BASTION
SECURITY GROUP

MFA, stories that make you go huh?

September 2024

Jacob & David

OWASP NZ Day

#whoami

- Jacob Hawthorne
- LinkedIn - /jacob-hawthorne-957920150/
- Wellington based
- Offensive Security Consultant
- Specialising in “the Cloud”

#whoami

- David Robinson
- X -@nzkarit
- Mastodon - @karit@infosec.exchange
- BlueSky - @karit.nz
- Hacker from Wellington
- Run Kākācon

Outline

- Background
- MFA Implementations Issues
- MFA Issues in Web Apps
- MFA Issues in the Cloud
- So What to Do

Takeaways

- Why you should be using MFA
- How to avoid common MFA mistakes
- How to implement a robust authentication system with MFA

Background

Terminology

- 2FA, MFA, 2SV - all subtly different but for today we are talking about the same thing
- Factors
  - Something you know – Password
  - Something you have - Token, Card, Phone App, etc
  - Something you are - Fingerprint, Iris Scan, etc

Why Username and Password is not enough

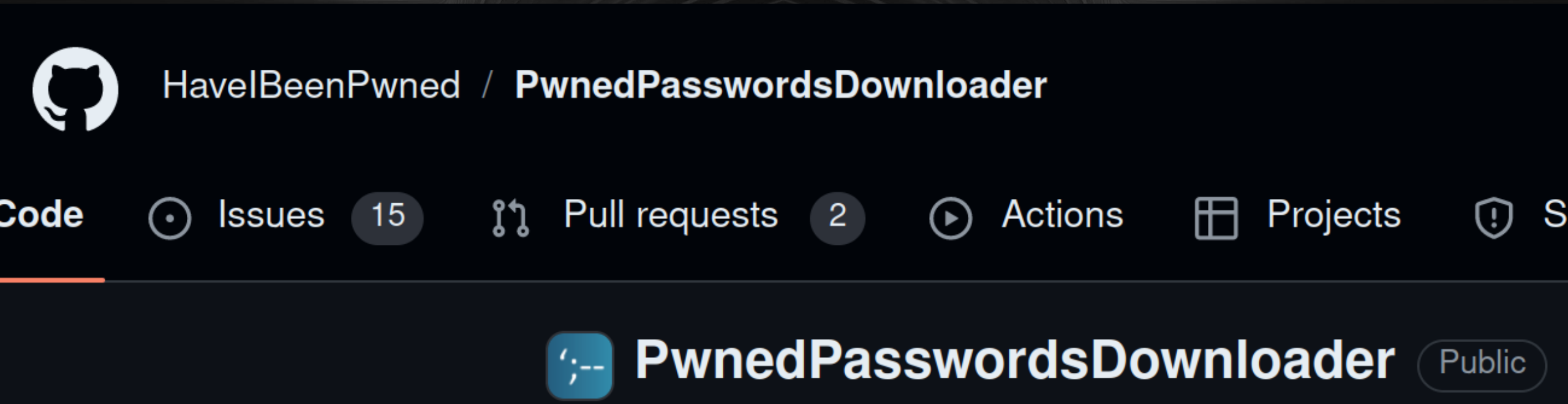
- Password Reuse
  - People use the same password on multiple sites
- Every year there are multiple breaches where the attackers use credentials gained from a breach to access other sites
- Some vendors deal with this well
  - Logmein for example forced a password reset after LinkedIn, MySpace & Tumblr were breached

Don’t allow passwords from breach corpus

- NIST gone as far as saying:
  - When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list MAY include, but is not limited to:
    - Passwords obtained from previous breach corpuses.
    - Dictionary words.
    - Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’).
    - Context-specific words, such as the name of the service, the username, and derivatives thereof.

Need a list of passwords from breaches?

- https://github.com/HaveIBeenPwned/PwnedPasswordsDownloader



Why are breaches an issue?

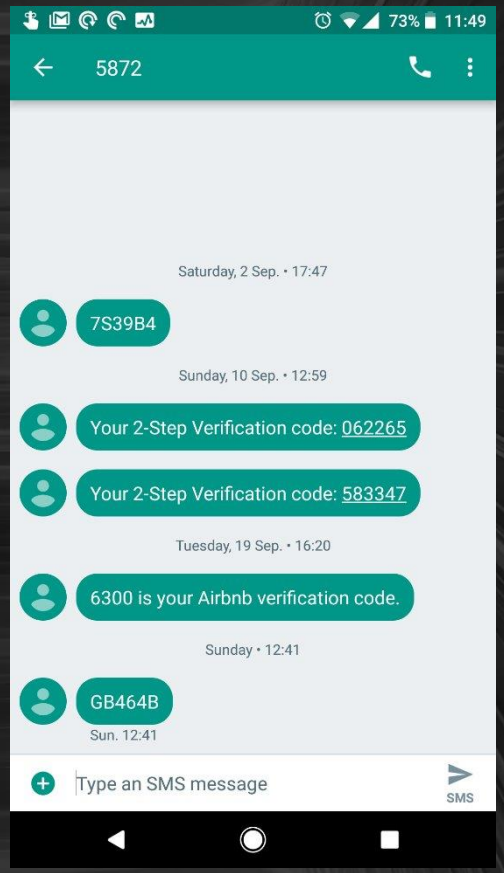
- Why does a breach of another site affect my site?
- People reuse passwords between sites
- Sites may not securely store passwords correctly
  - No hashing (unencrypted)
  - No salt or using the same salt
  - Using a weak hashing algorithm (MD5, SHA1)
- This makes the passwords easily crackable
- If storing passwords follow the OWASP Cheat Sheet on password storage

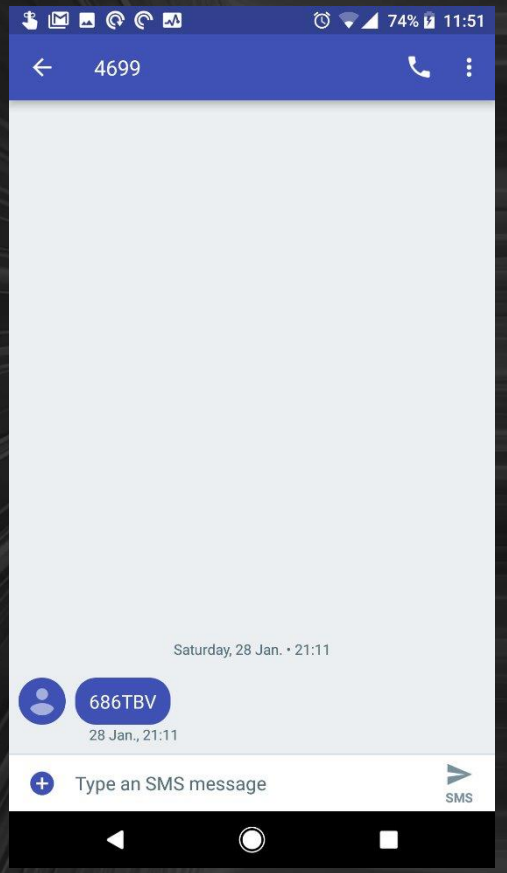
MFA to the Rescue

MFA to the Rescue

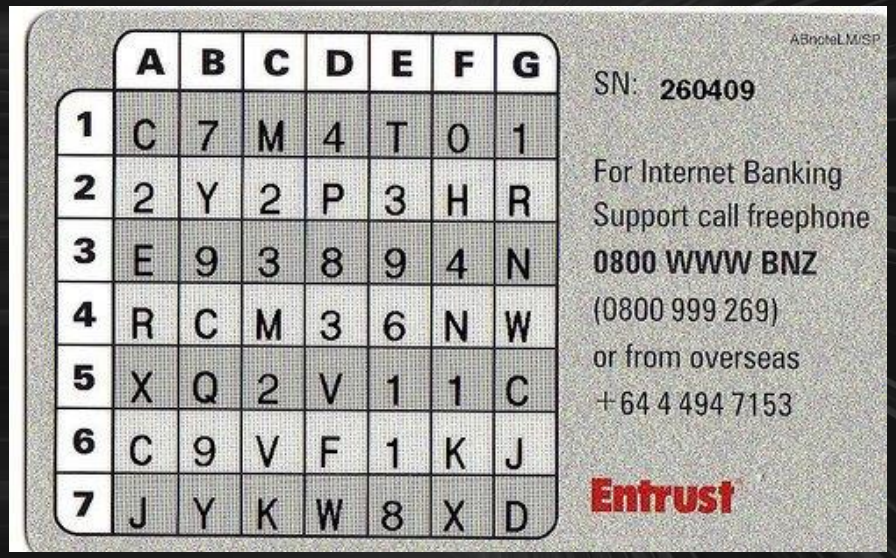
- What is MFA?
- Different implementations
- What are the different factors of MFA?

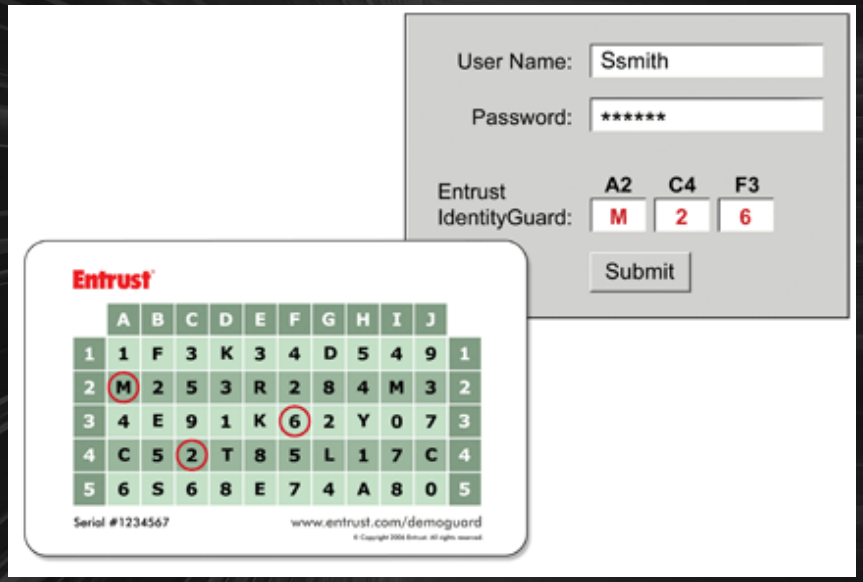
SMS


73% 11:49
5872
Saturday, 2 Sep. • 17:47
7S39B4
Sunday, 10 Sep. • 12:59
Your 2-Step Verification code: 062265
Your 2-Step Verification code: 583347
Tuesday, 19 Sep. • 16:20
6300 is your Airbnb verification code.
Sunday • 12:41
GB464B
Sun. 12:41
Type an SMS message
SMS

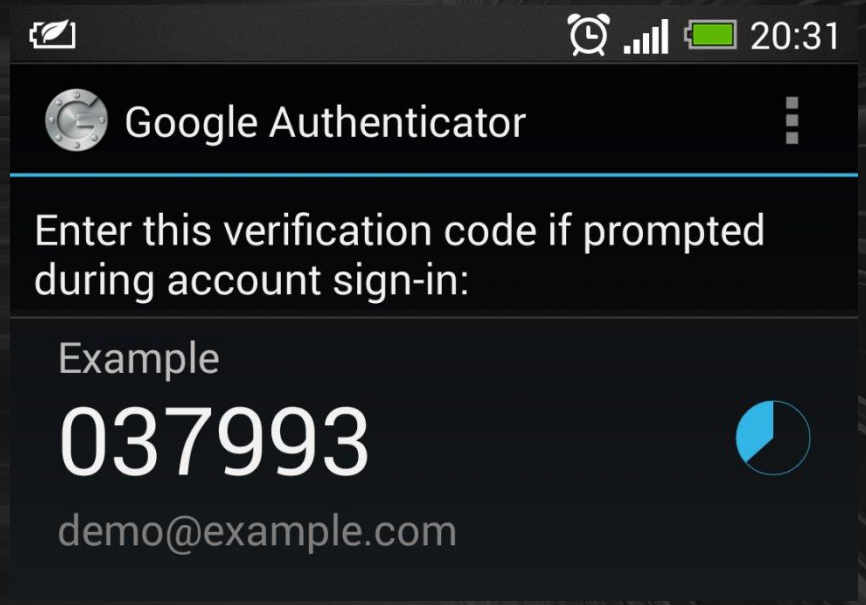

74% 11:51
4699
Saturday, 28 Jan. • 21:11
686TBV
28 Jan., 21:11
Type an SMS message
SMS

