the attackers would almost simultaneously enter the credentials into a real login page. In the event targets' accounts were protected by 2fa, the attackers redirected targets to a new page that requested a one-time password.

Sun, 17/05/2015

Your Google verification code is 252401

SMS 22:10

https://arstechnica.com/information-technology/2018/12/iranian-phishers-bypass-2fa-protections-offered-by-yahoo-mail-and-gmail/
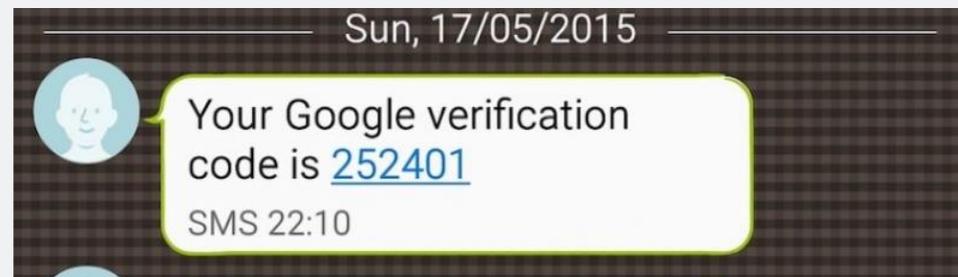
MFA Hacks

Endpoint Attacks

<u>Man-in-the-Endpoint Attacks</u>

If endpoint gets compromised, MFA isn't going to help you

- Attacker can just do everything they want that the user is allowed to do after successful authentication

- Start a second hidden browser session

- Directly steal session cookies

- Insert backdoors

- Invalidate protection all together

MFA Hacks

Endpoint Attacks
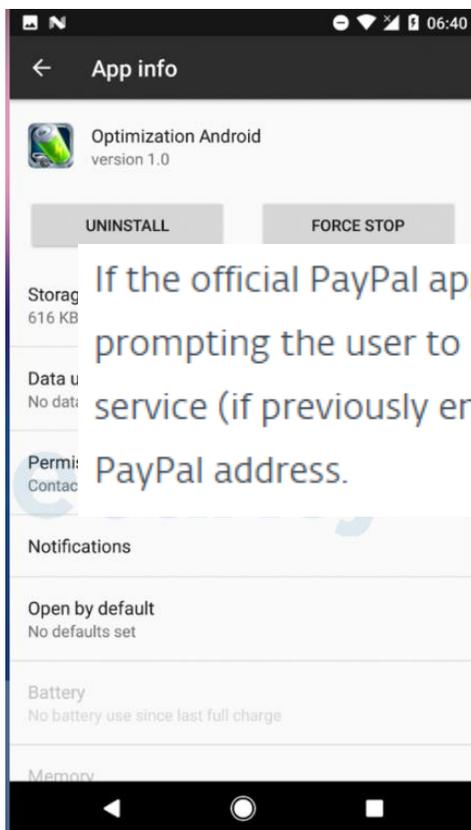
<u>Man-in-the-Endpoint Attacks</u>

- Start up a second session that the user isn't even aware

  - Ex. Bancos trojans

MFA Hacks

Man-in-the-Endpoint Attacks

- Start up a second session that the user isn't even aware

If the official PayPal app is installed on the compromised device, the malware displays a notification alert prompting the user to launch it. Once the user opens the PayPal app and logs in, the malicious accessibility service (if previously enabled by the user) steps in and mimics the user's clicks to send money to the attacker's PayPal address.

https://www.youtube.com/watch?v=yn04eLoivX8

MFA Hacks

Endpoint Attacks

KEY FINDINGS

» The Cybereason Nocturnus team is investigating EventBot, a new type of Android mobile malware that emerged around March 2020. EventBot is a mobile banking trojan and infostealer that abuses Android's accessibility features to steal user data from financial applications, read user SMS messages, and steal SMS messages to allow the malware to bypass two-factor authentication.

» EventBot targets users of over 200 different financial applications, including banking, money transfer services, and crypto-currency wallets. Those targeted include applications like Paypal Business, Revolut, Barclays, UniCredit, CapitalOne UK, HSBC UK, Santander UK, TransferWise, Coinbase, paysafecard, and many more.

» It specifically targets financial banking applications across the United States and Europe, including Italy, the UK, Spain, Switzerland, France, and Germany. The full list of banking applications targeted is included in the appendix.

Security researchers have warned that newly created mobile banking malware can not only grab passwords for more than 200 financial apps, but intercept two-factor authentication codes as well.

Posing as legitimate applications such as a Flash update, installed from unauthorised or compromised sources, EventBot relies upon the unsuspecting user granting it a bunch of permissions from reading external storage and SMS to creating system alert windows that can be shown on top of other apps.

MFA Hacks

SMS-based MFA

- Many MFA methods included sending additional authentication code via a user's cell phone short message service (SMS)

Your ID Experts MyIDCare Verification Passcode is 113497. This code will expire in 15 minutes.

