Authentication Afterlife

The dark side of making lost password recovery harder

Ewen McNeill
<ewen@naos.co.nz>

@ewenmcneill

2020-01-14 — SIP Miniconf, LCA2020

Tabletop Scenarios

https://twitter.com/badthingsdaily

Tabletop Scenario #1

There was a fire. A big fire.

It took out your main computer. And your backups.

Fortunately all your data is safe online. But you do not remember the passwords.

How do you get back in?

Administrivia

- About the speaker
  - Freelance consultant in Wellington, New Zealand through Naos Ltd
  - Works at intersection of Networking, Sysadmin, and Development
  - “Security Adjacent” for most of my career
- Questions Policy
  - Please save questions and general discussion until the end
  - Happy to discuss the topic after the presentation too
  - In person or on Twitter: @ewenmcneill
- Slides:
  `https://www.naos.co.nz/talks/authentication-afterlife/`

Tabletop Scenario #1 – Naive solution

- If you can still get email (eg, on your phone)
- Visit site, click "I forgot my password"
- Click on link in email, choose new password
- Repeat until all accounts recovered

Perils of the naive solution

Somdev Sangwan
@s0md3v

Incident: Account hacked despite having 2FA

Expectation: <some fancy technique>

Reality: Website had no 2FA on "Password Reset" mechanism and the attacker got straight in.

Sometimes bugs are too simple, hiding in plain sight.

7:45 pm · 1 Jan 2020 · Twitter for Android

440 Retweets **1.8K** Likes

https://twitter.com/s0md3v/status/1212263441500532736

Avoiding the 2FA bypass

- Require 2FA on password reset too
- User can only change one authentication factor at a time

Tabletop Scenario #2

You need to log in to an account on a new device.

All your important accounts are secured with 2FA.

Your 2FA device (phone or token) stopped working, or is not with you.

Tabletop Scenario #2 – Possible solutions

- Recovery tokens
- Alternative 2FA methods (eg, token, TOTP, and/or SMS)

Tabletop Scenario #3

Your bag was stolen. Containing your main computer, your phone, and all 2FA tokens you own.

Can the thief now impersonate you?

How do you recover access to your accounts first, and lock them out?

Tabletop Scenario #3 – Impersonation

- Do your SMS or other 2FA codes pop up on your home screen?
- That's certainly convenient...
- ... for you *and* any thief

Tabletop Scenario #3 – Impersonation

- Do your SMS or other 2FA codes pop up on your home screen?
- That's certainly convenient...
- ... for you *and* any thief

Tabletop Scenario #3 – Recovery

- Race to reset your passwords
- ... and invalidate login tokens
- Maybe you remember/can get at your passwords...
- ... but not your 2FA

Tabletop Scenario #3 – Recovery

- Race to reset your passwords
- ... and invalidate login tokens
- Maybe you remember/can get at your passwords...
- ... but not your 2FA

Tabletop Scenario #3 – Security Questions

- **“What is your mother’s maiden name?”**
- Perhaps it is... your surname?
- Or maybe it is “Raida40hv3ujee7J”
- Or was that “Raida39hv3ujee7J”
- Or maybe “nX1^L^PX0KkjIPz@aibH”

https://twitter.com/alicegoldfuss/status/1213917492768174081

Tabletop Scenario #3 – Security Questions

- “**What is your mother’s maiden name?**”
- Perhaps it is... your surname?
- Or maybe it is “Raida40hv3ujee7J”
- Or was that “Raida39hv3ujee7J”
- Or maybe “nX1^L^PX0KkjIPz@aibH”

https://twitter.com/alicegoldfuss/status/1213917492768174081

Tabletop Scenario #3 – Security Questions

- “**What is your mother’s maiden name?**”
- Perhaps it is... your surname?
- Or maybe it is “Raida40hv3ujee7J”
- Or was that “Raida39hv3ujee7J”
- Or maybe “nX1^L^PX0KkjIPz@aibH”

https://twitter.com/alicegoldfuss/status/1213917492768174081

Tabletop Scenario #3 – Security Questions

- “**What is your mother’s maiden name?**”
- Perhaps it is... your surname?
- Or maybe it is “Raida40hv3ujee7J”
- Or was that “Raida39hv3ujee7J”
- Or maybe “nX1^L^PX0KkjIPz@aibH”

https://twitter.com/alicegoldfuss/status/1213917492768174081

Tabletop Scenario #3 – Security Questions

- “**What is your mother’s maiden name?**”
- Perhaps it is... your surname?
- Or maybe it is “Raida40hv3ujee7J”
- Or was that “Raida39hv3ujee7J”
- Or maybe “nX1^L^PX0Kkj!Pz@aibH”