Battleship Cards



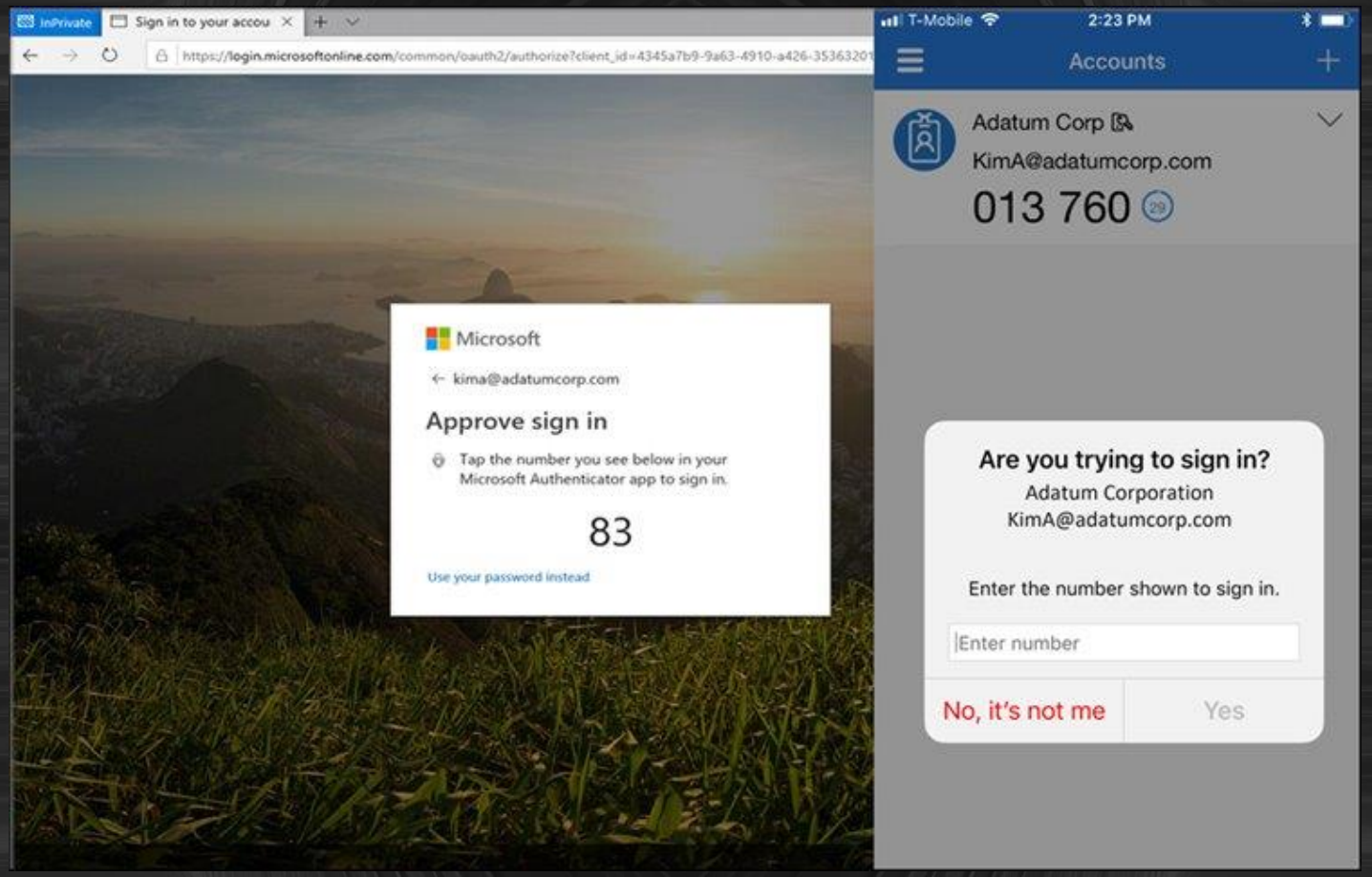


Time Based One Time Passwords (TOTP)



Biometrics

Push Notifications



Universal Second Factor (U2F)

Universal Second Factor (U2F)

- Most costly option

- Uses a hardware Security Module which is very difficult to clone
- Hard for user to misuse
- Has proof of presence

- Supported by most major browsers now

Passwordless/Passkeys

- WebAuthN
- TPM with Fingerprint
- U2F with PIN

- Ties the login to the Device

MFA Implementation Issues

SMS

- User has a phone number associated with their account
- They are text'ed a code which they enter when authenticating

- Pros:
  - Telco's worry about device enrolment, lost phones, etc

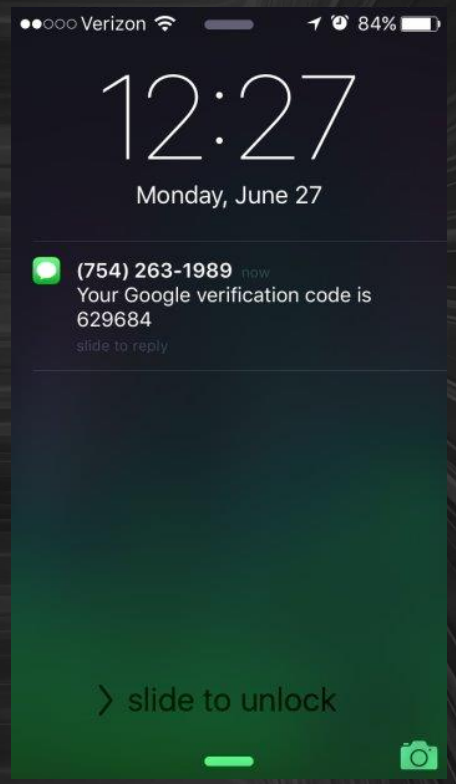
- Cons:
  - As a service provider you have to pay for each text, or block of text's
  - Text messages don't roam well through text message gateways
  - The Telco is responsible for your security (and someone trying to port your number)

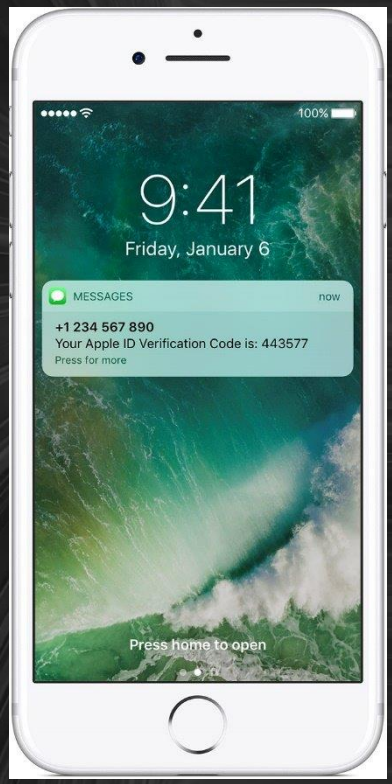
Telco responsible for your security

- SIM Card Swap
  - We have tried social engineering but Spark, Vodafone and 2 Degrees all asked for photo ID
  - Maybe an attacker could just access the person account through password reuse?

- It is policy to ask for photo ID but depends on the person
  - You may have some luck porting a number without a photo ID

Your phone will just display the code to everyone



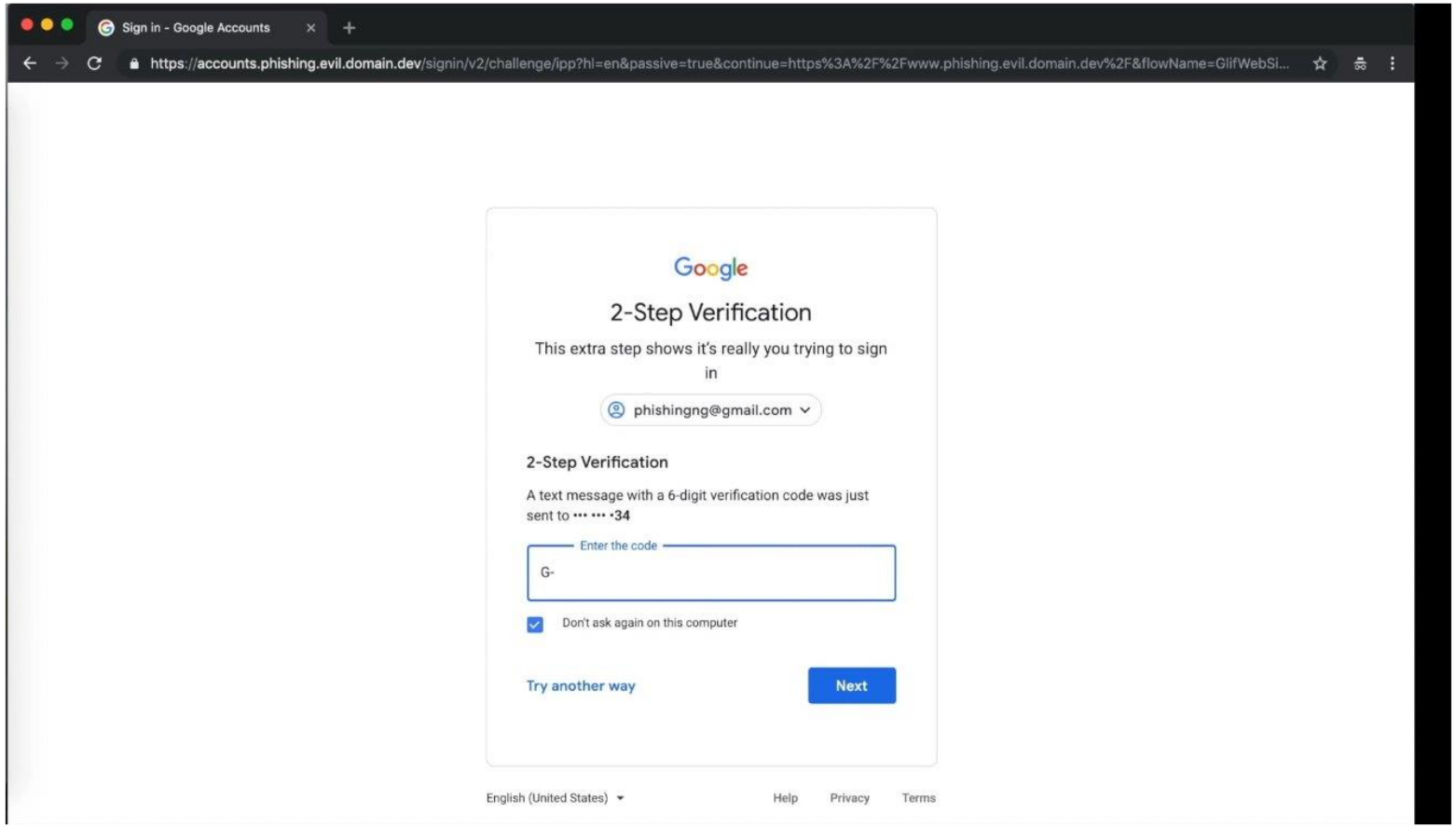


Phishing 2FA Authentication Tokens

Proxying In Action (2FA bypass)

"A picture is worth a thousand words":

Modlishka in action against an example two factor authentication scheme (SMS based bypass proof-of-concept) :



Evilginx

```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                        no nginx - pure evil

        by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+----------+------------+------------+--------+------------------+------------------+
| id  | phishlet | username   | password   | tokens |    remote ip     |       time       |
+-----+----------+------------+------------+--------+------------------+------------------+
| 19  | google   |            |            | none   | [redacted]       | 2018-05-28 08:23 |
+-----+----------+------------+------------+--------+------------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+----------+-----------------------+---------------+----------+-------------+------------------+
| id  | phishlet |       username        |   password    |  tokens  |  remote ip  |       time       |
+-----+----------+-----------------------+---------------+----------+-------------+------------------+
| 19  | google   | [redacted]@gmail.com  | [redacted]    | captured | [redacted]  | 2018-05-28 08:24 |
+-----+----------+-----------------------+---------------+----------+-------------+------------------+

:
```

U2F Keys

Yubico to replace vulnerable YubiKey FIPS security keys

Yubico staff discovers bug in YubiKey FIPS Series keys; offers replacements for affected customers.