From Marriott: To authorize your Rewards transaction, enter 003452. If you did not request this message, please contact Guest Services at (801) 468-4000.

Your Bank of America SafePass code is "575085". This code will expire in 10 minutes. Please do not reply to this message.

4/22/18 11:00 AM

Your Bank of America SafePass code is "425217". This code will expire in 10 minutes. Please do not reply to this message.

871610 Use this code for Microsoft verification

Use 802912 to log into Facebook.

SIM Swapping

SIM Basics

- SIM stands for **S**ubscriber **I**dentity **M**odule

- SIM storage contains the cell phone vendors network's information, device ID, and the subscriber's (user/owner) phone number and other info, plus can store app data

- Traditionally was stored on micro-SD card

- Today, often stored and moved digitally

- An activated phone with your SIM info will act as your phone, accept and receive phone calls and SMS messages

MFA Hacks

SIM Swapping Attacks
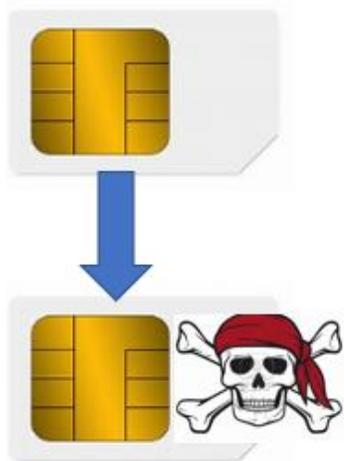
- In a SIM swapping attack, the attacker transfers the victim's SIM information to another phone, allowing the attacker to get the any sent codes used by SMS-based MFA solutions

  - Old phone "silently" stops working

- Usually done by hack social engineering cell phone vendor's support techs; or using a compromised insider

- Often is done using cell phone network logon information the attacker has previously phished out of the victim using another precursor phishing attack

- Some mobile phone trojans steal SIM information

- NIST (in SP 800-63) does not accept SMS codes as valid authentication because of how easy it is to hack

MFA Hacks

SIM Swapping Attacks

- Has been successfully used in many of the world's biggest personal attacks

Smartphone Crypto Hack: The $24 Million AT&T 'Sim Swapping' Mistake

07 Florida Man Arrested in SIM Swap Conspiracy

Food writer Jack Monroe 'loses £5,000 in phone-number hijack'

...n accused of being part of a multi-state ...umbers in online attacks that siphoned ...nd other cryptocurrencies from victims.

'TELL YOUR DAD TO GIVE US BITCOIN:'
How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers

California authorities say a 20-year-old college student hijacked more than 40 phone numbers and stole $5 million, including some from cryptocurrency investors at a blockchain conference Consensus.

01 Reddit Breach Highlights Limits of SMS-Based
AUG 18 Authentication

This Binance User's Account With $50k In Crypto Was Hacked Through A SIM Swap
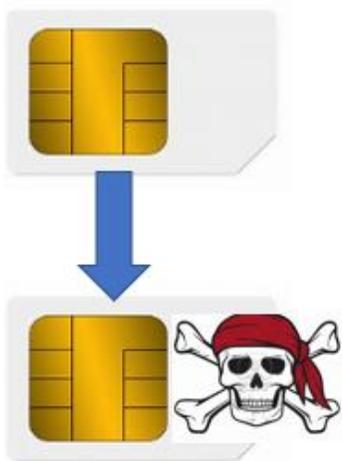
SIM Swapping

SIM Swapping Attack (con't)

- Defense: Use non-SMS-based apps

  - App travels with authenticated user, not phone number or SIM

  - Can't be as easily transferred by 3rd party without your knowledge or participation

  - Not perfect, but stops easy SIM-swapping attacks

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

SMS Rogue Recovery Hack

- There is an inherent problem in that SMS message origination cannot be easily authenticated within SMS itself

- Anyone can claim to be anyone

To pull off hacker must have:

- You email address and associated phone number

Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

1. Hacker sends you a text pretending to be from your email provider asking for your forthcoming SMS PIN reset code
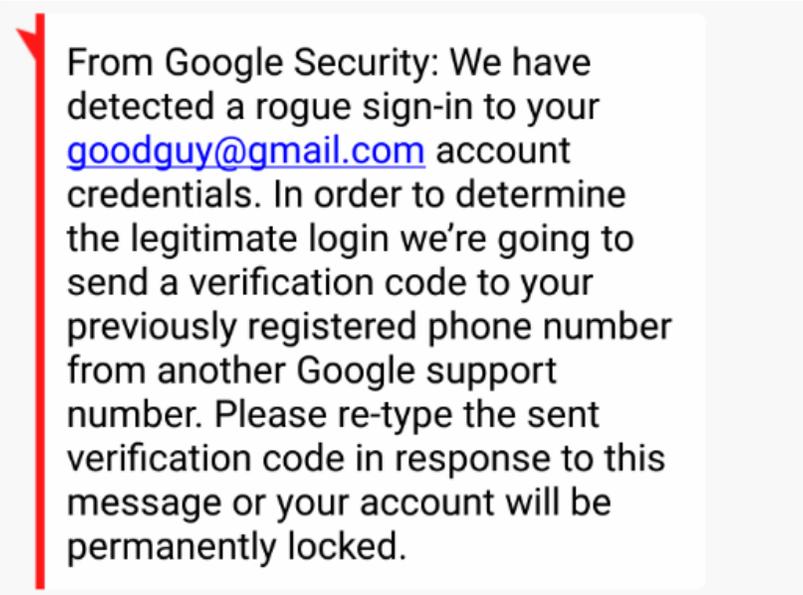
From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

