

Eleven Ways to Defeat Two-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, 2FA since 1998
- Consultant to world's largest and smallest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 10 books and over 1000 magazine articles
- InfoWorld and CSO weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certifications passed include:

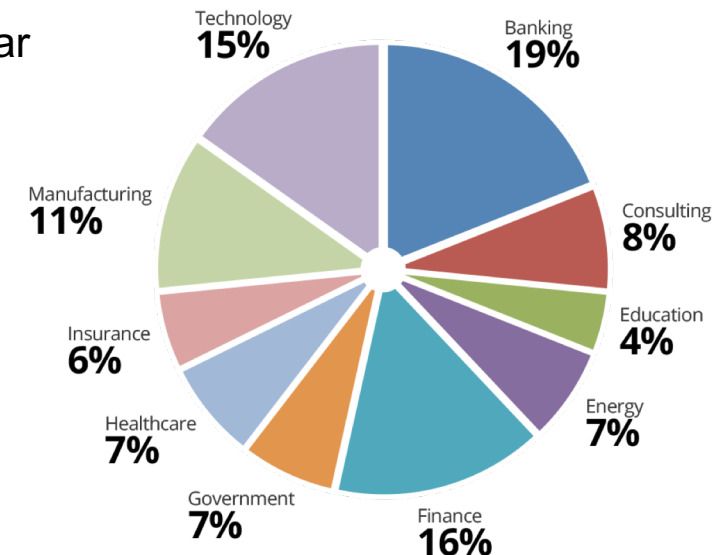
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Over
17,000
Customers