By Catalin Cimpanu for Zero Day | June 13, 2019 -- 18:12 GMT (04:12 AEST)

YubiKeys are vulnerable to cloning attacks thanks to newly discovered side channel

Sophisticated attack breaks security assurances of the most popular FIDO key.

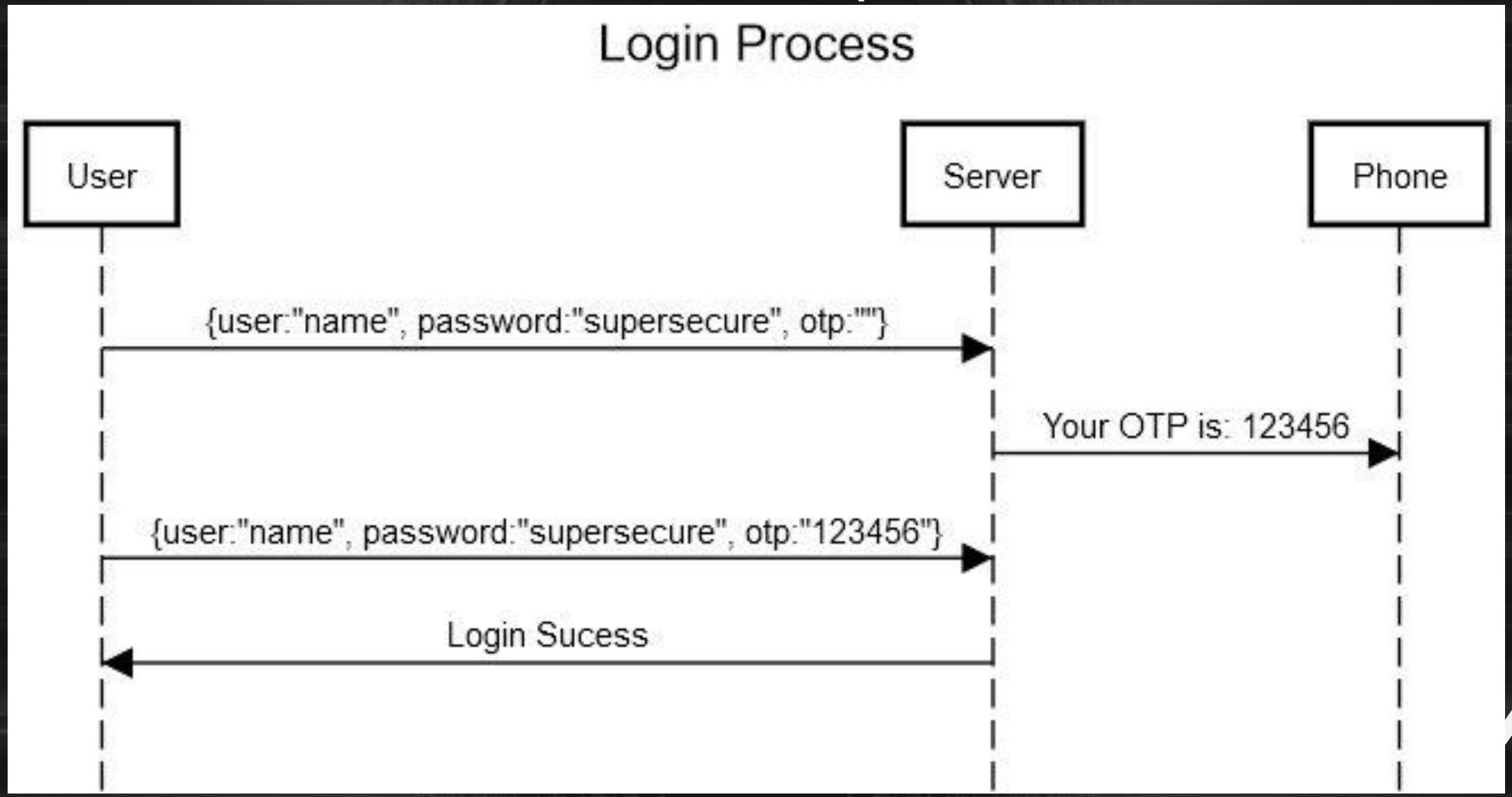
DAN GOODIN - 9/4/2024, 5:58 AM

Issues with Web Apps

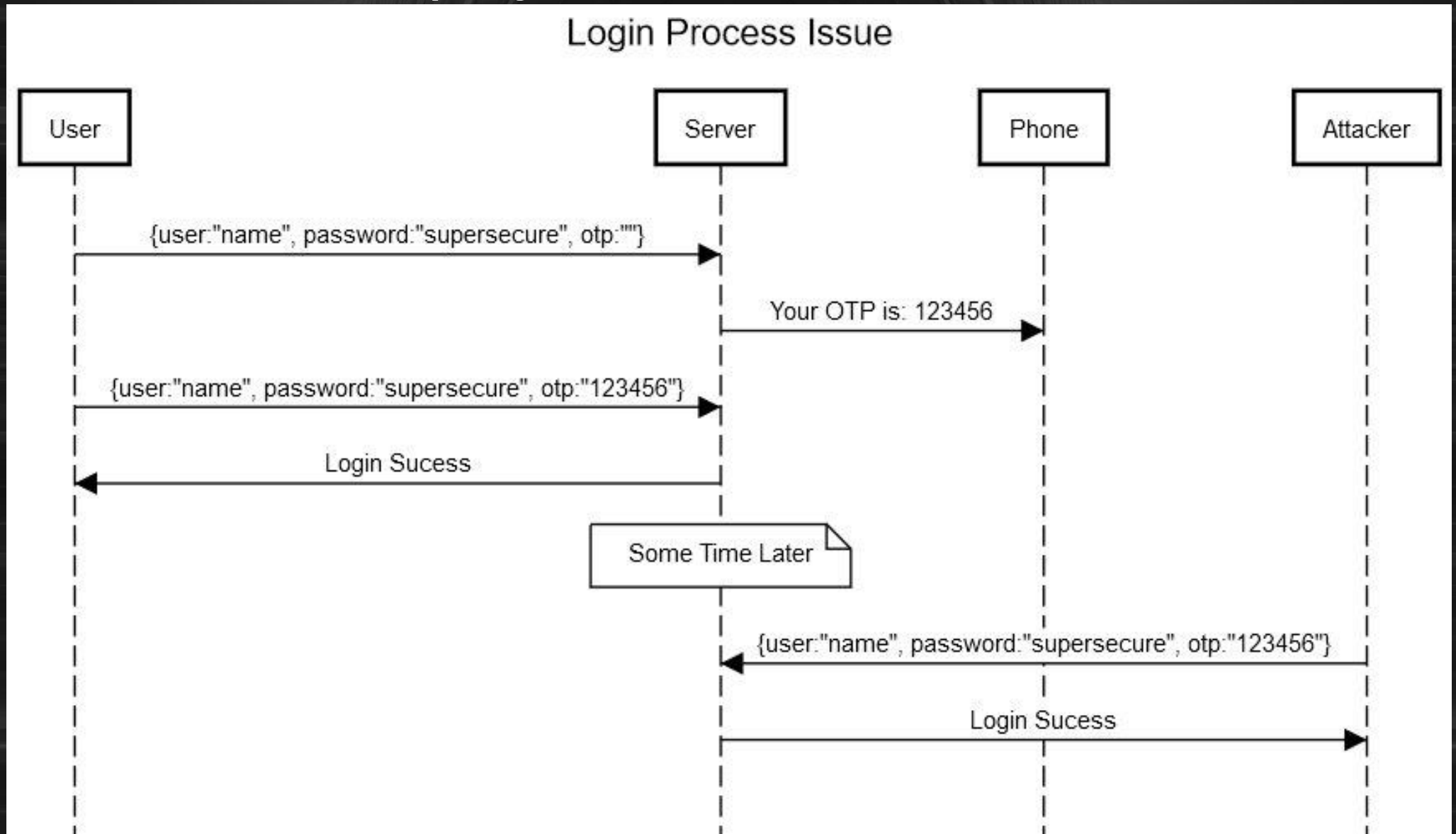
Only one form or one at time

- If want to change MFA type have to disable and then renable
- Can't add two or more tokens, TOTP, etc

OTP - The “ONE” in OTP is important



OTP - Token Replay



OTP - Recommendation

- Expire the OTP after use
- Have a time window

SQL Query Example

- SELECT * FROM otp WHERE otp = ?;

SQL Query Update

```
SELECT *
    FROM otp
    WHERE username = ?
        AND otp = ?
        AND used = FALSE --check if code has already been used
        AND current_time() < (generated_time + 5min) -- check code age
        FOR UPDATE; -- Stop concurrent login race conditions
```


SQL Query - Recommendations

- Ensure that:
  - You match the user with the generated code
  - Check if the OTP has already been used
  - Check the generation time of the OTP
  - Use Transactions to ensure don't allow race conditions

TOTP - Seeds

- Only show the once when set up

- Session takeover can navigate to TOTP settings
- See the code enrol a device

TOTP – Seeds – Recommendations

- Only show the once

TOTP Seeds, what about preauth

- Login into form
- Taken to MFA Prompt

- If direct browse to a page returned to Login Form

- But if direct browse to MFA setup can configure MFA
- Including adding new MFA

TOTP Seeds, what about preauth – What Happening?

- Because MFA setup is needed for first login
- Had different RBAC applied to it
- The cookie from a login was enough

- MFA was set up so flow prompted
- But Cookie enough to setup MFA as that would be like first login flow to setup MFA

MFA Enrolment Scenario

- Org required MFA for their PAM solution
- To be "safer" didn't use web flow emailed details
- Admin email user the QR code
- Person email back the challenge response
- Corporate level no MFA

MFA Enrolment - Hack the Org

- Was an internal job
- Used responder to get password hashes
- One cracked hash was for that user
- But the email didn't have MFA
  - So when we use Responder and crack the Admin's hash
  - Had all the MFA details in the inbox