`https://twitter.com/alicegoldfuss/status/1213917492768174081`

Alternate Authentication Methods

- From a security point of view....
- ... you have **multiple** *alternate* authentication methods
- A primary (every day) method, and
- One or more backup authentication methods
- **But they are *all* authentication methods**

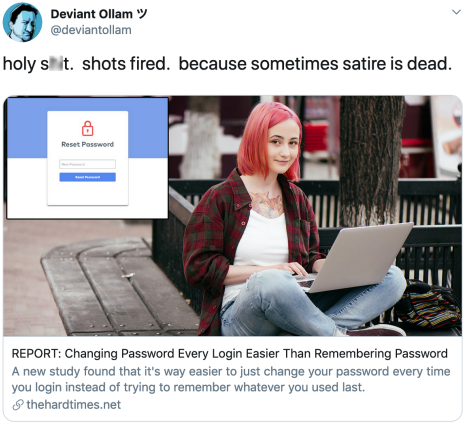
Alternate Authentication Methods

- From a security point of view....
- ... you have **multiple** *alternate* authentication methods
- A primary (every day) method, and
- One or more backup authentication methods
- But they are *all* authentication methods

Alternate Authentication Methods

- From a security point of view....
- ... you have **multiple** *alternate* authentication methods
- A primary (every day) method, and
- One or more backup authentication methods
- **But they are *all* authentication methods**

Changing Password Every Login Easier Than Remembering Password



https://twitter.com/deviantollam/status/1207161968223805440

Alternate Authentication Methods – for Attackers

- Like users, attackers will use the easiest authentication method
- Those authentication methods include "contact the helpdesk"
- And social engineering the counter staff (eg, SIM swapping)

Alternate Authentication Methods – for Attackers

- Like users, attackers will use the easiest authentication method
- Those authentication methods include “contact the helpdesk”
- And social engineering the counter staff (eg, SIM swapping)

Alternate Authentication Methods – for Attackers

- Like users, attackers will use the easiest authentication method
- Those authentication methods include “contact the helpdesk”
- And social engineering the counter staff (eg, SIM swapping)

Mat Honan (2012)

“How Apple and Amazon Security Flaws
Led to My Epic Hacking”

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Recovery with 2FA enabled

- Recovery from lost credentials with 2FA enabled will be harder
- Recovery from lost credentials with 2FA enabled **should** be harder

Recovery with 2FA enabled

- Recovery from lost credentials with 2FA enabled will be harder
- Recovery from lost credentials with 2FA enabled **should** be harder

Recovery with 2FA enabled

- Recovery from lost credentials with 2FA enabled should be harder
- Which can lead to losing your account entirely (2014): “The Dark Side of Apple’s two factor authentication”

`https://thenextweb.com/apple/2014/12/08/`

`lost-apple-id-learnt-hard-way-careful-two-factor-authentication/`

2FA recovery

- Recommended: GitHub's 2FA recovery guide:

  `https://help.github.com/en/github/authenticating-to-github/recovering-your-account-if-you-lose-your-2fa-credentials`

Tabletop Scenario #4

Your startup had a security conscious founder. They used cloud services and 2FA for everything.

After the startup got bought out, the founder left, and wiped all their devices on the way out the door.

One of the first used cloud providers threatens to delete the entire account if the new terms and conditions are not accepted, by the end of the week, by the original user account.

Tabletop Scenario #4 – Happy Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and they all live happily ever after
- Or do they?

Tabletop Scenario #4 – Happy Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and they all live happily ever after
- Or do they?