Steps

2. Hacker forces your email account into SMS PIN recovery
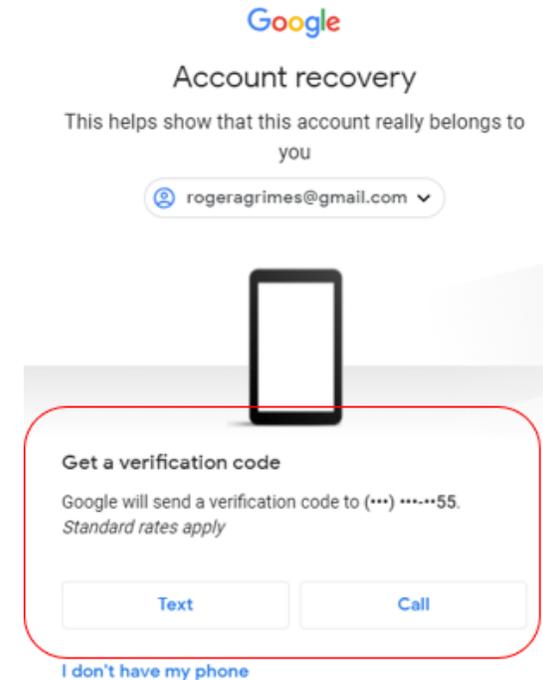
Rogue Recoveries

SMS Rogue Recovery

<u>Hacking Into Your Email Using Recovery Methods</u>

Steps

3. You get text from vendor with your reset code, which you then send to other number

Your Google verification code is
954327

From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.
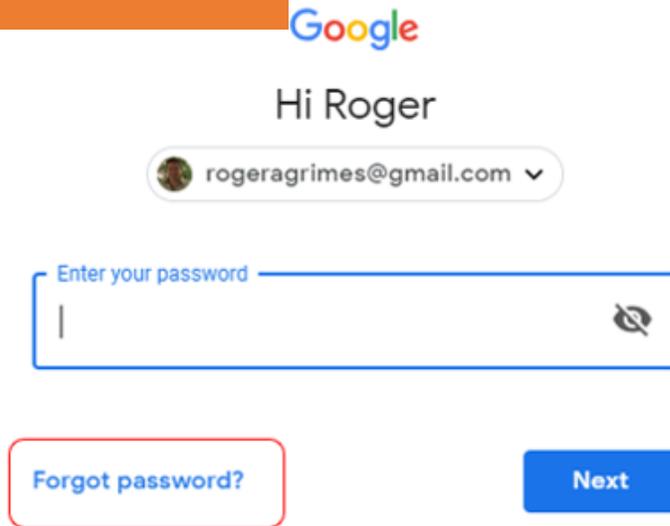
954327

Sent

Rogue Recoveries

SMS Rogue Recovery

Hacking Into Your Email Using Recovery Methods

Steps

4. Hacker uses your SMS PIN code to login to your email account and take it over

Note: To be fair, Google has some of the best recovery options of any email provider, including that it can send a non-SMS message to your phone before the hacker can even get to the SMS code screen to get Google to send an SMS message

Rogue Recoveries

Hacking Into Your Email Using Recovery Methods

Then it got weird.

After confirming that he did not use his card in Miami, Gunst says the caller told him that the transaction had been blocked, and then asked him for his member number.

Gunst then received a legitimate verification pin from the bank's regular number via text, which he promptly read back to the caller -- not realizing that it was a password reset code.

The person on the line -- a scammer -- was in. She could access his account and began to read off recent transactions that Gunst had actually made, lending a bit more credibility to the call.

Then came the next question, which immediately set off a red flag: "We now want to block the pin on your account, so you get a fraud alert when it is used again. What is your pin?"

954327

https://www.msn.com/en-us/news/crime/a-scam-targeting-americans-over-the-phone-has-resulted-in-millions-of-dollars-lost-to-hackers-dont-be-the-next-victim/ar-AAJpE2J

Rogue Warnings

Fake Malicious Warnings

- Similar attack – Fake warning message

- Sends you to a fake, look-alike "verification" web page

⊙ | Instagram

Hi Roger

Someone tried to log in to your Instagram account.