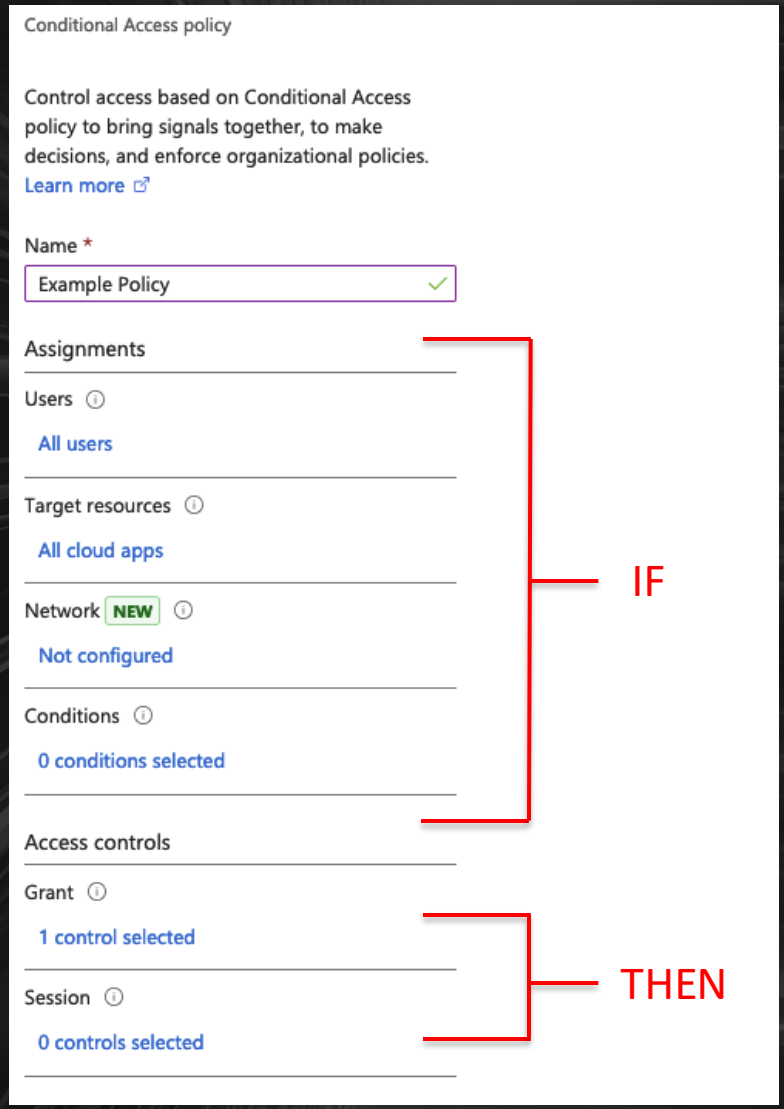
MFA Enrolment – What to Do

- Make sure not saving/storing MFA setup details
- MFA everything

Issues With Cloud

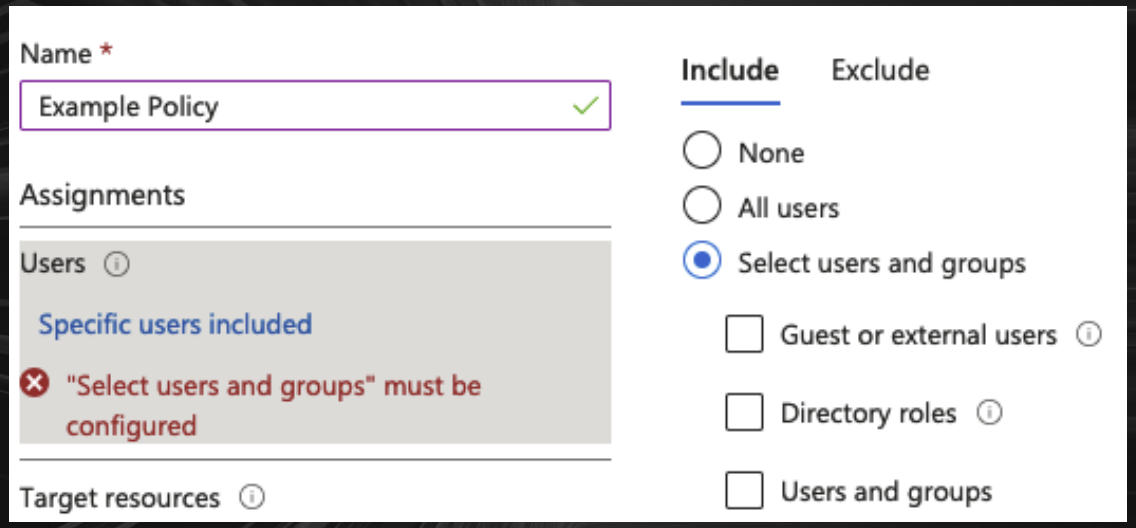
What are Conditional Access Policies?

- “CAPs”
- Microsoft defines them as if-then statements



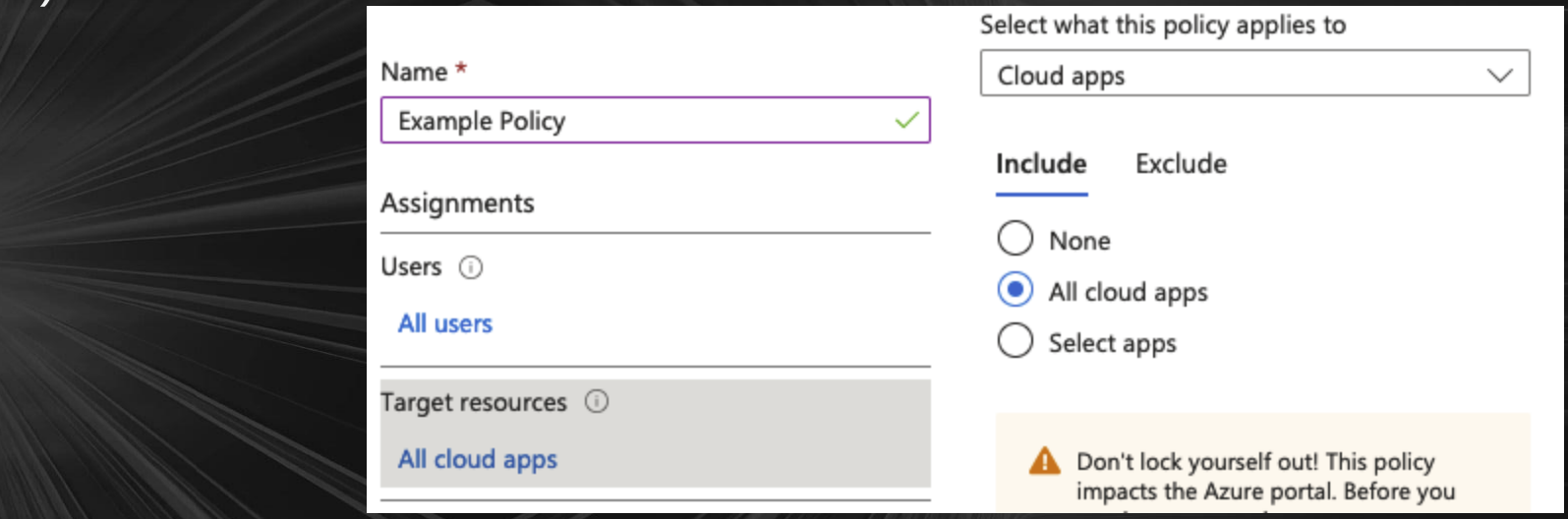
The ‘IF’

- Users
  - Users and Groups
  - Guests or external users
  - Directory roles – administrators



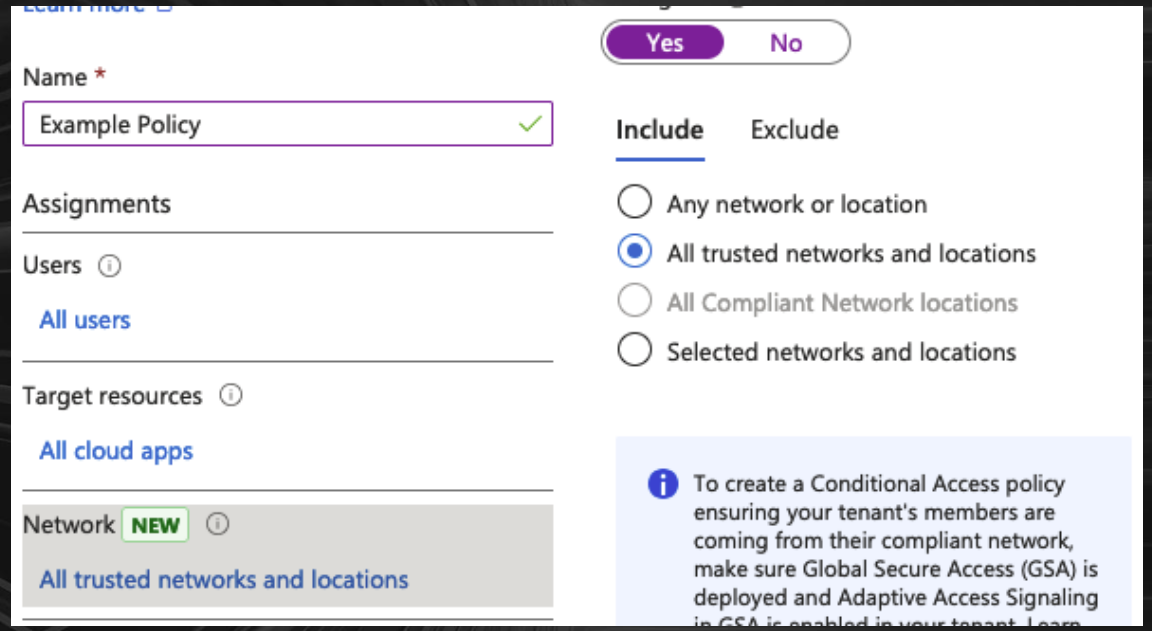
The ‘IF’

- Cloud Apps (applications)
  - Internal
  - SSO
  - Microsoft



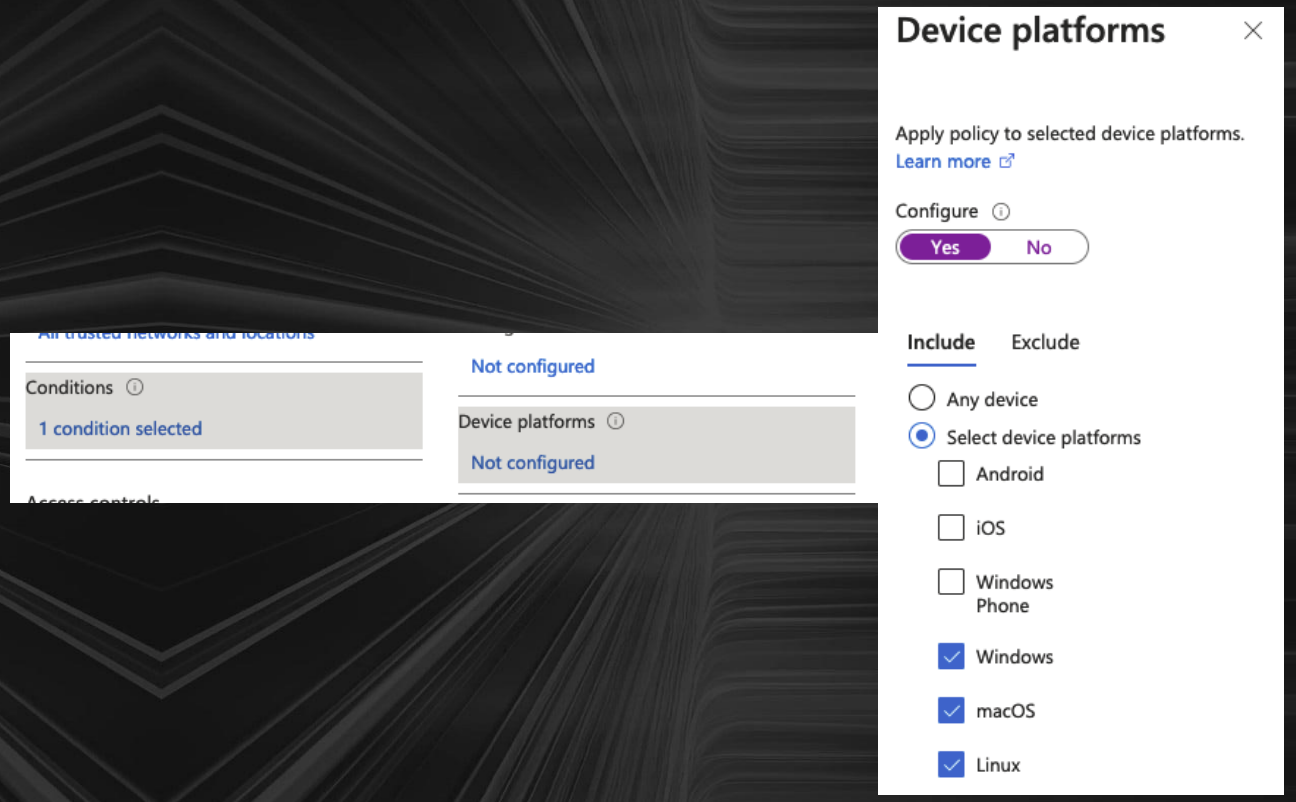
The ‘IF’