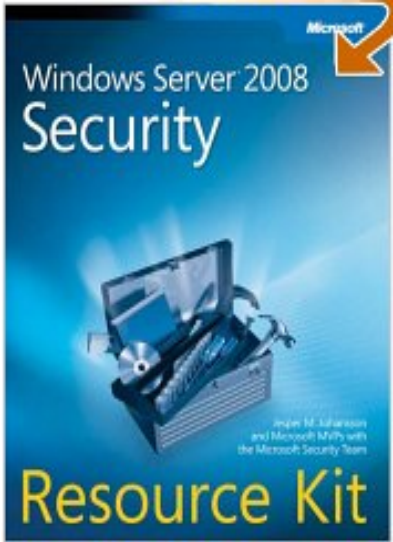
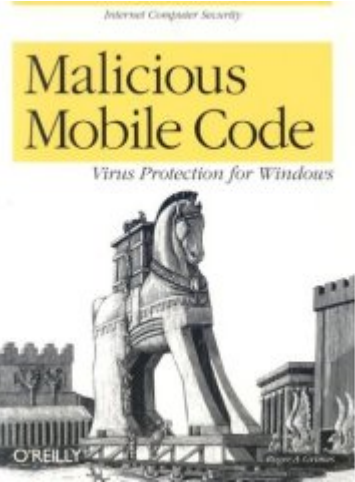
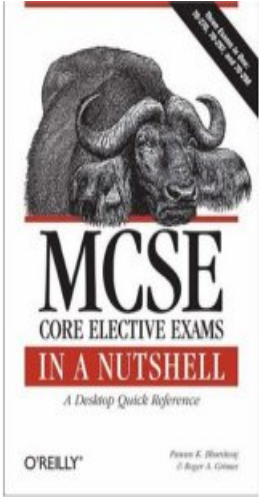
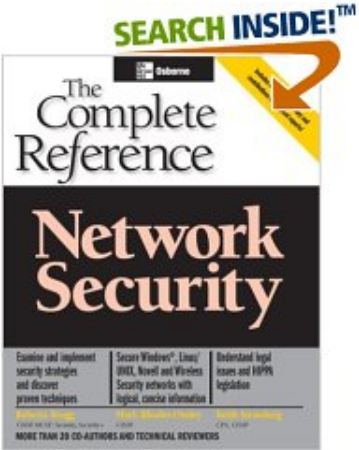
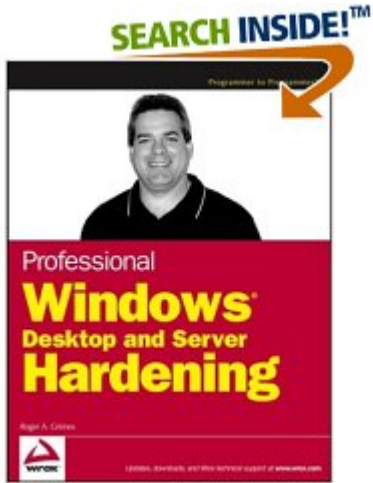
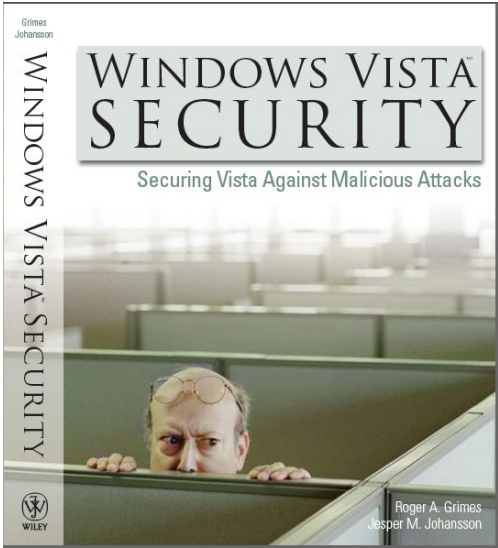
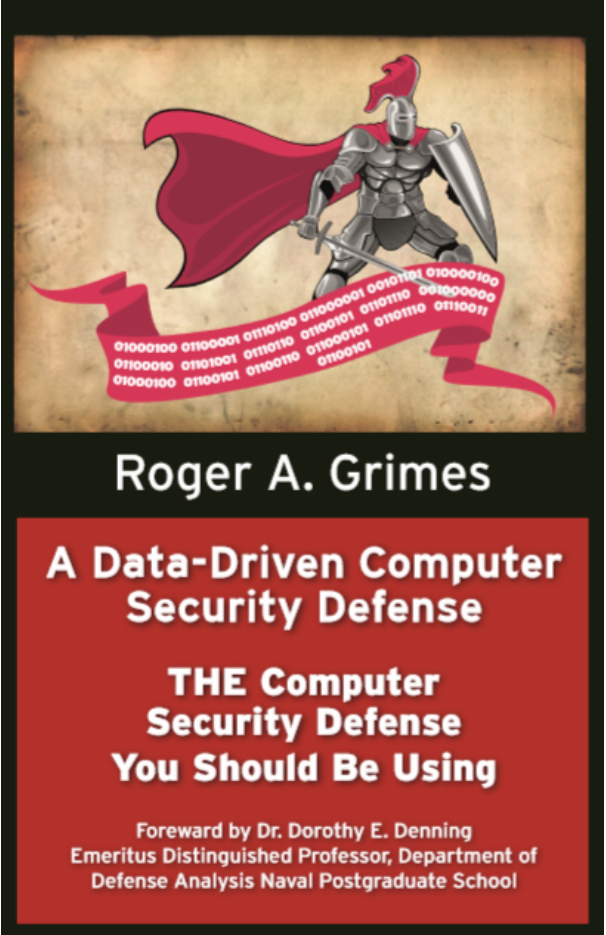
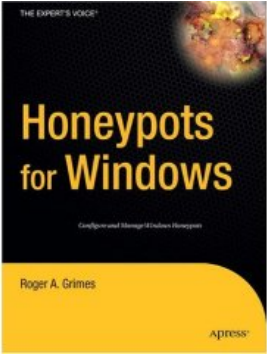
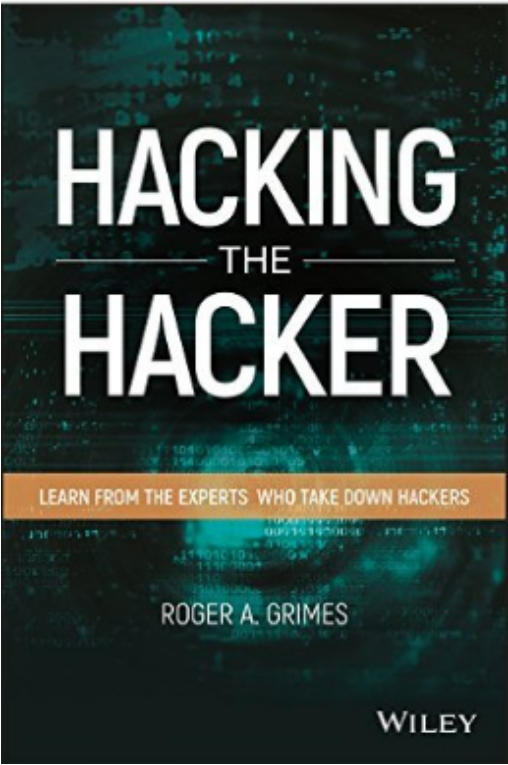
Inc.
500

