

# MFA, stories that make you go huh?

September 2024

Jacob & David

OWASP NZ Day



# #whoami



- Jacob Hawthorne
- LinkedIn - [/jacob-hawthorne-957920150/](https://www.linkedin.com/in/jacob-hawthorne-957920150/)
- Wellington based
- Offensive Security Consultant
- Specialising in “the Cloud”



# #whoami



- David Robinson
- X - @nzkarit
- Mastodon - [@karit@infosec.exchange](mailto:@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>



HaveIBeenPwned / **PwnedPasswordsDownloader**

Code



Issues

15



Pull requests

2



Actions



Projects



S



**PwnedPasswordsDownloader**

Public



# 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

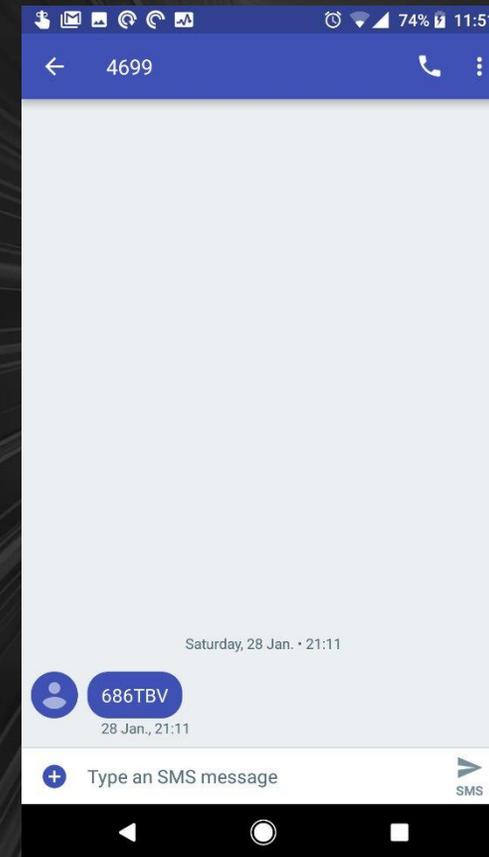
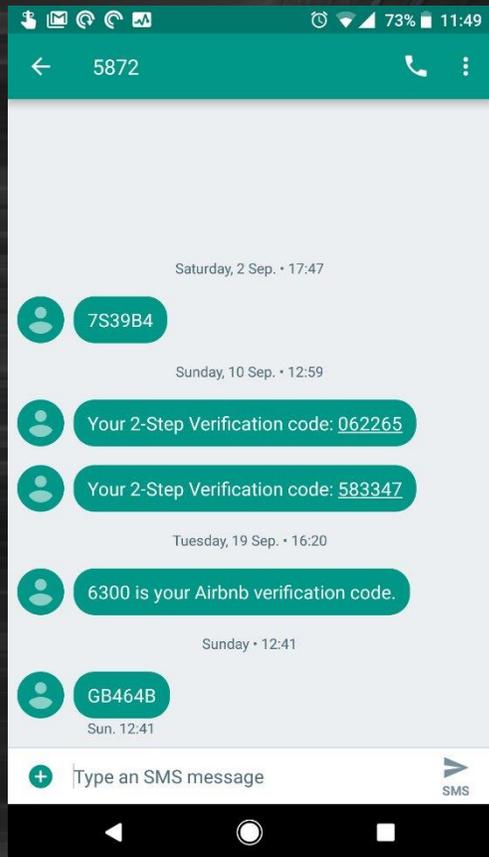


# MFA to the Rescue

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



# SMS



# Battleship Cards

	A	B	C	D	E	F	G
1	C	7	M	4	T	0	1
2	2	Y	2	P	3	H	R
3	E	9	3	8	9	4	N
4	R	C	M	3	6	N	W
5	X	Q	2	V	1	1	C
6	C	9	V	F	1	K	J
7	J	Y	K	W	8	X	D

SN: 260409

For Internet Banking  
Support call freephone  
0800 WWW BNZ  
(0800 999 269)  
or from overseas  
+ 64 4 494 7153

**Entrust**

User Name:

Password:

Entrust IdentityGuard:

**Entrust**

	A	B	C	D	E	F	G	H	I	J	
1	1	F	3	K	3	4	D	5	4	9	1
2	M	2	5	3	R	2	8	4	M	3	2
3	4	E	9	1	K	6	2	Y	0	7	3
4	C	5	2	T	8	5	L	1	7	C	4
5	6	S	6	8	E	7	4	A	8	0	5