If this wasn't you, please use the following code to confirm your identity. Please sign in:

453212

PayPal: Due to a recent failed payment request your account has been restricted. Visit: https://▨▨▨ to remove any pending restrictions.

PAYPAL: We have detected unusual activity on your account, follow at https://▨▨▨ to continue

Rogue Recoveries

SMS Rogue Recovery

Defenses

- Be aware of rogue recovery messages

- Recognize when SMS recovery PINs should be typed into browsers, not (usually) back into SMS

- Use MFA when possible

- Try to avoid alternate email-based recovery methods

- Try to avoid SMS-based recovery based methods

- Try to minimize public posting of phone numbers related to your recovery account methods

MFA Hacks

Social Engineer Tech Support

- There have been many real-world instances where the user had MFA to a particular web site or service, maybe even required that it be used;

- And hackers socially engineered tech support into disabling it and resetting password, using other information they had learned

- Hackers like to use "stressor" events to achieve their goals

- Humans just want to help, and will bypass policy and controls to do so

MFA Hacks

Social Engineer Tech Support

<u>Great Example</u>

Check out the "Crying baby" social engineering live demo video:

https://www.youtube.com/watch?v=lc7scxvKQOo
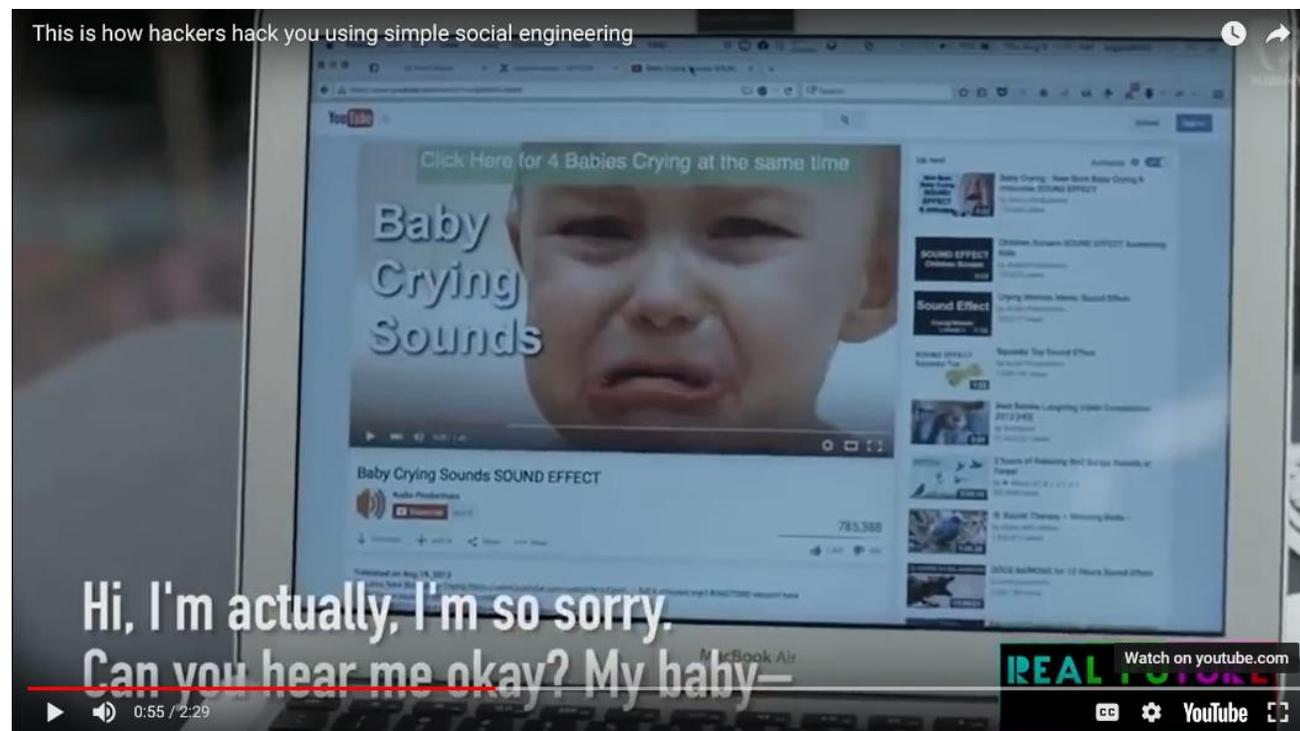
MFA Hacks