About Us

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer
- 200% growth year over year
- We help thousands of organizations manage the problem of social engineering



Roger's Books



Today's Presentation

- Two-Factor Authentication Intro
- Hacking 2FA
- Defending Against 2FA Attacks

Two-Factor Authentication Intro

Factors

Introduction to Two-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

Factors

Introduction to Two-Factor Authentication

- Single Factor
- Two Factor (2FA)
 - 1.5 factor (slang for soft token vs. hard token)
- Multi-Factor
 - 2-3 factors
- Two or more of the same factor isn't multi-factor
- Must be different types of factors to provide additional protection

Factors

Introduction to Two-Factor Authentication

- All things considered, 2FA is better than 1FA
- We all should strive to use 2FA wherever and whenever possible
- But 2FA isn't unhackable
 - More on this later

We need to understand some basic concepts to better understand hacking 2FA

Auth vs. Auth

Introduction to Two-Factor Authentication

- Identity
 - Unique label within a common namespace
 - indicates a specific account/subject/user/device/group/service/daemon, etc.
- Authentication
 - Process of providing one or more factors that only the subject knows, thus proving ownership and control of the identity
- Authorization
 - Process of comparing the now authenticated subject's access (token) against previously permissioned/secured resources to determine subject access

Auth vs. Auth

Introduction to Two-Factor Authentication

Hugely Important Point to Understand

- No matter how I authenticate (e.g. one-factor, two-factor, biometrics, etc.), rarely does the authorization use the same authentication token
 - They are completely different processes, often not linked at all to each other
 - Many 2FA hacks are based on this delineation

For example

- Even if I authenticate to Microsoft Windows using biometrics or a smartcard, after I successfully authenticate, an LM, NTLM, or Kerberos token is used for authorization/access control
- No matter how I authenticate to a web site, the authorization token is likely to be a text-based cookie (e.g. session token)

Auth vs. Auth

Introduction to Two-Factor Authentication

1-way vs. 2-way

Authentication can be:

- One-way
 - server-only or client-only
 - Most common type
 - Vast majority of web sites use one-way authentication, where server has to prove its identity to client before client will conduct business with it
- Two-way (mutual)
 - Both server and client must authenticate to each other
 - Not as common, but more secure
 - Two-way may use different auth methods and/or factors for each side