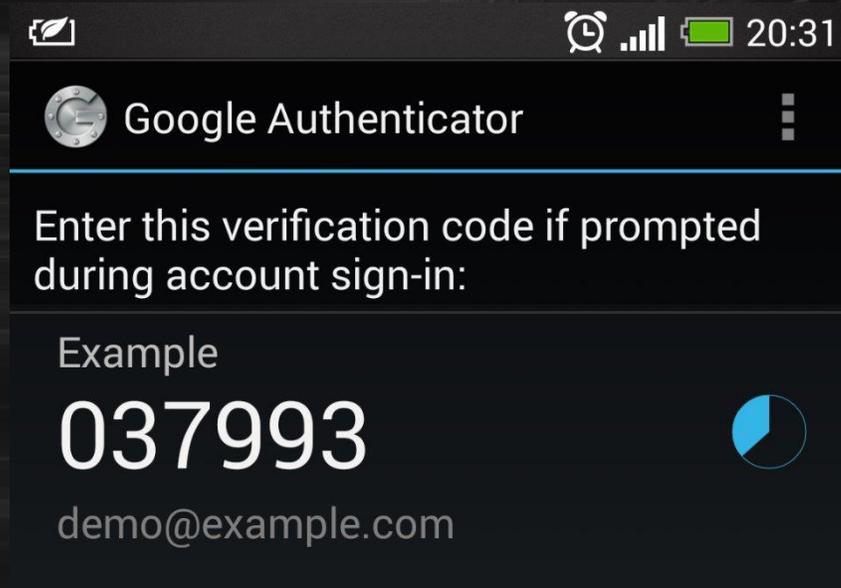
Serial #1234567

[www.entrust.com/demoguard](http://www.entrust.com/demoguard)

© Copyright 2005 Entrust. All rights reserved.



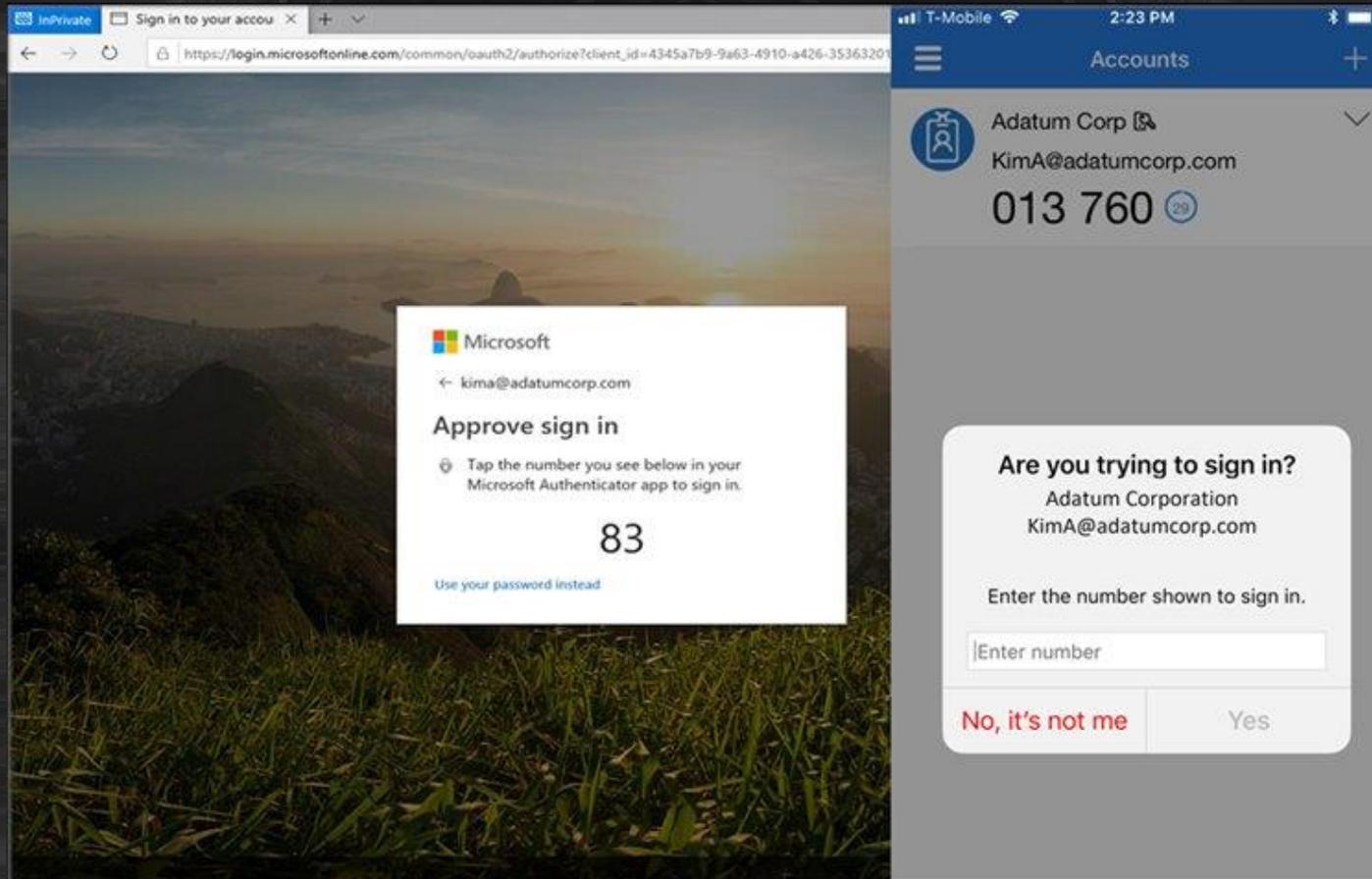
# Time Based One Time Passwords (TOTP)