Duplicate Code Generator
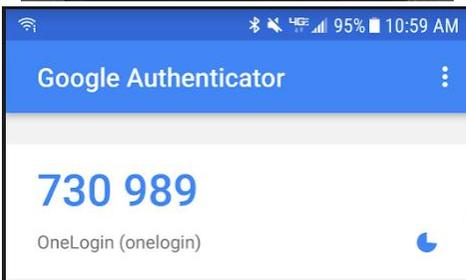
- Most MFA code-generating tokens start with a (randomly) generated (permanently) stored "seed" or "shared secret" value, which is then incremented by some sort of counter/algorithm which generates all subsequent values
  - Known as **one-time passwords** (OTP)
  - "Will never be repeated again"
- Unique user/device identifier usually involved
- May also use current time/date to "randomly" generated code good only for a particular time interval
  - Known as **time-based one-time passwords** (TOTP)

MFA Hacks

Duplicate Code Generator

- Shared secret will always be present in at least two places (e.g. source database/verifier and device itself)

- Attackers that learn seed/shared secret and algorithm can generate duplicate/identical code generators that match the victim's code generator

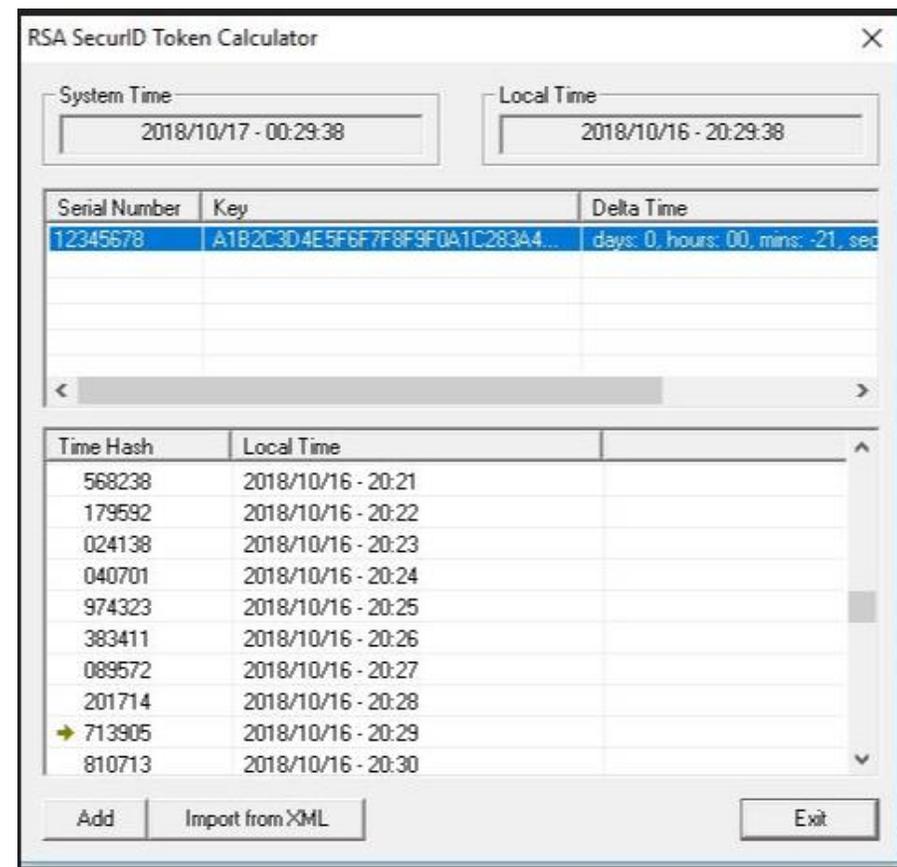Taken from Cain & Abel hacking tool

MFA Hacks

Duplicate Code Generator

- Shared secret will always be present in at least two places (e.g. source database/verifier and device itself)

- Attackers that learn seed/shared secret and algorithm can generate duplicate/identical code generators that match the victim's code generator

Real-Life Example: Chinese APT, RSA, and Lockheed Martin attack

Duplicate Code Generator

- When you first use Google Authenticator, you will usually be sent a QR code

- It may or may not expire

- That QR code has all the token secrets necessary to create the same Google Authenticator instance

- I can install on multiple devices at the same time (hacker's love this)

Google Authenticator

Please scan the barcode below:

Google Authenticator

730 989
OneLogin (onelogin)
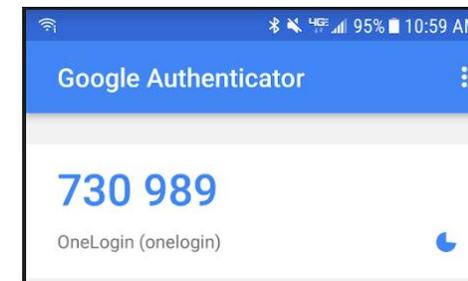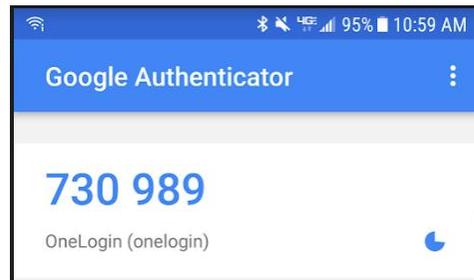
MFA Hacks

Duplicate Code Generator

/r/coinbase   COMMENTS

Welcome to Reddit,
the front page of the internet.