- Networks and Locations



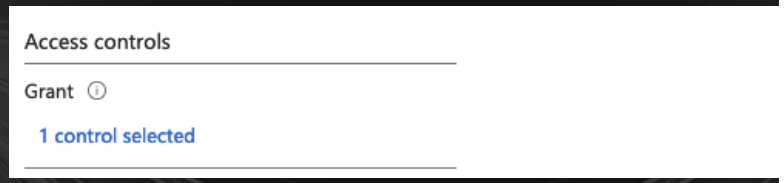
The ‘IF’

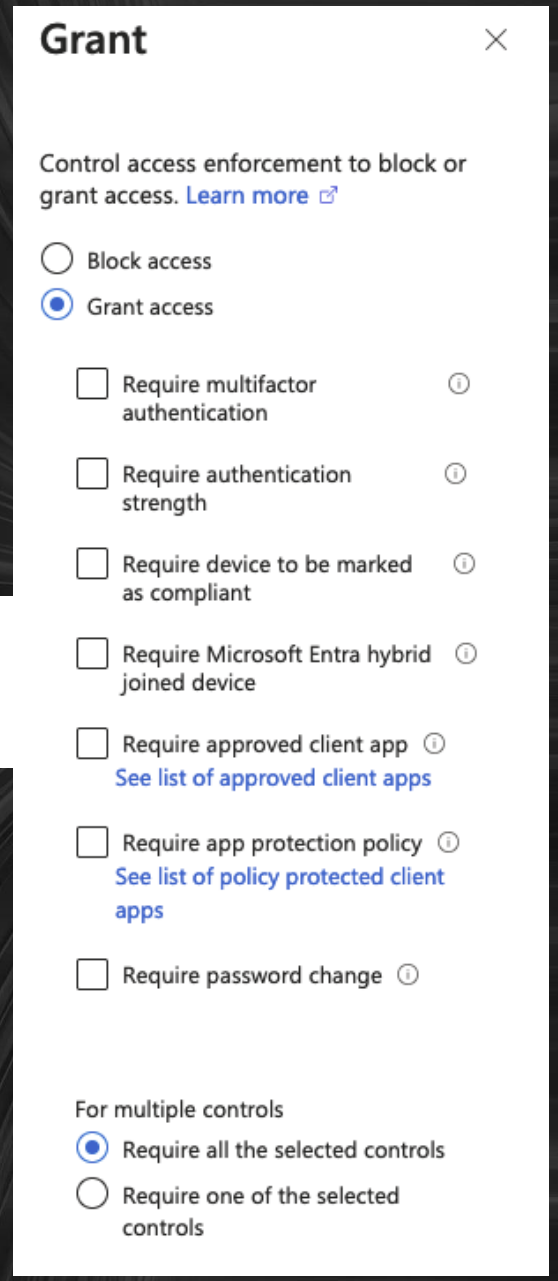
- Device platforms



The ‘THEN’

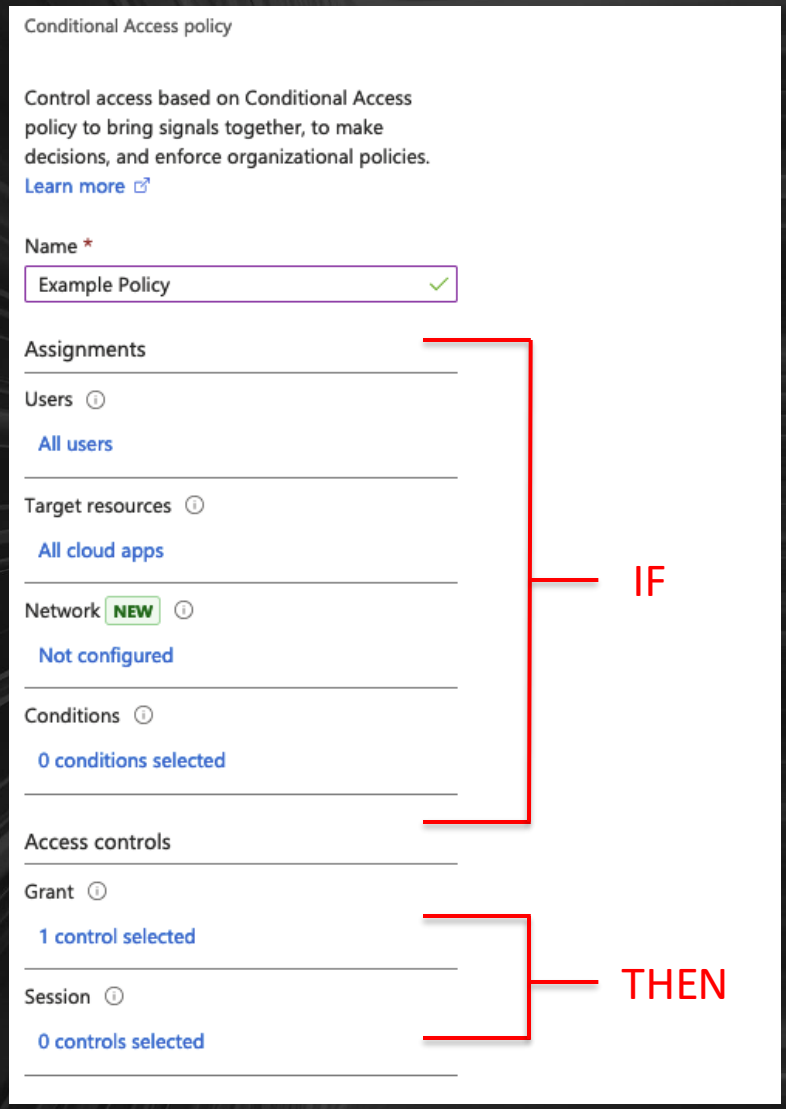
- Block access
- Grant access
- Grant access with controls





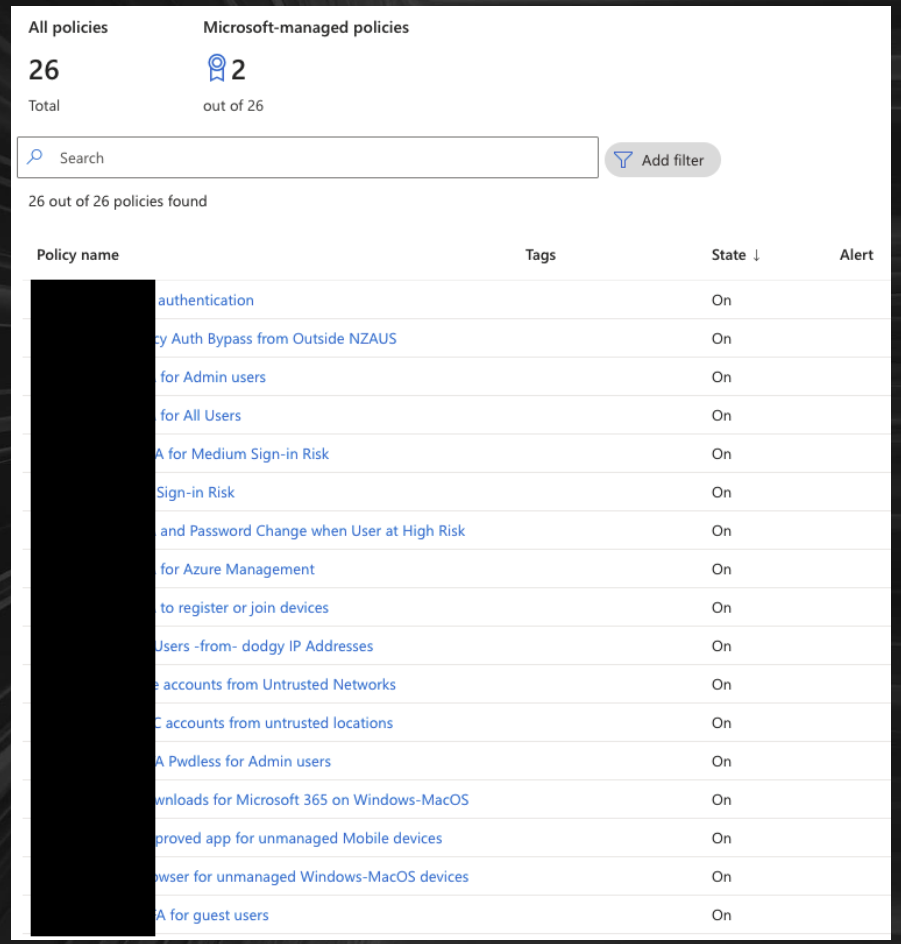
The nitty gritty of CAPs

- They are applied at the authorisation stage, NOT authentication
- All “IF” checks defined in a CAP must be met before the “THEN” (access control) is applied



The nitty gritty of CAPs

- CAPs that match an authentication flow are ALL applied, at the same time
- Unlike most firewalls, they default open