# Biometrics



# Push Notifications



# Universal Second Factor (U2F)



fido  
CERTIFIED 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)

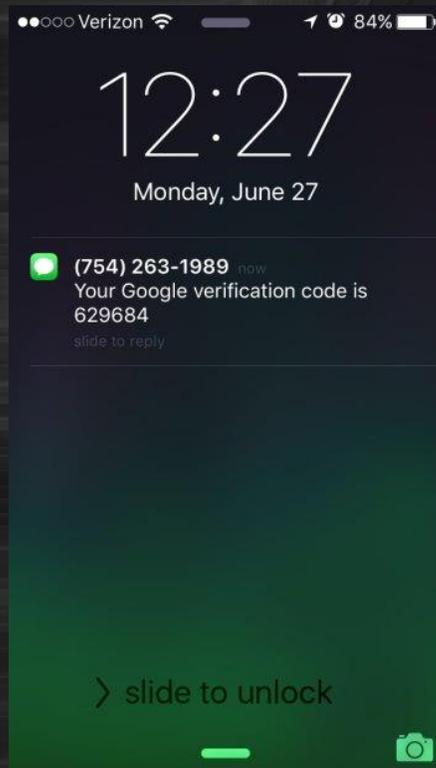


# Telco responsible for your security

- 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

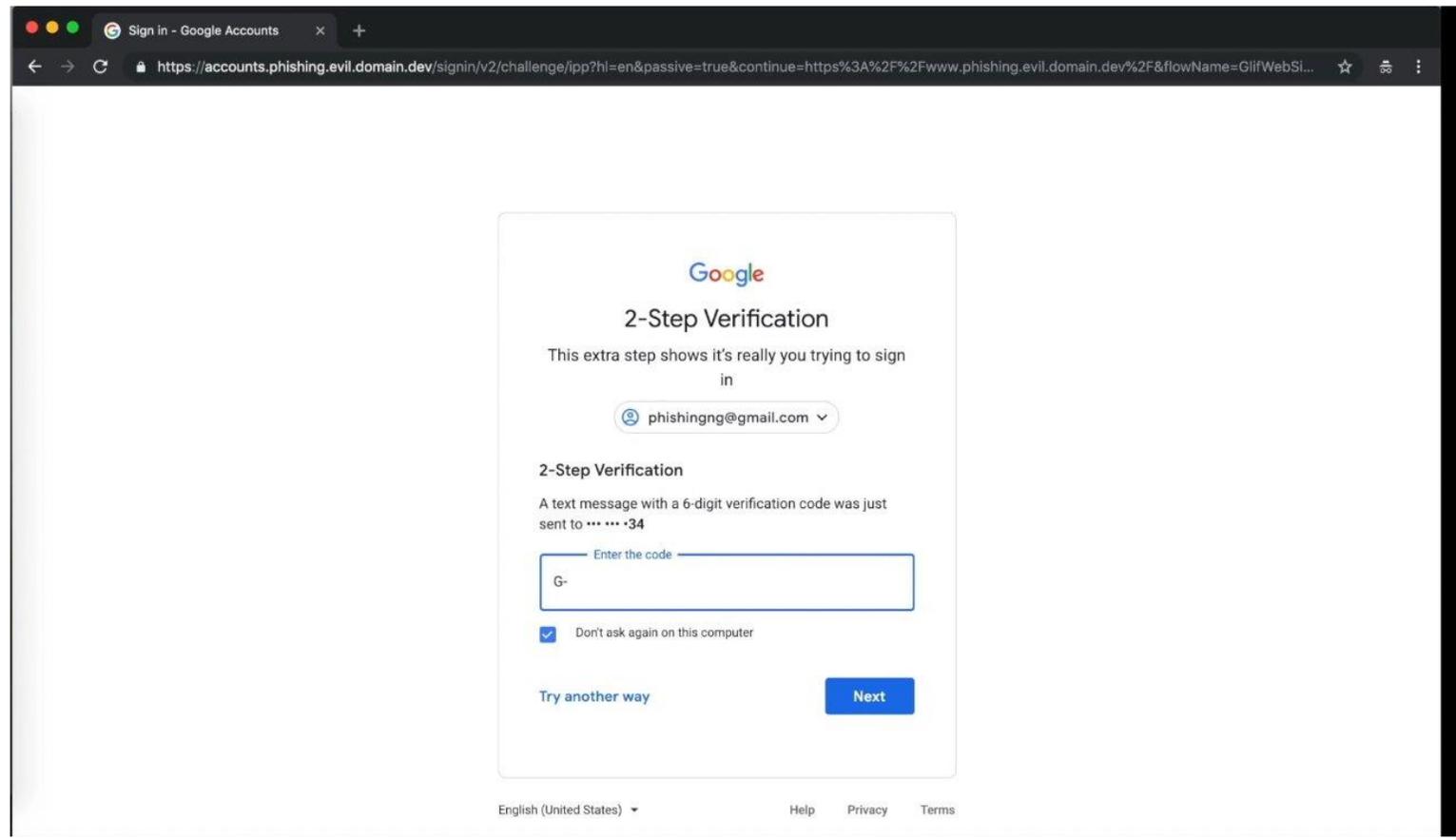


# Phishing 2FA Authentication Tokens

## Proxying In Action (2FA bypass)

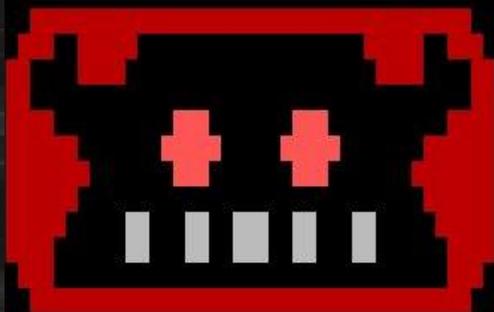
"A picture is worth a thousand words":