BECOME A REDDITOR   and join one of thousands of communities.

low:

↑
9
↓

2-Factor can be hacked, apparently self.CoinBase
Submitted 2 years ago * by Parsloe-Parsloe

EDIT: Mystery (probably solved): I am now 95% certain as to how 2FA was bypassed, and the answer is fairly obvious: when I set up the Google Authenticator for 2FA, I left a copy of the Key in my email. Anyone reading this is probably shaking their head... rightly so. The moral of the story is an obvious one: sign up for 2FA, and destroy the key used to set it up, if you don't, it's worse than useless. Leave a trace of the key, and the 2FA serves only as a dangerous false sense of security. As someone pointed out in the comments our security measures are only as strong as the weakest link. Thoroughness is crucial.

Google Authenticator

730 989

OneLogin (onelogin)

95% ▮ 10:59 AM
Google Authenticator

730 989

OneLogin (onelogin)
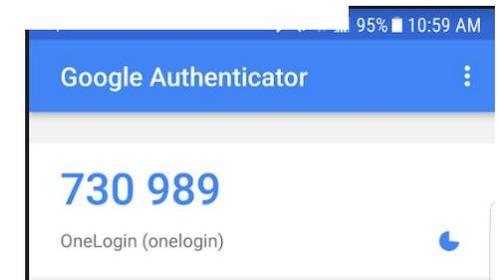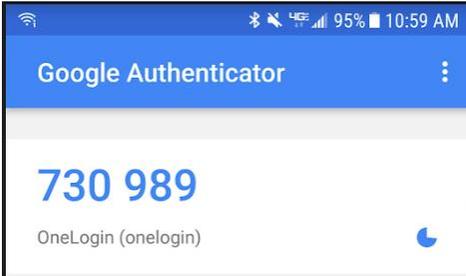
MFA Hacks

Duplicate Code Generator

Google Authenticator

730 989
OneLogin (onelogin)

- Google Authenticator uses an 80-bit secret key

- Not that hard to hack

- US gov't says a min. of 128-bit key is required for any TOTP

- I guess it's only a problem if someone knows the Google Authenticator algorithm

- Yeah, turns out, someone does

Google Authenticator
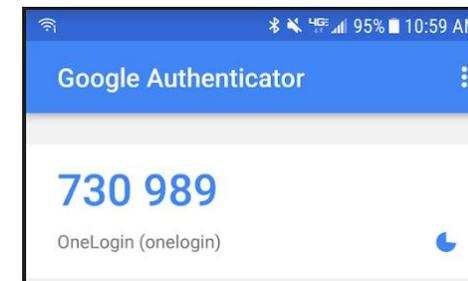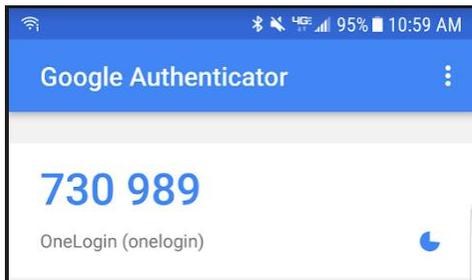
Please scan the barcode below:

Google Authenticator

730 989
OneLogin (onelogin)

Duplicate Code Generator


```
authenticator := GoogleAuthenticator new.

authenticator base32Secret: 'HXDMVJECJJWSRB3HWIZR4IFUGFTMXBOZ'.

authenticator nextPadded. "'672812'"
```

Playground
Page

enticator

the barcode below:

Inspector on a GoogleAuthenticator

a GoogleAuthenticator

Raw Meta

Variable	Value
self	a GoogleAuthenticator
codeLength	6
hashMode	SHA1
period	30

Google Authenticator

730 989

OneLogin (onelogin)

ogle Authenticator

80 989

login (onelogin)

MFA Hacks

Not Required/ Downgrade Attacks

- If you still have a 1FA solution for a site or service, and it can still be used, then it's like you don't really have MFA

- Many sites and services that allow MFA, don't require it

- If your MFA comes with a non-MFA "master key" or code, then that code can be stolen

- Which means attacker can use non-MFA credential to access

- May allow both more secure and less secure MFA methods, but you likely can't force only one method

MFA Hacks

- ALL logon recovery methods are far less secure than MFA

- Can bypass many MFA requirements by answering much less secure password reset answers

- Attackers can spoof your registered recovery phone number and automatically be authenticate to some services/voicemail systems

Account recovery options

If you forget your password or cannot access your account, we will use this information to help you get back in.

