The Gentle Art of Password Management

David Trepp, M.S.
Partner, IT Assurance

Housekeeping

- Questions and Comments
  - Please have your microphone muted when you are not speaking to the group
  - Feel free to send a chat message or unmute & speak up when you have a question

- CPE Credit Rules
  - You will need to listen for & write down **3 code words** throughout the class in order to receive CPE credits for the one hour of training; the code words will be **bold, underlined, in red font**
  - At about five minutes before the end of the class, you will receive a survey from Survey Monkey
  - You will need to type in each of the code words & submit the survey in order to receive CPE
  - The expectation is that you complete the survey as soon as you receive it. We will only leave the survey open until half an hour after the class ends, & CPE will not be granted after this time

Password Expertise

- BPM InfoSec assessment team personnel **are not** experts at planning, building, or managing information security controls
  - We are not here to endorse or sell any password solutions

- BPM InfoSec assessment team personnel **are** experts at compromising information security controls
  - We are ethical hackers who've performed over 1,200 comprehensive penetration tests
  - We defeat passwords for a living

- This introductory presentation will provide a hacker's perspective on:
  - The Password Problem & What Makes A Password Strong
  - Defeating Password Controls
  - Practical Password Strategies

The Password Problem
&
What Makes A Password Strong

The Password Problem

“Password management continues to challenge even the most sophisticated IT security organizations. Nearly three-quarters (72%) of engagements resulted in at least one compromised password…”

- Rapid7 Under the Hoodie 2019

“81% of hacking related breaches leveraged either stolen &/or weak passwords”

- 2018 Verizon Data Breach Investigations Report

Password Requirements Are Painful

- Security & ease-of-use seem diametrically opposed when password change & strength requirements are instituted
  - Long, complex passwords can be hard to remember, store, & type
  - Users must remember generations of passwords, which may actually *weaken* the organization’s security posture
    - Write down the most recent password on a sticky note or store it in an unprotected Word or Excel file
    - Use easy to guess passwords
      - P@ssw0rd#
      - Summer2019!

Password Strength, What Really Matters…

- ***…To Users:***
  - Must be easy to remember
  - Must be easy to create generations of credentials
  - Must be easy to type
- ***…To Support Personnel:***
  - Must be easy to administer, i.e.
  - Create few support calls
- ***…To Security Administrators:***
  - Must be secure
  - Long
  - Hard to guess
  - Well-encrypted, both at rest & in transit

Passphrases can meet most of these criteria

Passphrases Make Everyone Happy

Consider the following passphrase:

I l0ve to eat chocolate.

- It's easy to recall
  - There is only one numerical **substitution** to remember
  - Substitutions can follow a pattern, e.g. replace first o with 0
- It's easy to create generations of distinct, yet related, passphrases
  - *I enj0y berries in spring.*
  - *Iced tea f0r me in summer.*
- It's easy to type
  - There is no need to hit the shift key a bunch of times or hunt and peck around on the number pad
    - It's just a normal sentence with one patterned substitution

Ease of use results in happy end users & fewer support calls

The Not-So-Gentle Math of Passwords

Again, consider the passphrase:

I l0ve to eat chocolate.

- Consists of 24 characters (#'s, letters, etc.)

- On a typical PC keyboard there are 94 characters
    - A one-character long password requires up to 94 guesses
    - A 2-character long password requires up to 94 guesses for the first character, and another 94 for the second or 94^2 (94 x 94 = 8,836)

Every character added to the length of a password makes it exponentially stronger!

Our passphrase has *94^{24} or 2×10^{47} (which is 2 followed by 47 zeroes!)* possible combinations of characters

- At a typical offline attack rate of 8×10^{11} guesses per second (800 billion) this passphrase, if well-encrypted, will require **up to 9 x 10^{27} years** to brute force
    - For reference: the estimated age of the universe is 1.3×10^{10} years

Even Complex 8-Character Passwords Don’t Make Security Administrators Happy

Now, consider the following 8-character password:

1Ns@n3Pw
(Insane Password)

- It contains 8 characters:

  Hence there are: *94^{8} = 6.1×10^{15}* possible combinations of characters

- At 800 billion guesses per second this password, if well-encrypted, will require ***up to* 2.1 hours** to brute force
  - And, if it’s weakly hashed/encrypted, it will crack in a matter of seconds

Which Is Better?

I l0ve to eat chocolate.