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/
```



Evilginx

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-almost-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  
[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)

Recommended Content:

### White Papers: 5 Signs Your Healthcare Network is due

If you're relying on an older network to keep pace with the fast-changing healthcare whitepaper explores the five signs your healthcare network is due for an upgrade.



## 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

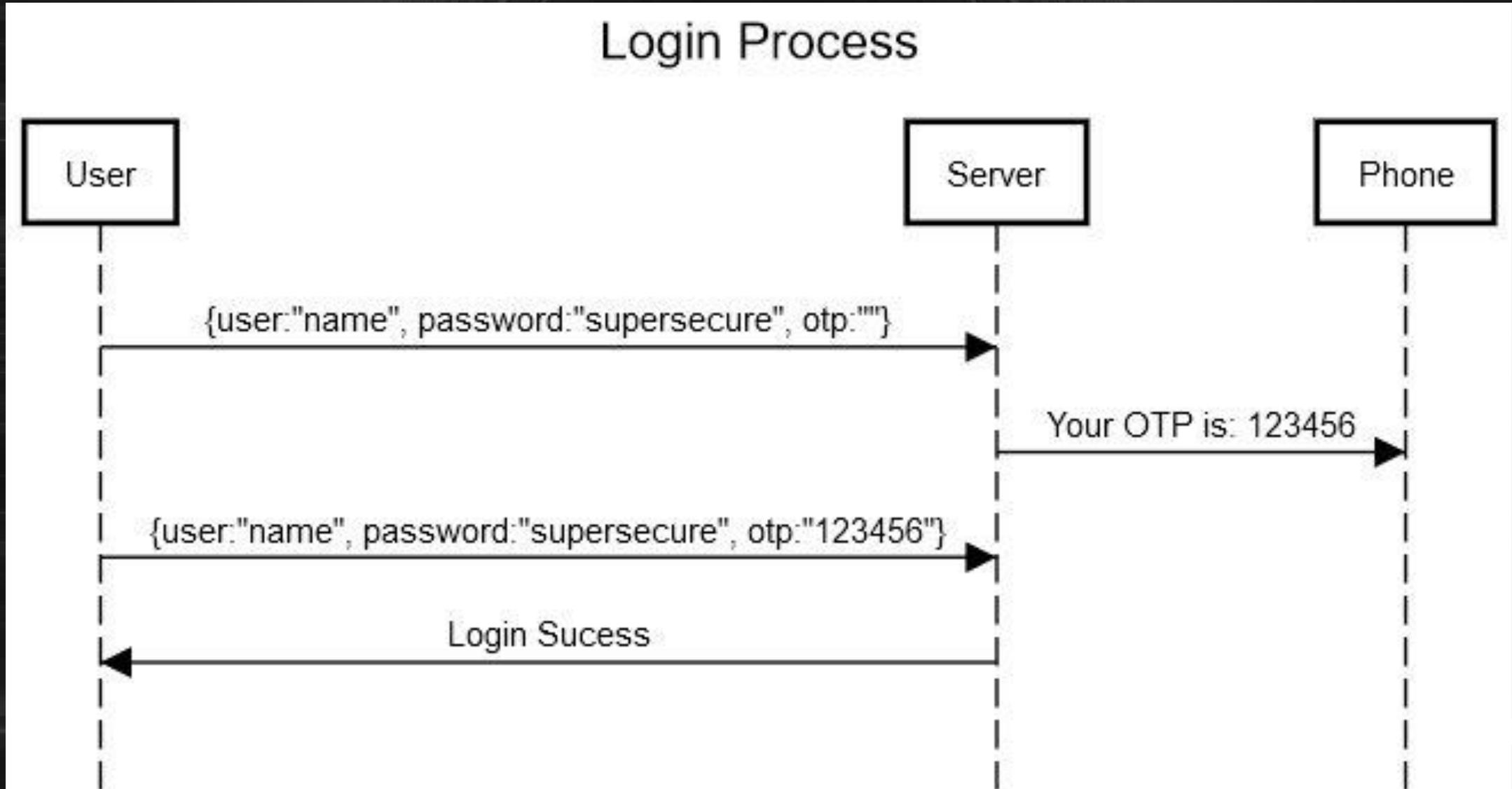


# Only one form or one at time

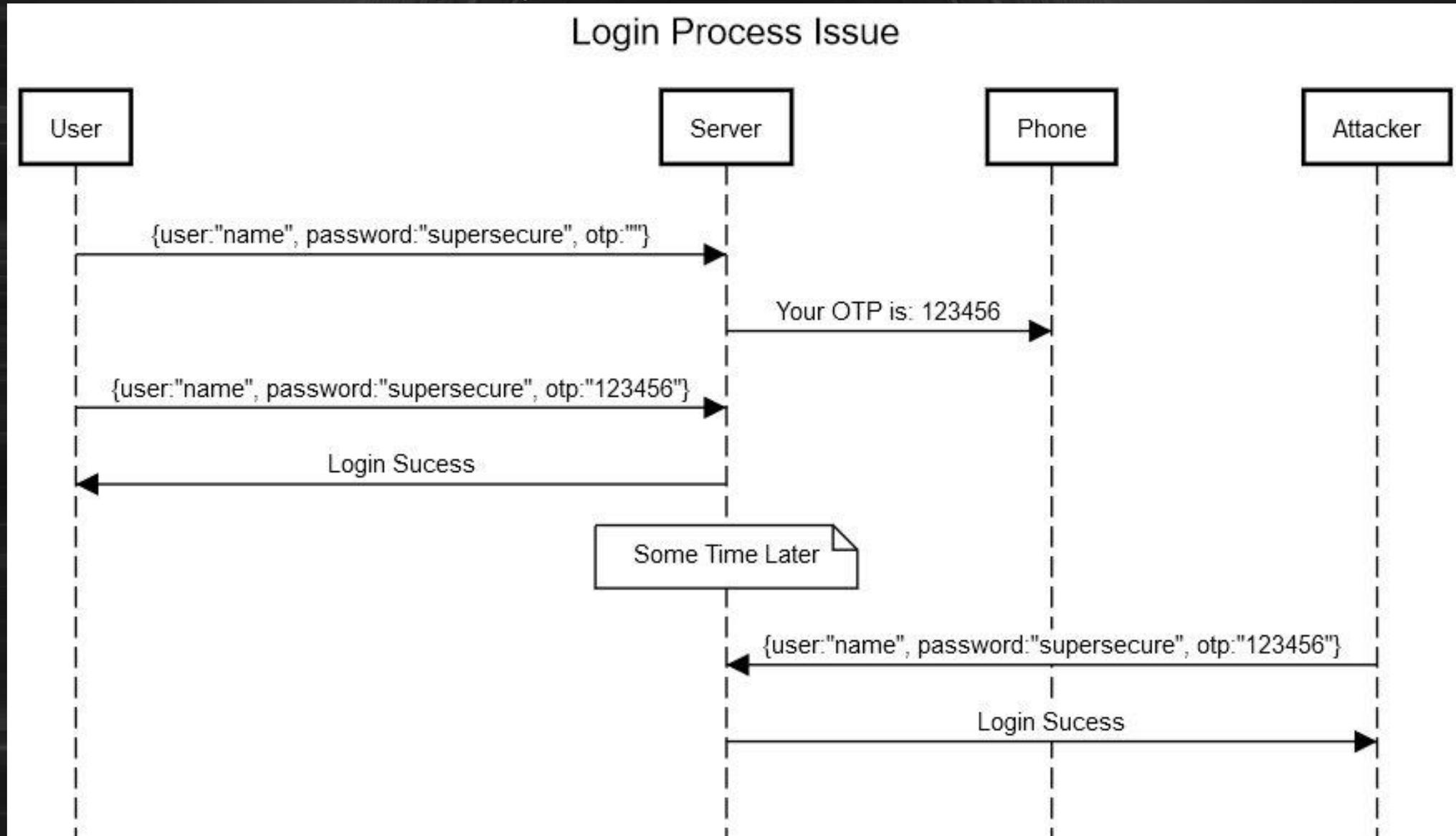
- If want to change MFA type have to disable and then renable
- Can't add two or more tokens, TOTP, etc



# 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

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*  
Example Policy ✓

Assignments

Users ⓘ  
All users

Target resources ⓘ  
All cloud apps

Network **NEW** ⓘ  
Not configured

Conditions ⓘ  
0 conditions selected

Access controls

Grant ⓘ  
1 control selected

Session ⓘ  
0 controls selected

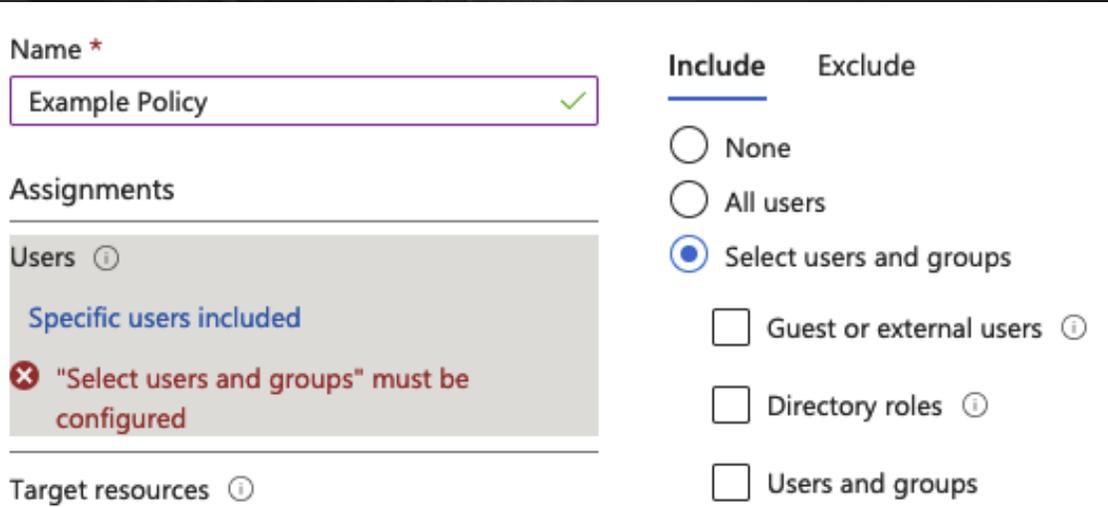
IF

THEN



# The 'IF'

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



Name \*

Example Policy ✓

Assignments

Users ⓘ

[Specific users included](#)

✘ "Select users and groups" must be configured

Target resources ⓘ

**Include**   Exclude

None

All users

Select users and groups

Guest or external users ⓘ

Directory roles ⓘ

Users and groups



# The 'IF'

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