Recovery email   roger@⬛⬛⬛⬛   >

Recovery phone   (⬛)⬛⬛⬛   >

Microsoft account

Security code

Please use the following security code for the Microsoft account ro*****@hotmail.com.

Security code: **0152772**

If you don't recognize the Microsoft account ro*****@hotmail.com, you can click here to remove your email address from that account.

Thanks,
The Microsoft account team

MFA Hacks

Not Required/ Recovery Questions

The worst recovery method on the planet is password recovery questions

- Usually REQUIRED by many web sites, you can't create a new account without them

MFA Hacks

Not Required/ Recovery Questions

<u>Problem:</u> Answers can often be easily guessed by hackers

- Great Google paper called *Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google*

  - http://www.a51.nl/sites/default/files/pdf/43783.pdf

  - For example, some recovery questions can be guessed on first try 20% of the time

  - 40% of people were unable to successfully recall their own recovery answers

  - 16% of answers could be found in person's social media profile

- Attack has been involved in many well known attacks (e.g. Sarah Palin's compromised email)

MFA Hacks

Not Required/ Recovery Questions

Solution: Never answer the questions with the real answers!

Unfortunate that means you have to record them somewhere else just like passwords (password managers help with this)

MFA Hacks

Reuse Stolen Biometrics

- If your biometric identity is stolen, how do you stop a bad guy from re-using it?

- Once stolen, it's compromised for your life

- You can change a password or smartcard, you can't easily change your retina scan or fingerprint

- Known as non-repudiation attack in the crypto world

- Attacker might even steal your biometric attribute (e.g. finger/hand) to reuse

- But more likely to steal in digital form and replay

Example: June 2015 OPM attack stole biometrics of 5.6 million people

MFA Hacks

Reuse Stolen Biometrics

Another example:

- Aug. 2019 breach

- Biostar2 platform

- Fingerprints and facial recog

- Top 50 biometric app vendor

- Over 1 million fingerprints breached

- The breachers claim company was largely unresponsive and uncooperative to their reports and ongoing discussions

Report: Data Breach in Biometric Security Platform Affecting Millions of Users

Biostar 2 Breach: Millions of Users Exposed in Huge Data Leak

vpnMentor

MFA Hacks

Brute Force

- If the MFA auth screen doesn't include ~~account lockouts for x~~

Takashi (kamikaze)
338 Reputation | - Rank | 1.63 Signal | 73rd Percentile | 10.36 Impact | 76th Percentile

21 #121696 **Bypass two-factor authentication** Share:

State   ● Resolved (Closed)   Severity   No Rating (---)
Disclosed publicly   November 18, 2017 7:00am -0500   Participants
Reported To   Slack   Visibility   Public (Full)
Weakness   Improper Authentication - Generic

Researcher Bypasses Instagram 2FA to Hack Any Account

Mar 9th (2 years ago)

...s" because your bug

The recovery mechanism does have a rate-limiting protection – i.e., the number of log-in attempts within a set amount of time from any one IP address is restricted. In Muthiyah's first attempt, he sent around 1,000 requests, but only 250 of them went through. However, he also discovered that Instagram doesn't blacklist IP addresses that have exceeded the number of allowed attempts for a certain time period, so he could toggle between IP addresses in order to perform a continuous attack.

...can enter wrong 2FA codes. I didn't use any automated tools

...imes manually. It seems that a user can brute force 2FA codes.

- Happens all the time

2. Go to "Password Reset" page from #1's message.

3. Set a new password and Brute force two-factor auth code

CVE-2018-11082: UAA MFA doesn't prevent brute force of MFA code

#202425   Two-factor authentication bypass on Grab Android App

MFA Hacks

Buggy MFA

- Bugs are bugs, some bypass MFA

After ignoring for months, Uber fixes two-factor bypass bug after all

"There is no need for a novelty 2FA if it doesn't actually serve a purpose."

By Zack Whittaker for Zero Day | January 21, 2018 -- 14:26 GMT (06:26 PST) | Topic: Security

Bypass Code | Duo Security
https://duo.com/product/trusted-users/two-factor-authentication/.../bypass-codes ▼
The use of **bypass** codes is one of many **two-factor authentication** methods that Duo supports to ensure Trusted Users, part of a complete Trusted Access ...

How to Bypass PayPal Two Factor Authentication - Ivanti
https://www.ivanti.com/blog/bypass-paypal-two-factor-authentication/ ▼
Mar 8, 2018 - That's the concern raised by security researchers who uncovered a method of **bypassing** PayPal's **two-factor authentication** (2FA), the ...

Breaking Apple iCloud: Reset Password and Bypass Two-Factor ...
https://blog.elcomsoft.com/.../breaking-apple-icloud-reset-password-and-bypass-two-f... ▼
Nov 28, 2017 - Who am I to tell you to use **two-factor authentication** on all accounts that support it? This recommendation coming from someone whose ...