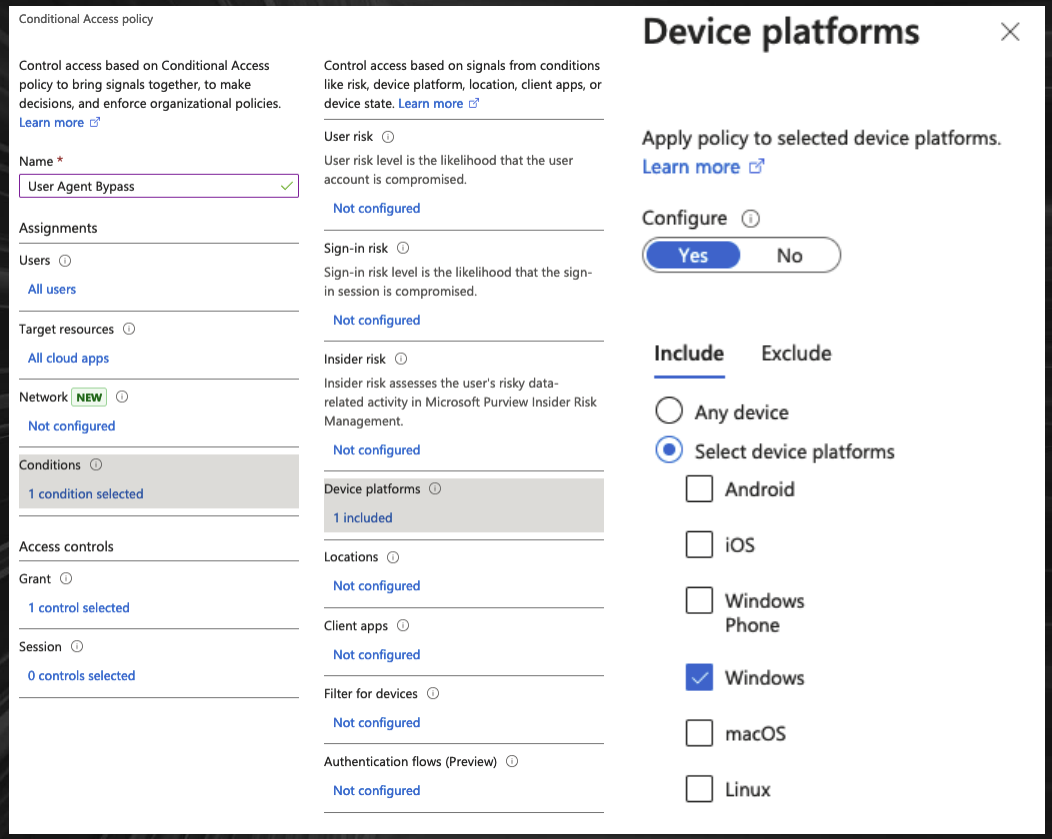


User Agent Bypass

The Conditional Access Policy

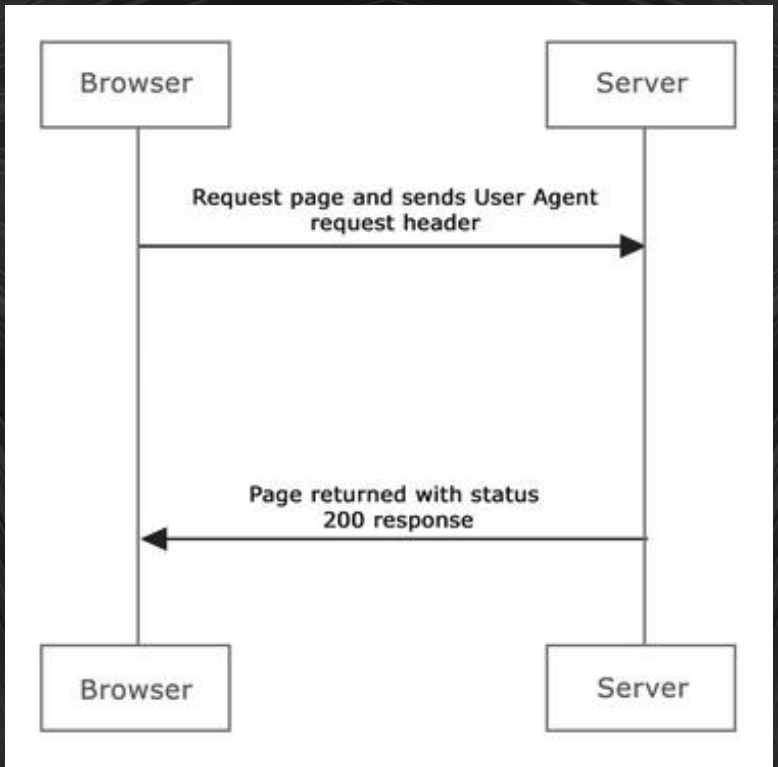
- Our organisation wants to require MFA for users accessing applications from a Windows device

- We create a Conditional Access Policy with the following:
  - All users
  - All applications
  - Logging in from Windows devices
  - Require MFA



How does our CAP know what device we are using?

- When sending a request to the webserver our request includes the “User Agent” header



What is it?

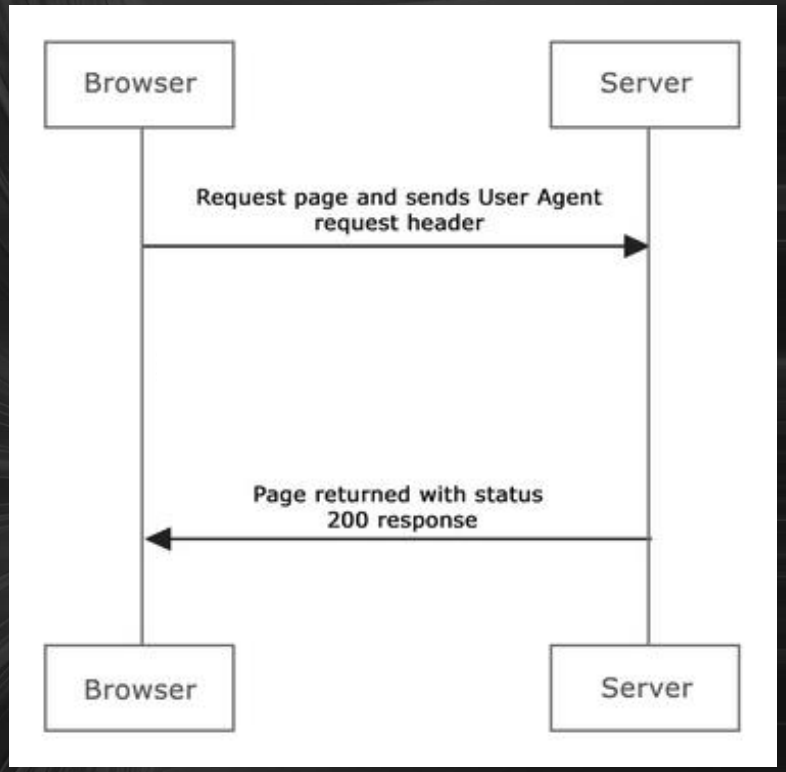
User agent header includes the following information:

- Browser and version
- Operating System and version
- Device

```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) Edge/127.0.0.0
```

Abusing the misconfiguration

- The user agent header is sent to the webserver from the client
  - And... we control the client



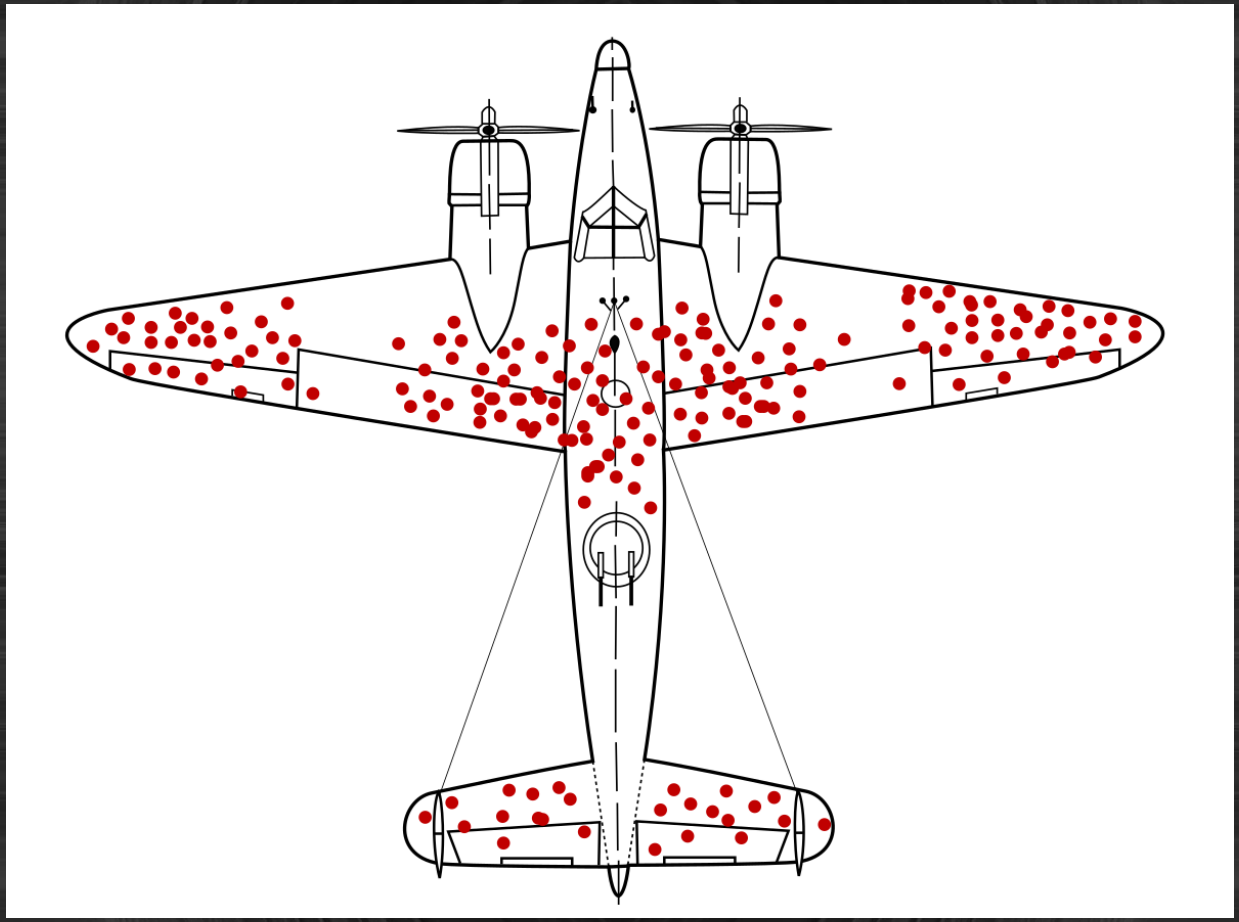
Let’s make a change to our “user agent”

- Maybe we want to come from a “Windows phone”

- Our request no longer matches our CAP

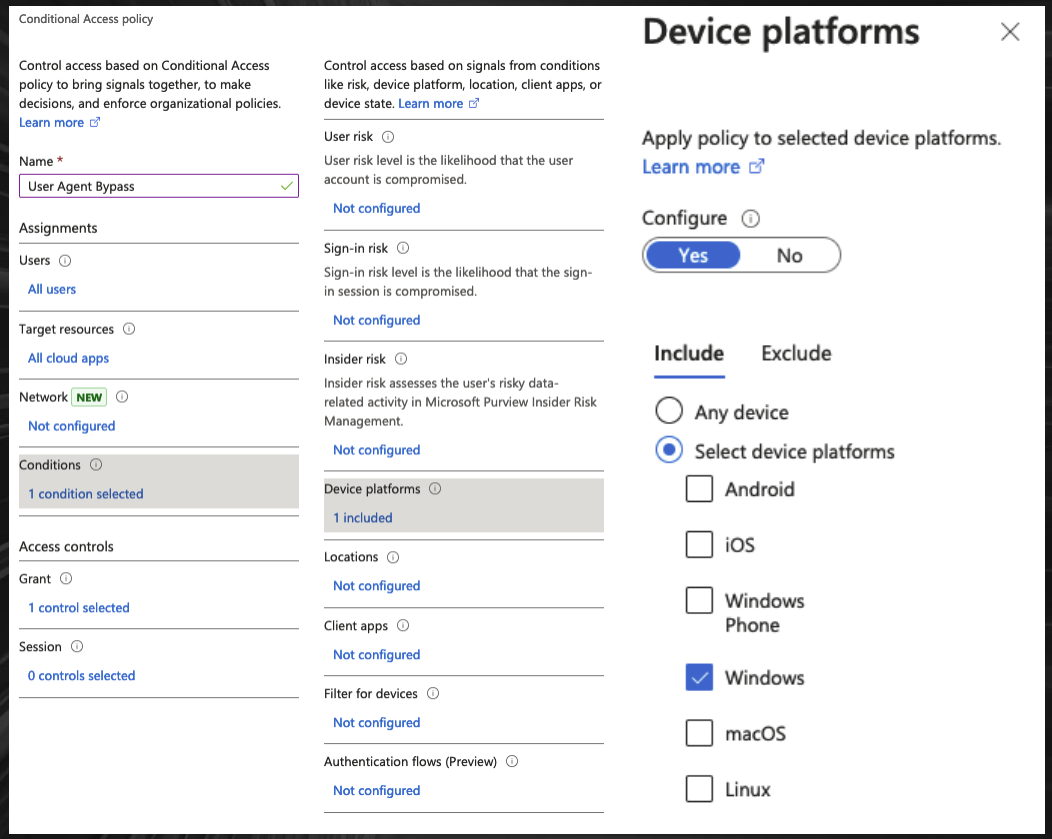
```
Mozilla/5.0 (Windows Phone 10.0; Android 4.2.1; Microsoft; Lumia 650)
```

So why does this happen?