Hacking 2FA

Session Hijacking

2FA Hacks

- 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

Session Hijacking

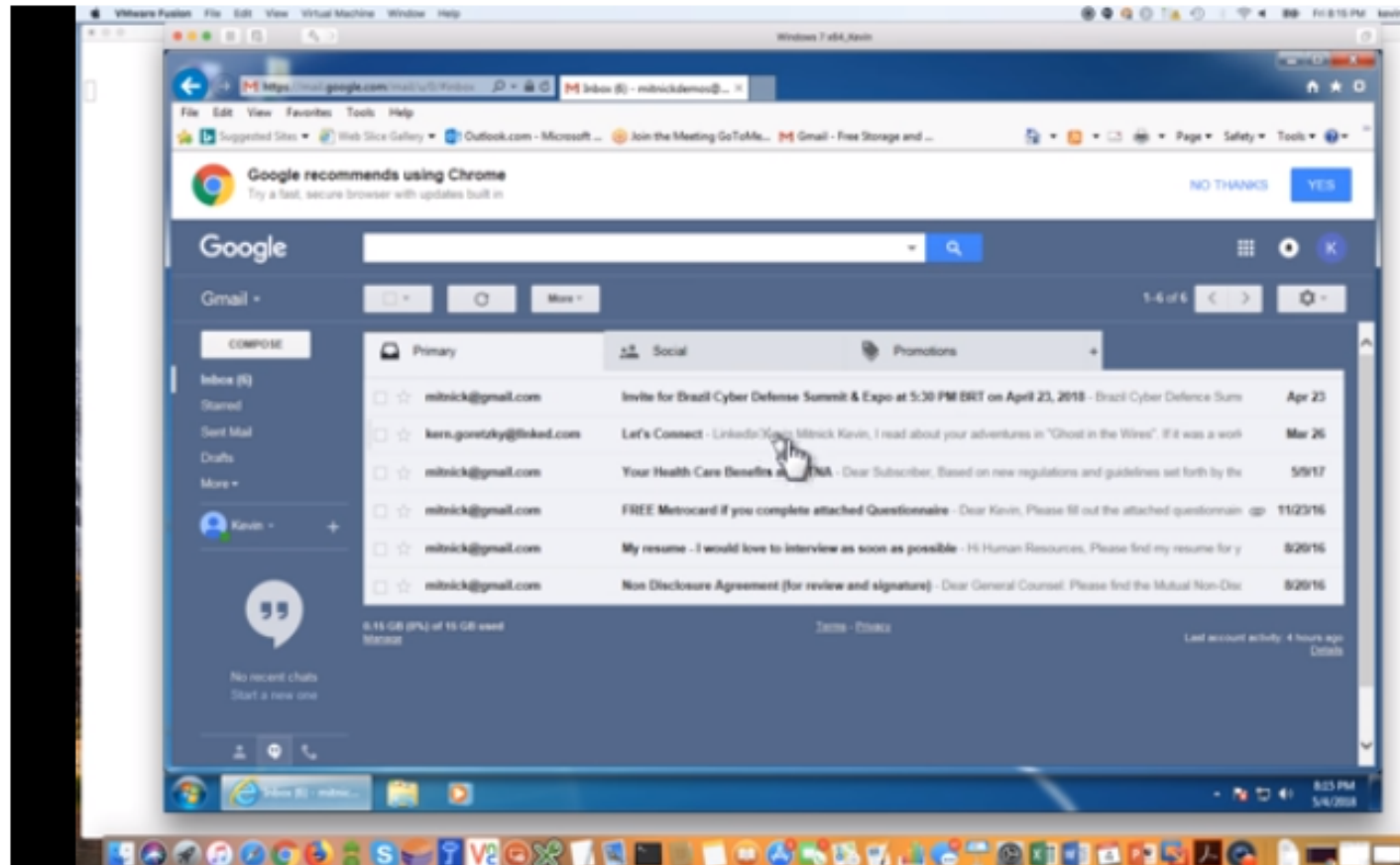
2FA Hacks

- Session Hijacking has been around since computers have been networked
 - ARP spoofing, cookie stealing, URL tampering, etc.
- Bancos trojans did it in the early 2000's
- Firesheep made it super popular and easy in 2010
- Defense against web-based session hijacking was for vendors to use unpredictable cookie contents and to use HTTPS (SSL/TLS)
 - Hackers got around
- Better defense was to use 2FA
 - Hackers got around