- Easy to remember with a simple substitution pattern
- Meets complexity requirements
- Surprisingly easy to type
- Easy to create generations of passphrases that share a single motif
  - Sequences of events e.g. directions or instructions
  - Food references
  - Sports or hobby references
  - Get creative
- If well encrypted, *<u>requires an astronomical number of years to brute force</u>*

OR

1Ns@n3Pw

- Hard to remember substitutions & caps choices
- Requires lots of on & off of the shift key to type
- Hard to include in a series of distinct passwords that share a single motif
- If well encrypted, *<u>requires 2.1 hours to brute force</u>*

What’s Even Better Than a Passphrase?

A long, randomly generated string of characters

- Generated by a password management application
  - KeePass
  - RoboForm
  - LastPass, etc.
- No more need to remember anything
  - Except one’s password manager passphrase
- Supports unique, strong credentials for all applications
  - Can use Web URL for easy username and password copy/paste
- Encrypts stored credentials
- Allows for multi-factor authentication
  - Password + keyfile residing on computer
  - Password + one-time passcode to phone or fob

What’s Even Better Than a Random String of Characters?

A strong password plus Multi Factor Authentication (MFA)

- MFA combines something one ***knows***, e.g. username + password
  - Something one ***is*** and/or
  - Something one ***possesses***

  - Tokens, encryption keys, or smartphones (something one possesses)
    - Synchronous: follows a clock in synch with the application server
    - Asynchronous: server sends PIN & PIN is then entered by user
    - Static: usually a mag swipe, RFID card, or key, e.g. YubiKey adds convenience for people logging in repeatedly
    - Apps like KeePass, LastPass, & RoboForm can require key file

  - Additional biometric authentication (something one is)
    - Scans: fingerprint, face, retina, iris, palm or overall hand geometry
    - Patterns: Heart/pulse, voice, signature or keystroke
    - Pictures/Facial Recognition: e.g. iPhone, selfies at Amazon & MasterCard

Defeating Password Controls

Where Passwords Reside

MORE OBVIOUS

- PW vaults
- Word & Excel files
- Sticky notes
- Browsers
- Email inboxes
- Vendor defaults
- Unauthenticated application access
- People's heads

LESS OBVIOUS

- Moving across the wire
- .ini files
- Web.config files
- LSASS memory process
- Hard **coded** in applications
- Hashes & tickets
- Group Policy XML files (weak AES)
- People's retinas, fingertips, etc.

How Attackers Capture Credentials

- Find
- Intercept
- Guess
- Crack
- Bypass
- Ask
- Spoof

Defeating MFA

- Fail-Open vs. Fail-Secure
  - What if the Fob or phone is lost, stolen, or broken?
  - What if the computer is not attached to the enterprise network?
- Spoof
  - Pass-The-Ticket
  - Cell Towers, e.g. IMSI catchers like Stingray
- Ability to change receiving device phone # or SIMM
  - See headlines on calls to cell provider help desks
- MiTM attacks
  - SS7, the SMS protocol, is trivially easy to spoof
    - 8/3/2016 NIST SP800-63B Digital Authentication Guideline (Draft) "[Out of band verification] using SMS is deprecated, & will no longer be allowed in future releases of this guidance."
  - Online Banking man-in-the-browser attacks
    - Watch for online banking activities & intercept credentials
    - Xbot for Android steals SMS messages before they hit the device
- Find Matrices, daily codes & other MFA data
  - Email inboxes
- Ask the user!

Defeating Biometric Authentication

- Sensitivity Settings
  - Type I Error: false negative - reject valid user (FRR)
    - Lots of helpdesk calls
  - Type II Error: false positive - accept invalid user (FAR)
    - Security weakness
- Fail-Open vs. Fail-Secure
  - What if the reader is broken?
  - What if the biometric component scanned has been scarred?
- Man-in-The-Middle Attacks
- Ability to Create High Resolution Facsimiles
  - Hi-res cameras, e.g. Japan's Nat'l. Inst. of Informatics fingerprint demo
  - Play-Doh, e.g. Germany's Chaos Computer Club fingerprint demo
  - Hi-Res printers, photocopiers, & voice recorders
  - 3D printers, e.g. fake contact lens generated from hi-res photo
- Impact Consideration: Biometric Credentials Are Forever!
  - One's fingerprints or retinal pattern do not change every 90 days, so consider the impact of a stolen biometric credential database

Practical Password Strategies

Password Construction Do's & Don'ts

- Password Do's
  - Make it 15 characters or longer
    - use passphrases or password application random strings
  - Change it frequently, the more critical, the more frequently
    - PCI requires every 90 days
  - If you really want to **annoy** hackers, add a blank space at the end
  - An odd number of characters is more secure (against dictionary attacks)
- Password Don'ts
  - Make it fewer than 12 characters long
  - Use dictionary words
  - Use variations on "Password"
  - Date/Season-related
  - Double words
  - Common phrases
    - Ad slogans
    - Song lyrics