Summary

- Our CAP did not consider ”other” devices
- Organisations often build Conditional Access policies around the devices they have and do not consider access from devices they don’t have
- Because we must meet all ”IF”s, changing our ”user agent” did not match this policy



The Fix / Recommendations

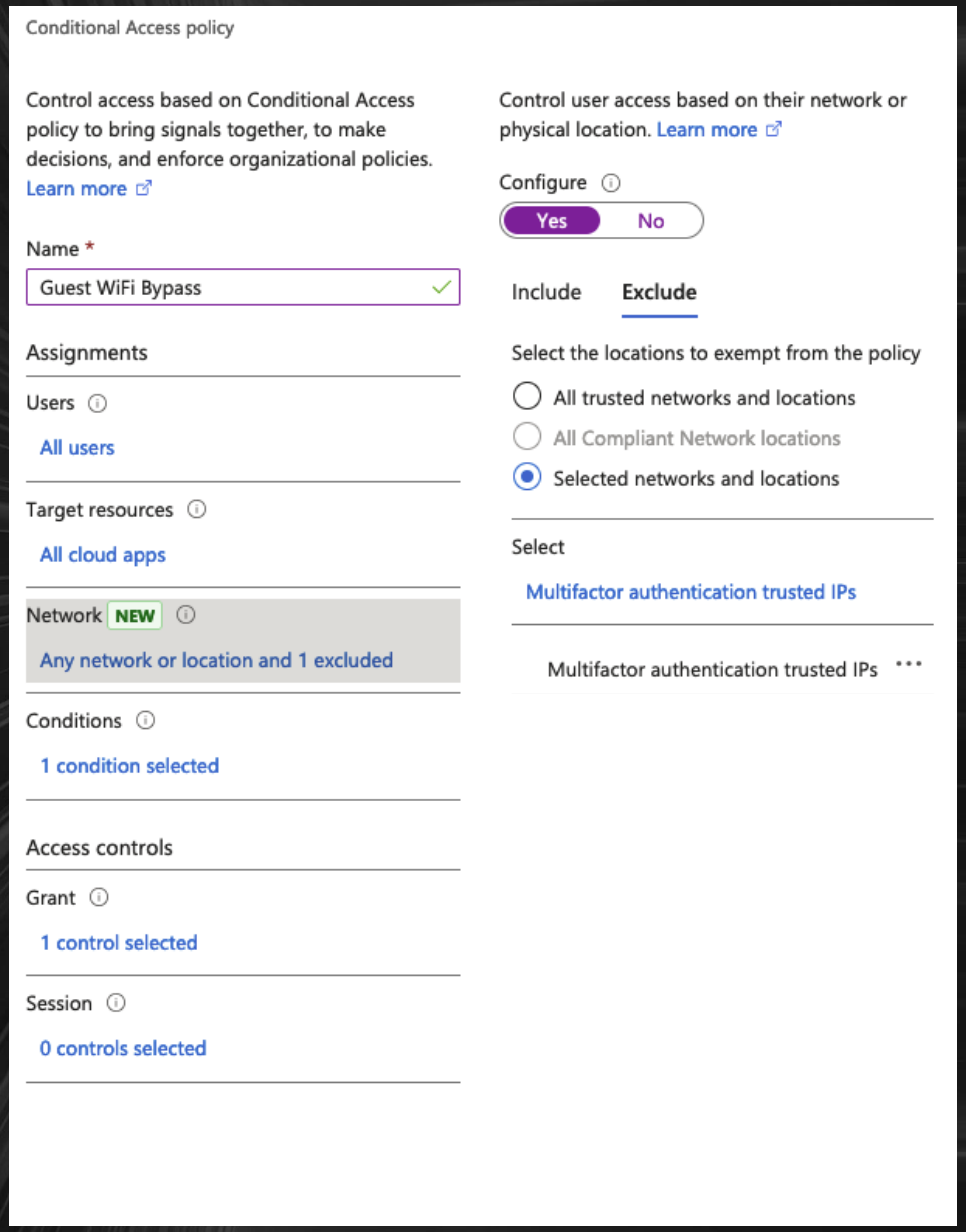
- Do not consider any client controlled/provided information in a security check
- Ensure you are protecting against devices you do AND don’t have
- Consider using “Filter for devices” in the policy, as a replacement

Guest WiFi Bypass

The Conditional Access Policy

- Our organisation wants to require MFA for users accessing any application from all locations except for the corporate network

- We create a Conditional Access Policy with the following:
  - All users
  - All applications
  - Logging in from any IP
    - Require MFA
  - Logging in from a corporate IP
    - Do not require MFA



Why is this an issue?

- If you only have one outbound IP address, the guest network will also use the same IP.
- With only a single outbound IP address you have now told your CAP to ignore the guest Wi-Fi.
- Guest Wi-Fi has little security control
  - Weak/no password
  - Password found at reception or on the wall
  - Access points allow connection from public areas

Abusing the misconfiguration

- Connect to the guest WiFi...
- Have a valid username and password for the target account

The Fix / Recommendations

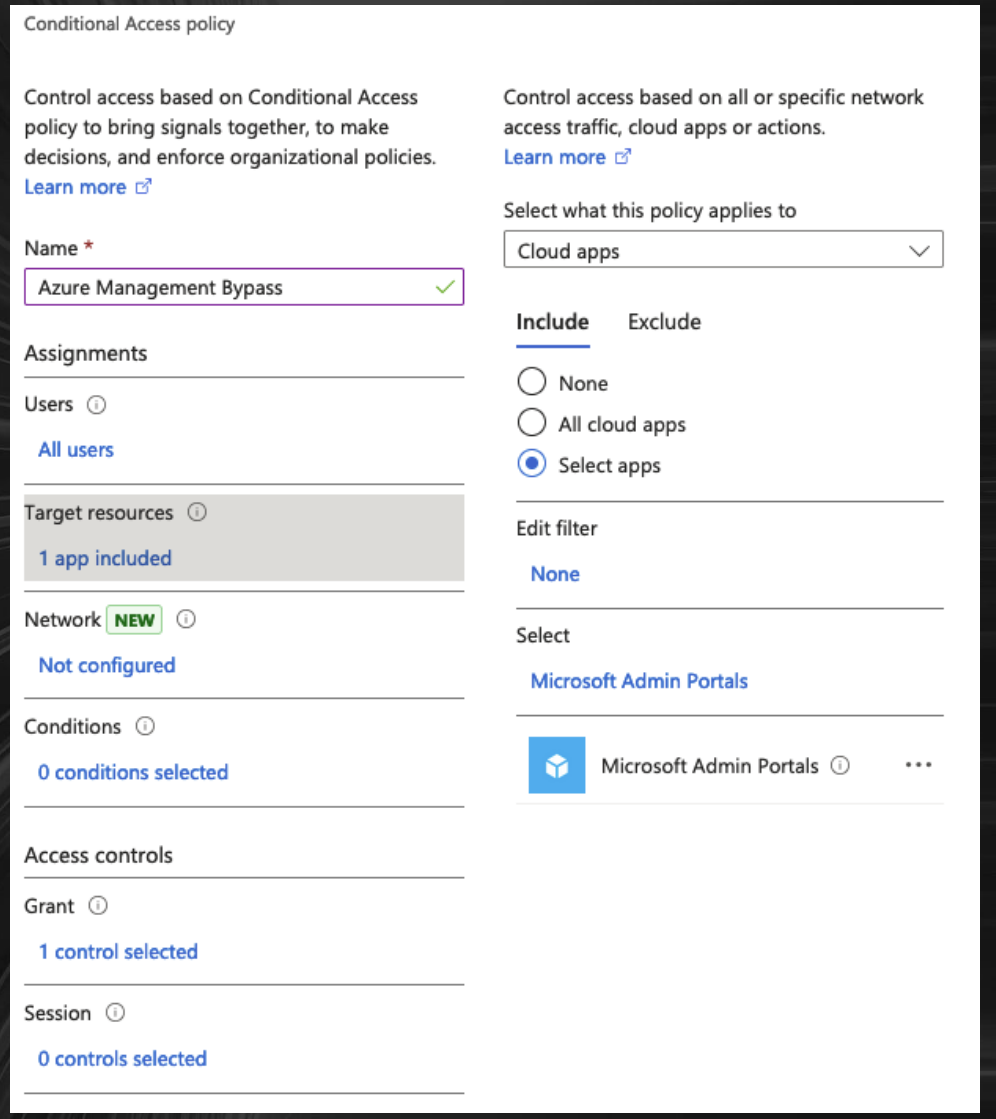
- Educate users on MFA
- Enforce MFA for all locations
- If you must exclude the corporate network, ensure you have a different outbound IP address for the secured and unsecured network.

Azure Management Tools Bypass

The Conditional Access Policy

- Our organisation wants to require MFA for users and administrators accessing the Azure Portal

- We create a Conditional Access Policy with the following:
  - All users
  - Microsoft Admin Portals
  - Require MFA



Why is this an issue?

- “Microsoft Admin Portals” cloud app, does not co… …ols

Abusing the misconfiguration

If the “Azure Resource Manager” client app is not included, we can use single factor for any of the following:

- Azure CLI
- Azure Data Factory portal
- Azure DevOps
- Azure Event Hubs
- Azure PowerShell
- Azure Service Bus
- Azure SQL Database
- Azure Synapse
- Classic deployment model APIs
- Microsoft 365 admin center
- Microsoft IoT Central
- SQL Managed Instance
- Visual Studio subscriptions administrator portal

Abusing the misconfiguration

- If Graph API is not included, we can single factor to it and access the REST APIs and client libraries to access data on the following Microsoft cloud services:
  - Microsoft Graph exposes **Microsoft 365 core services:** Bookings, Calendar, Delve, Excel, Microsoft 365 compliance eDiscovery, Microsoft Search, OneDrive, OneNote, Outlook/Exchange, People (Outlook contacts), Planner, SharePoint, Teams, To Do, Viva Insights
  - **Enterprise Mobility + Security services:** Advanced Threat Analytics, Advanced Threat Protection, Microsoft Entra ID, Identity Manager, and Intune
  - **Windows services:** activities, devices, notifications, Universal Print
  - **Dynamics 365 Business Central services**

The Fix / Recommendations

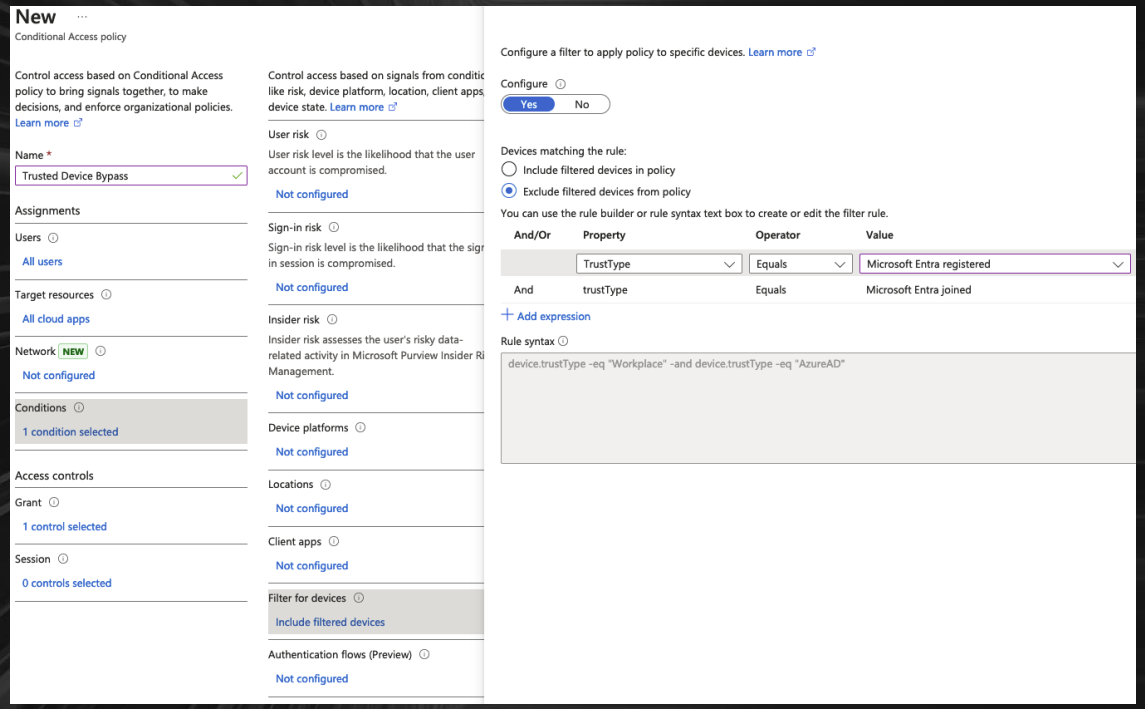
- Ensure all “all cloud apps” are included in the policy
  - Microsoft Admin Portals
  - Azure Resource Manager
  - Azure Credential Config
  - Azure AD Identity Governance
  - AAD Reporting
- Understand the limitations of security defaults – this starting point.
- Ensure any “administrative” apps are included in the policy
- **any cloud app that uses Graph API

Trusted Devices Bypass

The Conditional Access Policy

- Our organisation wants to allow single factor for users accessing applications from corporate enrolled devices

- We create a Conditional Access Policy with the following:
  - All users
  - All applications
  - Logging in from any “device”
    - Require MFA
  - Logging in from a corporate “enrolled” devices
    - Do not require MFA



How does our CAP know if our device is enrolled?