Tabletop Scenario #4 – Happy Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and they all live happily ever after
- **Or do they?**

Tabletop Scenario #4 – **Unhappy** Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and it isn't accepted
- You try them all, none of them work :-(
- Nor do any of the security question answers

Tabletop Scenario #4 – **Unhappy** Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and it isn't accepted
- You try them all, none of them work :-(
- Nor do any of the security question answers

Tabletop Scenario #4 – **Unhappy** Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and it isn't accepted
- You try them all, none of them work :-(
- Nor do any of the security question answers

Tabletop Scenario #4 – **Unhappy** Story

- Open your company/team shared password store
- Find the cloud provider entry
- Enter a recovery token
- ... and it isn't accepted
- You try them all, none of them work :-(
- Nor do any of the security question answers

Tabletop Scenario #4 – Recovery

- Contact the helpdesk
- Contact your account manager
- Contact your lawyer
- Ask for help on social media

Tabletop Scenario #4 – Recovery

- Contact the helpdesk
- Contact your account manager
- Contact your lawyer
- Ask for help on social media

Tabletop Scenario #4 – Recovery

- Contact the helpdesk
- Contact your account manager
- Contact your lawyer
- Ask for help on social media

Tabletop Scenario #4 – Recovery

- Contact the helpdesk
- Contact your account manager
- Contact your lawyer
- Ask for help on social media

Tabletop Scenario #4 – Potential Mitigations

- Use role based authorization (multiple admins)
- Use role based accounts (noc@COMPANY)
- ... and store 2FA/recovery tokens centrally
- How do you **audit** that?
- ... **regularly?**

Tabletop Scenario #4 – Potential Mitigations

- Use role based authorization (multiple admins)
- Use role based accounts (noc@COMPANY)
- ... and store 2FA/recovery tokens centrally
- How do you **audit** that?
- ... **regularly?**

Tabletop Scenario #4 – Potential Mitigations

- Use role based authorization (multiple admins)
- Use role based accounts (noc@COMPANY)
- ... and store 2FA/recovery tokens centrally
- How do you **audit** that?
- ... regularly?

Tabletop Scenario #4 – Potential Mitigations

- Use role based authorization (multiple admins)
- Use role based accounts (noc@COMPANY)
- ... and store 2FA/recovery tokens centrally
- How do you **audit** that?
- ... **regularly?**

Tabletop Scenario #5

A close relative (or close family friend) suddenly passes away. You are asked by the family to assist with their digital affairs.

Your first step is to log into all their online accounts, and figure out what to preserve, what to close, and what needs to be renewed.

Where do you even begin?

Tabletop Scenario #5 – First steps

- Start with what you know (eg, social media accounts)
- Gain access to email
  (email redirect? password recovery?)
- Followup on all notifications to email
- Build an inventory of accounts
- This will take **months**, if not years,
  to complete

Tabletop Scenario #5 – First steps

- Start with what you know (eg, social media accounts)
- Gain access to email
  (email redirect? password recovery?)
- Followup on all notifications to email
- Build an inventory of accounts
- This will take **months**, if not years,
  to complete

Tabletop Scenario #5 – Ongoing steps

- This will take **months** if not years
- You will find out about accounts by surprise ... much later
- Sometimes when they threaten to delete data

Tabletop Scenario #5 – Ongoing steps

- This will take **months** if not years
- You will find out about accounts by surprise ... much later
- Sometimes when they threaten to delete data

Tabletop Scenario #5 – Account discovery

- Sometimes when they threaten to delete data
- Eg, Flickr

  `https://blog.flickr.net/en/2018/11/01/changing-flickr-free-accounts-1000-photos/`

- or, Twitter

  `https://www.theverge.com/2019/11/26/20984328/twitter-removing-inactive-accounts-usernames-available-date`

Tabletop Scenario #5 – Account discovery

- Sometimes when they threaten to delete data
- Eg, Flickr

  `https://blog.flickr.net/en/2018/11/01/changing-flickr-free-accounts-1000-photos/`

- or, Twitter

  `https://www.theverge.com/2019/11/26/20984328/twitter-removing-inactive-accounts-usernames-available-date`