The screenshot shows the configuration page for a Conditional Access policy in Azure AD. The 'Name' field is set to 'Example Policy'. Under 'Assignments', 'Users' is set to 'All users' and 'Target resources' is set to 'All cloud apps'. On the right, the 'Select what this policy applies to' dropdown is set to 'Cloud apps'. Under the 'Include' section, 'All cloud apps' is selected. A warning message at the bottom right states: 'Don't lock yourself out! This policy impacts the Azure portal. Before you'.

Name \*

Example Policy ✓

Assignments

Users ⓘ

All users

Target resources ⓘ

All cloud apps

Select what this policy applies to

Cloud apps

**Include** Exclude

None

All cloud apps

Select apps

⚠ Don't lock yourself out! This policy impacts the Azure portal. Before you



# The 'IF'

- Networks and Locations

[Learn more](#)

**Yes** **No**

**Name \***  
Example Policy ✓

**Assignments**

**Users** ⓘ  
[All users](#)

**Target resources** ⓘ  
[All cloud apps](#)

**Network** **NEW** ⓘ  
[All trusted networks and locations](#)

**Include** **Exclude**

Any network or location  
 All trusted networks and locations  
 All Compliant Network locations  
 Selected networks and locations

**i** To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. [Learn more](#)



# The 'IF'

- Device platforms

The screenshot displays the Microsoft Intune configuration interface. At the top, a blue header reads "All trusted networks and locations". Below this, a "Conditions" section shows "1 condition selected". To the right, a "Device platforms" section is currently "Not configured".

On the right side, a "Device platforms" configuration pane is open. It includes a close button (X) and the instruction "Apply policy to selected device platforms." with a "Learn more" link. Below this is a "Configure" section with a "Yes" button (highlighted in purple) and a "No" button. The "Include" section is active, showing radio button options for "Any device" and "Select device platforms". Under "Select device platforms", there are checkboxes for "Android", "iOS", "Windows Phone", "Windows", "macOS", and "Linux". The "Windows", "macOS", and "Linux" options are checked with blue checkmarks.