More Practical Password Strategies

- Encrypt password storage at the disk & file levels
  - Use a password management application, e.g. LastPass, KeePass, Yubikey
    - Secure access to your password manager application
      - Long passphrase
      - Use MFA, e.g. keyfile &/or one-time passcode
      - Back it up
  - At the very least, passphrase protect Word & Excel files (Office 2010 or newer)
- Never re-use Windows & key application passwords
- Use MFA, wherever the vendor supports it
- Don’t send or store passwords in plaintext emails
  - Put up with the hassle of encrypted email solutions
    - Gpg4Win, S/MIME
    - Office365 message encryption
  - Use a different data transfer method

A Few Password Strategies for System Admins

- Enable SMB signing, if possible
- Disable LLMNR and NBT-NS name resolution protocols
- Disable or de-prioritize IPv6 on internal networks
- Purge old LM password hashes & secure NT hashes (or replace with Kerberos)
  - Limit time-to-live for Kerberos tickets
- Establish strict vendor default password requirements
- Change service account passwords frequently
- Search LAN shares for strings like “password,” “credentials,” & “confidential”

A Few Password Strategies for System Admins

- Migrate all SSL to TLS 1.2 or later
- Disable Windows Wdigest (Win7 & older)
- Check out Windows LAPS for local admin password management
- Do not perform authenticated vulnerability scans against unrecognized hosts
- Proactively monitor authentication logs
  - Especially for high privilege accounts
- Assign separate “admin” & “user” accounts to high-privilege users
  - & limit all user privileges in order to limit breach impact, relay, & pass-the-hash attacks

The Art of Password Management: Garnering Buy-In

- Emphasize that the organization is only as secure as its weakest password, & is faced with many threat sources, including:
  - Foreign governments (seeking command/control or disruption of services)
  - Overseas & domestic organized crime syndicates (seeking $ or commandeered hosts)
  - Competitors (seeking competitive advantage)
  - Folks with a grudge (seeking vigilante justice)
- Explain why regulatory guidance & good practices require long passwords; it's not just some IT or management scheme to make their lives miserable, i.e. we're all in this together
- Emphasize that management personnel have thought a lot about how to make this inconvenience as palatable as possible & recommend passphrases (&/or password management software):
  - Ease of recall
  - Ease of typing
  - Ease of creating generations of related phrases
- Distribute a draft password policy & ask employees for their input & ideas before finalizing
- Encourage employees to extend these strong credential habits to their private lives (but don't reuse passwords)
- Lead by example
- Thank them!

Soon, Both Passwords & Passphrases Will Be Obsolete

- Cloud computing resources will result in widespread use of increasingly fast brute force password guessing routines
- Many password guessing dictionaries, which already contain huge databases of words, have begun adding common quotations & expressions
- Cloud computing resources will result in widespread use of increasingly powerful Rainbow Tables (pre-built databases of compressed hashes &/or prime & semi-prime factors), further accelerating the cracking process
- Functional quantum computers would render most password use cases obsolete (along with all modern encryption)

A World Without Passwords?

Assume Users Will Always Construct Weak Passwords

- Fast IDentity Online (FIDO) Alliance
  - Google, Microsoft, Amazon, Intel, Visa, M/C, etc. Keyfile standard
- Google Abacus API
  - Monitors user activity, e.g. typing patterns, location data, search content, etc.
  - Combines with biometric data, e.g. voice recognition, facial recognition, fingerprints, etc.
  - Derives a “Trust Score” that, if high enough, allows the device to authenticate to an application without requiring the user to enter a password
- UC Berkley Lab’s Attempt to Identify & Authenticate via Brainwaves

CPE Credit Rules

- You will be receiving an email from Joel Segovia shortly.
- This email contains a link to the Survey Monkey survey.
- Please fill it out with all of your code words in the order they were given.
- Remember, the expectation is that you complete it right away, as the survey will close half-an-hour after the end of today’s class. No CPE will be granted after this time.

A Few Password References

- Microsoft TechNet

https://blogs.technet.microsoft.com/msftcam/2015/05/19/password-complexity-versus-password-entropy/

Password entropy = log(C)/log(2) * L
where
C = the character set (94) &
L = password length

- National Institute of Standards & Technology (NIST)

SP 800-118, Draft-*Guide to Enterprise Password Management*
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

- NIST SP 800-63-3, *Digital Authentication Guidelines*

http://www.symantec.com/connect/articles/ten-windows-password-myths

Thank you!

Questions?

Q4 webinar:
How to Avoid Becoming the Next Phish Victim

David Trepp

dtrepp@bpmcpa.com

877-328-7475