2FA Hacks

Kevin Mitnick Hack Demo

Session Hijacking



2FA Hacks

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 2FA is involved

2FA Hacks

Man-in-the-Endpoint Attacks

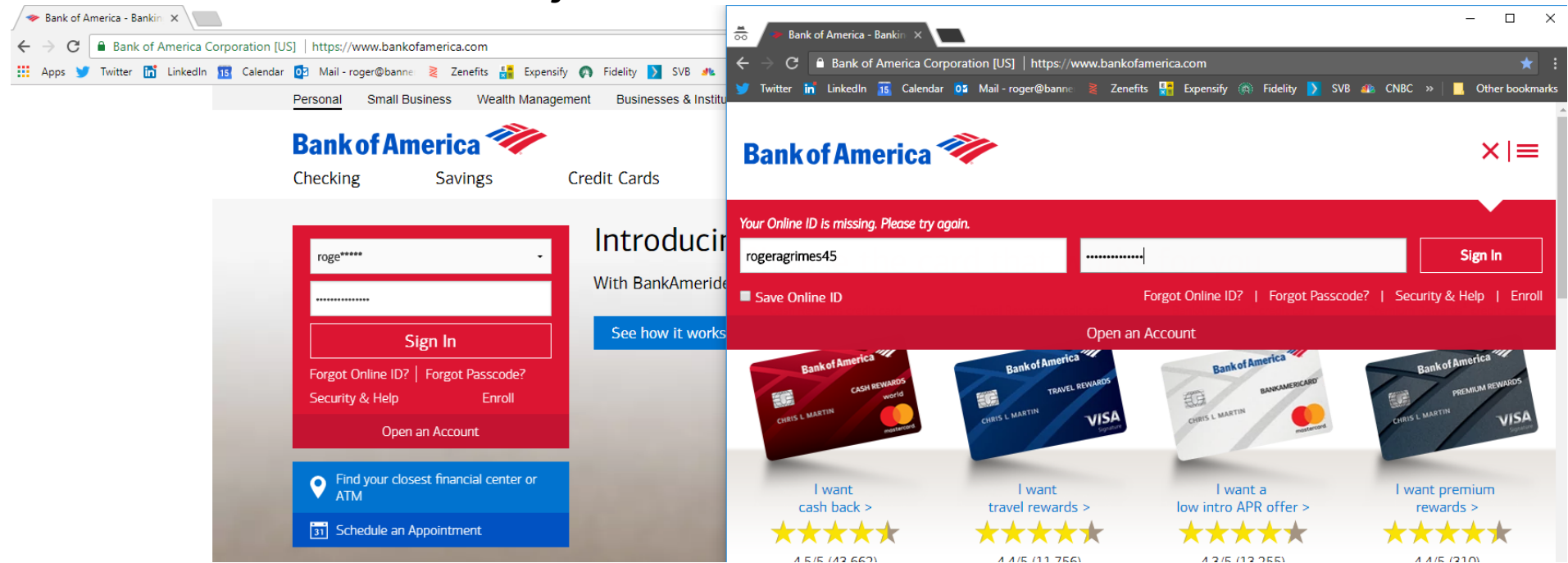
- If endpoint gets compromised, 2FA isn't going to help you
- Attacker can just do everything they want that the user is allowed to do after successful authentication
- Steal session cookies
- Attacker can modify 2FA software to even steal 2FA secrets
 - Smartcards and rogue CSPs

Endpoint Attacks

2FA Hacks

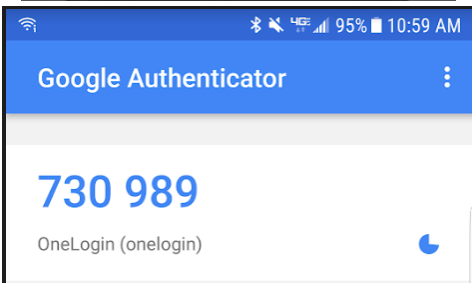
Man-in-the-Endpoint Attacks

- Start up a second session that the user isn't even aware
- Ex. Bancos trojans



2FA Hacks

Duplicate Code Generator



- Most “random” number generators start with a randomly generated “seed” value, which is used to generate the first value
 - May also use current time and a unique identifier so that randomly generated number is unique for that device and time
- Algorithm then uses first value to generate all subsequent values
- Attackers that learn seed number 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

Not Required/ Downgrade Attacks

2FA Hacks

- 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 2FA
- Many sites and services that allow 2FA, don't require it
- Which means attacker can use non-2FA credential to access
- Facebook/LinkedIn/Twitter will allow you to use 2FA to authentication, but doesn't require it, which means attacker can use some other lesser auth method
 - Can bypass many 2FA requirements by answer much less secure password reset answers

2FA Hacks

- There have been many real-world instances where the user had 2FA 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

2FA Hacks

- “Hi, I lost my 2FA token or it is broken, what can I do to get a new one?”
- “Hi, my laptop crashed and I had to reinstall Google Authenticator. Can you resend me a new QR code to my temporary email address so I can access my corp email?”