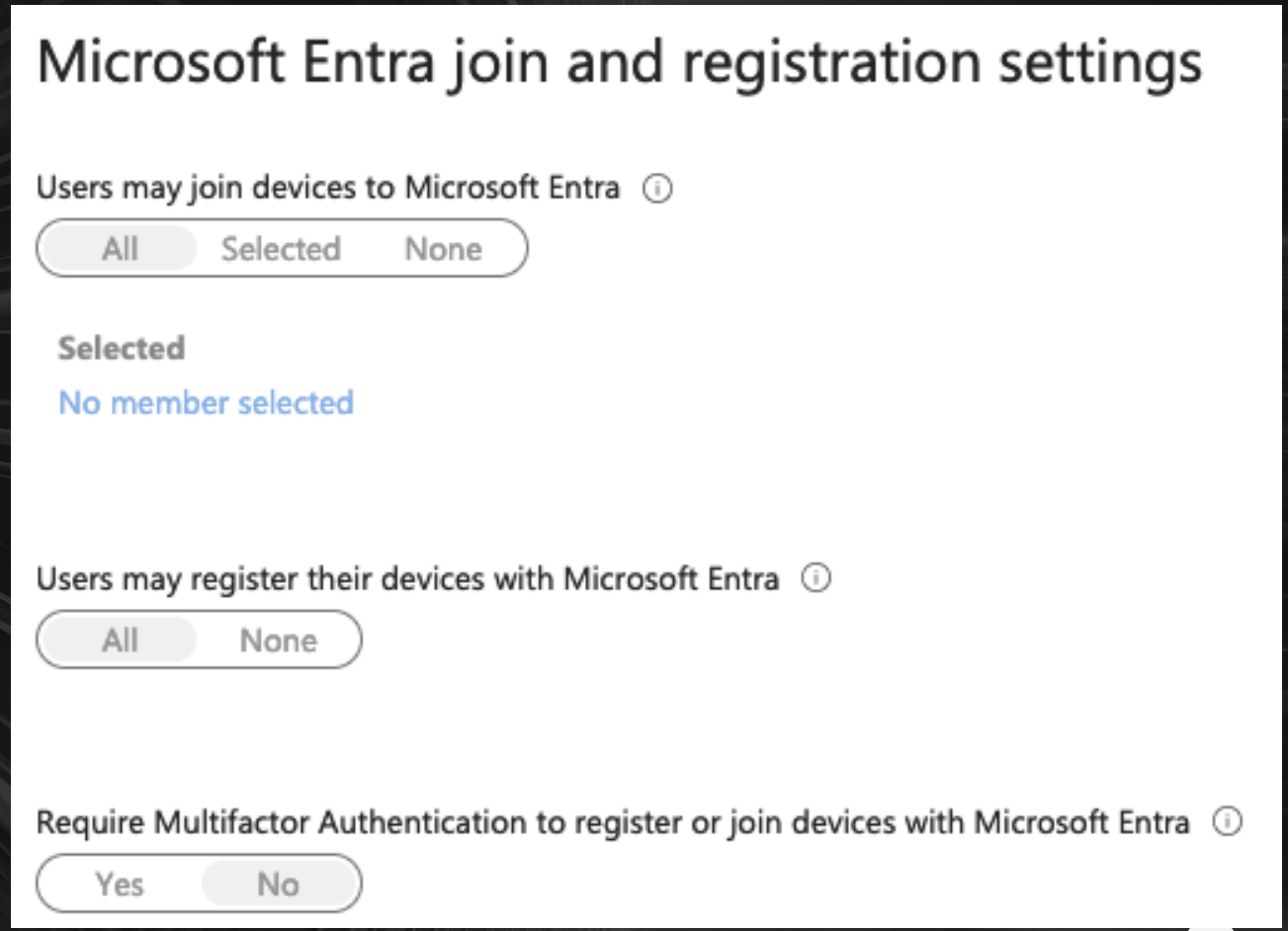
- Following certain sign in flows with our organisation credentials on a device will register or join that device to the Entra domain.

- Registered and Joined devices are different

OS	Version	Join type
Android	10	Microsoft Entra registered
Windows	10.0.22631.4037	Microsoft Entra joined

Abusing the misconfiguration

- Default settings in Entra are insecure
- Any user can register or join any device into the tenant
- WITHOUT MFA!
- Let’s enroll our own Windows VM, using single factor…



Summary

- Once an attacker enrolls their device, with single factor, this CAP allows single factor to all applications.
- Organisations try to reduce the amount of MFA required by their users, by trusting enrolled devices.
- Insecure device enrollment defaults allows an attacker to abuse this policy and gain access.

OS	Version	Join type
Windows	10.0	Microsoft Entra joined

The Fix / Recommendations

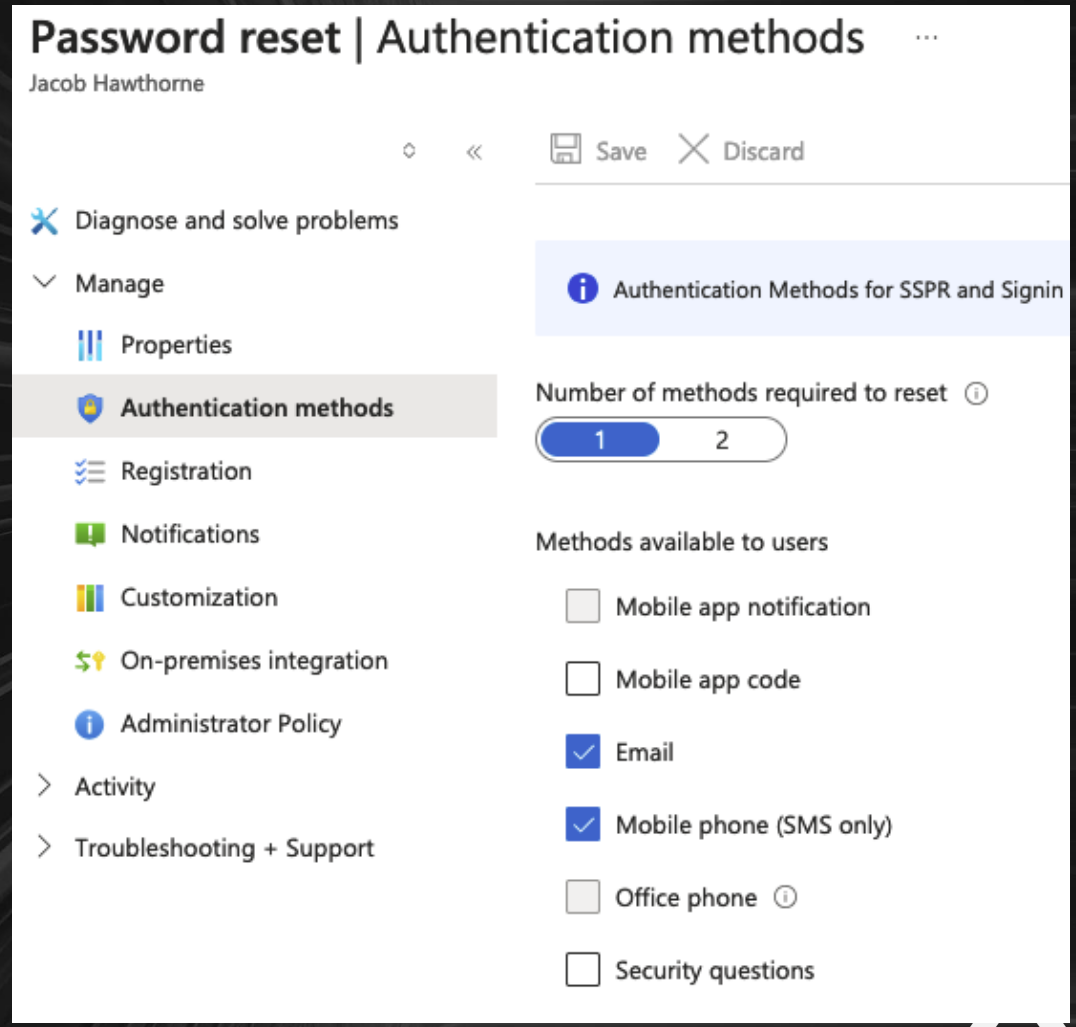
- Ensure the device enrollment defaults are secured
- Don’t use enrolled devices as a second factor

Self-Service Password Reset Bypass

The Configuration

- Organisation wants to allows users to reset their own passwords

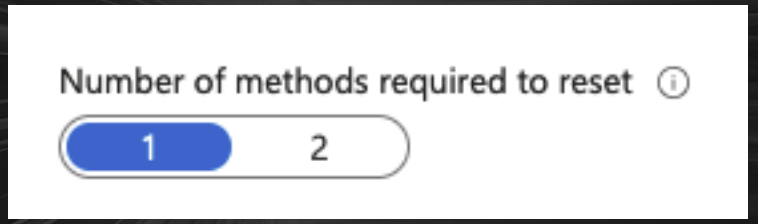
- We create a SSPR policy:
  - Number of methods required to reset: 1
  - Methods available:
    - Email
    - Mobile phone



Abusing the misconfiguration

- The misconfiguration is the requirement of only a single factor to reset a password.

- In this scenario the attacker needs control over the username and email/phone rather than the password.



The Fix / Recommendations

- Ensure the minimum methods required to reset a user’s password is 2
- Use strong methods when resetting a password
  - Mobile app notification
  - Mobile (SMS)

So, what can we do?

Remember it’s allow by default

- Occam’s Razor (adapted) - Sometimes the simplest CAP is the most secure
    - MFA All users, accessing all apps, from any location or device.

Mitigating Phishing

- Use Non phishable methods.
- e.g. WebAuthN, FIDO2

Always use MFA

- It is only going to be prompted for every 30 or 90 days or impossible travel
- Or it is a new device
- Turning it on isn’t really an issue for users

Single Sign On

- Make it a config problem
  - As an org you don't need to worry about implementing in all your apps
- Don’t have to make code changes when detect an issue
- The vendor is understanding all the patterns and keeping up with the new standards and methods

Passwordless/Passkeys

- Extensions to SSO with WebAuthN and device enrolment
- User just needs to touch

Don't Upsell

- If you are a provider don't make SSO or MFA a revenue stream
- https://sso.tax/

The SSO Wall of Shame

A list of vendors that treat single sign-on as a luxury feature, not a core security requirement.

► Why does this exist?

The List

Vendor	Base Pricing	SSO Pricing	% Increase	Source	Date Updated
Adobe Acrobat Pro	$23.99	$27.99	17%	🔗	2023-07-18
Adobe Creative Cloud	$84.99	$140.99	66%	🔗	2023-07-18
Airtable	$10 per u/m	$60 per u/m	500%	🔗 Quote	2019-10-19
Asana	$25 per u/m	$60 per u/m[1]	140%	🔗 Quote	2020-12-09
Atlassian (Jira Cloud)	$7.75 per u/m	$11.75 per u/m[2]	51%	🔗	2023-09-22

Wrapup

Takeaways

- Why you should be using MFA
- How to avoid common MFA mistakes
- How to implement a robust authentication system with MFA

Thanks

- Thanks to organisers for picking this talk and running a great conference
- Thanks to you for attending

Thank You to Our Sponsors and Hosts!

Without them, this Conference couldn't happen.

Questions?