Considering death

https://twitter.com/merxplat/status/1199786391778971648

Personal observations — 1/2

Been There, Done That:

- You will *not* have access to their cellphone
- ... or if you do at most it will be the lock screen
- Anything they told you which was “obvious” will not be obvious under stress
- You may not have access to their password store

Personal observations — 1/2

Been There, Done That:

- You will *not* have access to their cellphone
- ... or if you do at most it will be the lock screen
- Anything they told you which was “obvious” will not be obvious under stress
- You may not have access to their password store

Personal observations — 1/2

Been There, Done That:

- You will *not* have access to their cellphone
- ... or if you do at most it will be the lock screen
- Anything they told you which was “obvious” will not be obvious under stress
- You may not have access to their password store

Personal observations — 1/2

Been There, Done That:

- You will *not* have access to their cellphone
- ... or if you do at most it will be the lock screen
- Anything they told you which was “obvious” will not be obvious under stress
- You may not have access to their password store

Personal observations — 2/2

- You may not have access to their password store
- **Browser/application saved passwords are invaluable**

Personal mitigations — 1/3

- Consider your threat model
- If **you** losing access to an account is a bigger risk
- ... than a red team breaking into your house
- ... or living in your house
- Maybe optimise for **availability**

Personal mitigations — 1/3

- Consider your threat model
- If **you** losing access to an account is a bigger risk
- ... than a red team breaking into your house
- ... or living in your house
- Maybe optimise for **availability**

Personal mitigations — 1/3

- Consider your threat model
- If **you** losing access to an account is a bigger risk
- ... than a red team breaking into your house
- ... or living in your house
- Maybe optimise for **availability**

Keep good records

https://twitter.com/troyhunt/status/1213029203945410560

Personal mitigations — 2/3

- Maybe optimise for **availability**
- Fancy password stores have their place...
- ... but if they cannot be accessed,
  those passwords are gone, and have to be reset
- Which may not be what you want

Personal mitigations — 2/3

- Maybe optimise for **availability**
- Fancy password stores have their place...
- ... but if they cannot be accessed,
  those passwords are gone, and have to be reset
- Which may not be what you want

Personal mitigations — 2/3

- Maybe optimise for **availability**
- Fancy password stores have their place...
- ... but if they cannot be accessed,
  those passwords are gone, and have to be reset
- Which may not be what you want

Personal mitigations — 3/3

- Consider how you will recover from a 2FA device that is:
  - temporarily unavailable
  - permanently lost
  - broken
- How will you convince a person you are you if you need the helpdesk?
- ... and still avoid that being a means of account takeover by someone else

Personal mitigations — 3/3

- Consider how you will recover from a 2FA device that is:
  - temporarily unavailable
  - permanently lost
  - broken
- How will you convince a person you are you if you need the helpdesk?
- ... and still avoid that being a means of account takeover by someone else

Personal mitigations — 3/3

- Consider how you will recover from a 2FA device that is:
  - temporarily unavailable
  - permanently lost
  - broken
- How will you convince a person you are you if you need the helpdesk?
- ... and still avoid that being a means of account takeover by someone else

Personal mitigations — 3/3

- Consider how you will recover from a 2FA device that is:
  - temporarily unavailable
  - permanently lost
  - broken
- How will you convince a person you are you if you need the helpdesk?
- ... and still avoid that being a means of account takeover by someone else

Personal mitigations — 3/3

- Consider how you will recover from a 2FA device that is:
  - temporarily unavailable
  - permanently lost
  - broken
- How will you convince a person you are you if you need the helpdesk?
- ... and still avoid that being a means of account takeover by someone else

Personal mitigations — parallels

Is there a digital equivalent of:

- A power of attorney
- or “In case of emergency, break glass”
- ... and can you document that in a way that your loved ones will understand when they need to?

Personal mitigations — parallels

Is there a digital equivalent of:

- A power of attorney
- or “In case of emergency, break glass”
- ... and can you document that in a way that your loved ones will understand when they need to?

Personal mitigations — parallels

Is there a digital equivalent of:

- A power of attorney
- or “In case of emergency, break glass”
- ... and can you document that in a way that your loved ones will understand when they need to?