Subject Hijack

2FA Hacks

- Every 2FA token or product is uniquely tied to a subject that is supposed to be using the 2FA device/software
- If the hacker can take over the subject's identity within the same namespace, they can reuse the stolen identity with another 2FA token/software
- And system will allow a completely unrelated 2FA token/software to authenticate and track the fake user as the real user across the system
- Examples:
 - Email hijacking
 - Smartcard/Active Directory hijacking

2FA Hacks

Subject Hijack

Example attack – Hijacking smartcard authentication

Bad guy:

1. Obtains control over Subject2's smartcard
2. Changes target Subject1's UPN in Active Directory (AD) to anything else
3. Change's Subject2's UPN in AD to Subject1's UPN
4. Logs into AD using Subject2's smartcard, using Subject2's legitimate smartcard and/or PIN
5. System authenticates and tracks Subject2 as Subject1
6. Bad guy, as Subject2, performs malicious actions
7. System tracks all actions as Subject1
8. When bad guy is finished, they logout and switch UPN's back. No one knows the difference

2FA 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

Hijacking Shared Auth


2FA Hacks

- It's very possible for shared authentication schemes, like oAuth, to have session tokens stolen and reused
- When you successfully authenticate to one web site that supports integrate auth, you are essentially allowing hacker into any other web site that supports the same integrated auth method for your identity
- So even if the next web site requires 2FA, the integrated auth will usually seamlessly authenticate the person, bypassing the 2FA, using the previous shared master session token









Brute Force



- If the 2FA auth screen doesn't include account lockouts for x number of bad attempts, hackers can brute force their way into it
- Happens all the time


2FA Hacks

 **Takashi (kamikaze)**

338 Reputation | - Rank | 1.63 Signal | 73rd Percentile | 10.36 Impact | 76th Percentile

 21  **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**

Bounty **\$500** Collapse

TIMELINE

 **kamikaze** submitted a report to **Slack**. Mar 9th (2 years ago)

If a user set 2FA, a user has to enter verification code when a user tries to reset password.

Under the "Password Reset" page, a user can enter wrong two-factor authentication code many times. I said "many times" because your bug bounty policy stated...

Exclusions

Issues found through automated testing

So, I may not be allowed to brute force in order to check how many times a user can enter wrong 2FA codes. I didn't use any automated tools and didn't brute force for my testing.

I tested that I could still reset my password after I entered wrong 2FA codes 20 times manually. It seems that a user can brute force 2FA codes.

-----step to reproduce-----

1. A user sends a password reset message to user's registered email.
2. Go to "Password Reset" page from #1's message.
3. Set a new password and Brute force two-factor auth code

After a user reset password, a user will go to slack's home page. From that page a user can do anything.

2FA Hacks

- Bugs are bugs, some bypass 2FA

Buggy 2FA

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 ...



2FA Hacks



2017 ROCA vulnerability

- Sometimes a single bug impacts hundreds of millions of otherwise unrelated 2FA devices
- Huge bug making any 2FA 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

Buggy 2FA

2FA Hacks

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 2FA Attacks

Defenses

Defending Against 2FA Attacks

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

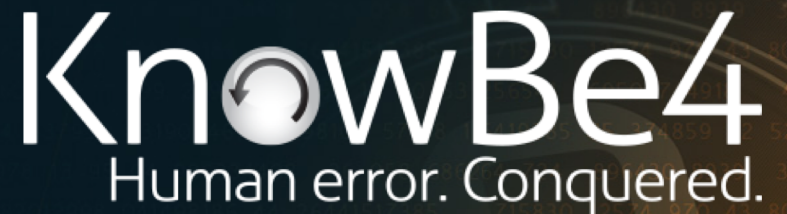
Defenses

Defending Against 2FA Attacks

- Make sure 2FA vendors use secure development lifecycle (SDL) in their programming
- Protect and audit identity attributes used by 2FA for unique identification of 2FA 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

Key Takeaways

- 2FA isn't an unhackable security panacea
- 2FA does not prevent phishing or social engineering from being successful
- 2FA is good. Everyone should use it when they can, but it isn't unbreakable
- If you use or consider going to 2FA, security awareness training has still got to be a big part of your overall security defense



» Learn More at «
www.KnowBe4.com/Resources

Resources



Free Phishing Security Test

Find out what percentage of your users are Phish-prone



Free Domain Spoof Test

Find out now if hackers can spoof an email address of your own domain.

Questions?

KnowBe4
Human error. Conquered.

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

Thank You!

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

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)

KnowBe4
Human error. Conquered.

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