How to Bypass Two-Factor Authentication - One Step at a Time - Black ...
https://www.blackhillsinfosec.com/bypass-two-factor-authentication-one-step-time/ ▼
Feb 21, 2017 - How to **Bypass Two-Factor Authentication** – One Step at a Time ... as you might have guessed, a time-sensitive token provided by **2FA**.

Bypass 2FA, account lock and change password on staging.login.gov ...
https://www.youtube.com/watch?v=WkWRjkHrGWM
Nov 14, 2017 - Uploaded by Mustafa Kemal Can
Bypass **2FA, bypass** account lock and change password on staging.login.gov You can read more details on ...
▶ 3:17

Buggy MFA

2017 ROCA vulnerability

- Sometimes a single bug impacts hundreds of millions of otherwise unrelated MFA devices

- Huge bug making any MFA product (smartcards, TPM chips, Yubikeys, etc.) with Infineon-generated RSA key lengths of 2048 or smaller (which is most of them), easy to extract the PRIVATE key from public key.

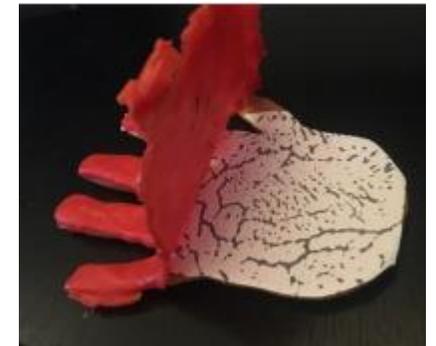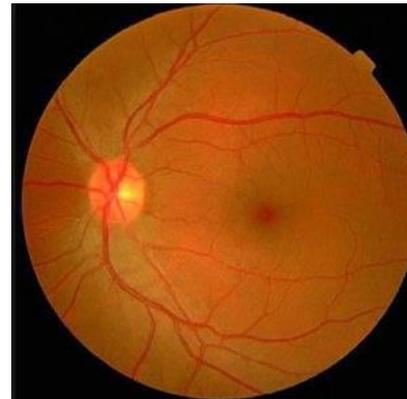- Still tens to hundreds of millions of devices impacted

Physical Attacks

Biometric

- Fake fingerprints, fake faces, etc.

    - Biometric vendors try to prevent fakes, but hackers just get around

- Stolen and replayed

MFA Hacks

Physical Attacks

Biometric – Fake Faces

- Pictures

- 3D Masks

- Photoshopped blinking eyelids in animated gifs

Facial recognition doesn't work as intended on 42 of 110 tested smartphones

Devices from Asus, BlackBerry, Huawei, Lenovo, LG, Nokia, Samsung, Sony, and Xiaomi failed a basic "photo test."

By Catalin Cimpanu for Zero Day | January 5, 2019 -- 13:49 GMT (05:49 PST) | Topic: Security

Physical Attacks

TPM Attacks

- Electron microscope can find private key on TPM chips

- Regular, computer cleaning canned air can be used to "freeze" regular RAM memory chips, so that private keys can be extracted

    - Bypasses all disk encryption products

Defending Against MFA Attacks

Defending Against MFA Attacks

Defenses

Social Defenses

- Education – for admins and end-users

- Realize nothing is unhackable

- Include MFA hacking awareness into your security awareness training

  - Share this slide deck with co-workers and mgmt.

- Don't get tricked into clicking on rogue links

- Block rogue links as much as possible

- Make sure URL is legitimate

Defending Against MFA Attacks

Defenses

Technical Defenses

- Enable REQUIRED MFA whenever possible

- Don't use SMS-based MFA whenever possible

- Use "1:1" MFA solutions, which require client-side to be pre-registered with server

- Use/require 2-way, mutual, authentication whenever possible

  - Ex. FIDO U2F's Channel or Token Binding

- Does your MFA solution specifically fight session token theft and/or malicious replays (i.e. replay resistant)

- Can your MFA vendor's support help be socially engineered?

- Make sure MFA vendors use secure development lifecycle (SDL) in their programming

- Make sure MFA has "bad attempt throttling" or "account lockout" enabled

Defending Against MFA Attacks

Defenses

Technical Defenses (con't)

- Spread factors across different "channels" or "bands" (in-band/out-band)

- Protect and audit identity attributes used by MFA for unique identification of MFA logons

- Don't answer password reset questions using the honest answers.

- Encourage and use sites and services to use dynamic authentication, where additional factors are requested for higher risk circumstances

- Understand the risks of "shared secret" systems

- For transaction-based authentication, need to send user all critical details out-of-band before confirmation is transmitted/required

Key Takeaways

Lessons

- MFA isn't unhackable

- MFA does not prevent phishing or social engineering from being successful

- MFA is good. Everyone should use it when they can, but it isn't unbreakable

- If you use or consider going to MFA, security awareness training has still got to be a big part of your overall security defense

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com