Securing people who do not look like you... yet

Recommended presentation:
“Kawaiicon 2019 - How can I help you?” — Laura Bell

`https://www.youtube.com/watch?v=YrMlo2SRFlM`

`https://www.slideshare.net/LauraBell15/`

`securing-people-that-dont-look-like-you-yet`

Classifying digital security needs:

`https://github.com/open-security-nz/sage`

Conclusions — 1/2

- You do not have one authentication method
- You have **several** authentication methods
- Used alternately, or in combinations (MFA)
- Attackers will attack the weakest one/combination

Conclusions — 2/2

- You might find yourself facing the strongest authentication combination
- ... unprepared
- Consider optimising for availability
- ... or at least recoverability

Conclusions — 2/2

- You might find yourself facing the strongest authentication combination
- ... unprepared
- Consider optimising for availability
- ... or at least recoverability

Conclusions — 2/2

- You might find yourself facing the strongest authentication combination
- ... unprepared
- **Consider optimising for availability**
- **... or at least recoverability**

Questions/Discussion

https://www.naos.co.nz/talks/authentication-afterlife/

Twitter: @ewenmcneill
Email: ewen@naos.co.nz

Questions?

Tabletop Scenario #1

There was a fire. A big fire.

It took out your main computer. And your backups.

Fortunately all your data is safe online. But you do not remember the passwords.

How do you get back in?

Tabletop Scenario #2

You need to log in to an account on a new device.

All your important accounts are secured with 2FA.

Your 2FA device (phone or token) stopped working, or is not with you.

Tabletop Scenario #3

Your bag was stolen. Containing your main computer, your phone, and all 2FA tokens you own.

Can the thief now impersonate you?

How do you recover access to your accounts first, and lock them out?

Tabletop Scenario #4

Your startup had a security conscious founder. They used cloud services and 2FA for everything.

After the startup got bought out, the founder left, and wiped all their devices on the way out the door.

One of the first used cloud providers threatens to delete the entire account if the new terms and conditions are not accepted, by the end of the week, by the original user account.

Tabletop Scenario #5

A close relative (or close family friend) suddenly passes away. You are asked by the family to assist with their digital affairs.

Your first step is to log into all their online accounts, and figure out what to preserve, what to close, and what needs to be renewed.

Where do you even begin?

URLs – #1

- Tabletop Scenarios
  - https://twitter.com/badthingsdaily
  - https://medium.com/starting-up-security/fun-with-incident-response-on-twitter-a7ea55cf18a6
- Password reset
  - https://www.troyhunt.com/everything-you-ever-wanted-to-know/
  - https://en.wikipedia.org/wiki/Self-service_password_reset
- Easier to change password
  - https://twitter.com/deviantollam/status/1207161968223805440
  - https://thehardtimes.net/culture/report-changing-password-every-login-easier-than-remembering-password/

URLs – #2

- 2FA recovery
  - https://help.github.com/en/github/authenticating-to-github/recovering-your-account-if-you-lose-your-2fa-credentials
  - https://thenextweb.com/apple/2014/12/08/lost-apple-id-learnt-hard-way-careful-two-factor-authentication/
- Finding accounts by deletion notices
  - https://blog.flickr.net/en/2018/11/01/changing-flickr-free-accounts-1000-photos/
  - https://www.theguardian.com/technology/2018/nov/02/flickr-delete-millions-photos-reduce-allowance-free-users
  - https://www.theverge.com/2019/11/26/20984328/twitter-removing-inactive-accounts-usernames-available-date
  - https://www.theverge.com/2019/11/27/20986084/twitter-inactive-accounts-usernames-memorialize-deceased-users-not-removing

URLs – #3

- Password storage
  - https://twitter.com/troyhunt/status/1213029203945410560
  - https://www.troyhunt.com/password-managers-dont-have-to-be-perfect-they-just-have-to-be-better-than-not-having-one/
- Digital Security Needs
  - https://www.youtube.com/watch?v=YrMlo2SRFlM
  - https://www.slideshare.net/LauraBell15/securing-people-that-dont-look-like-you-yet
  - https://github.com/open-security-nz/sage