# The 'THEN'

- Block access
- Grant access
- Grant access with controls

Access controls

---

Grant ⓘ

1 control selected

---

**Grant** ×

Control access enforcement to block or grant access. [Learn more](#) ↗

Block access

Grant access

Require multifactor authentication ⓘ

Require authentication strength ⓘ

Require device to be marked as compliant ⓘ

Require Microsoft Entra hybrid joined device ⓘ

Require approved client app ⓘ  
[See list of approved client apps](#)

Require app protection policy ⓘ  
[See list of policy protected client apps](#)

Require password change ⓘ

For multiple controls

Require all the selected controls

Require one of the selected 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

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*  
Example Policy ✓

Assignments

Users ⓘ  
All users

Target resources ⓘ  
All cloud apps

Network **NEW** ⓘ  
Not configured

Conditions ⓘ  
0 conditions selected

Access controls

Grant ⓘ  
1 control selected

Session ⓘ  
0 controls selected

IF

THEN





# 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

The screenshot displays the 'Conditional Access policy' configuration page in the Microsoft Entra admin center. The policy is named 'User Agent Bypass' and is assigned to 'All users' and 'All cloud apps'. It includes one condition and one access control. The 'Device platforms' section is expanded, showing that the policy is applied to 'Windows' devices. The 'Device platforms' configuration panel on the right shows the 'Include' section with 'Windows' selected and 'Any device', 'Android', 'iOS', 'Windows Phone', 'macOS', and 'Linux' unselected. The 'Apply policy to selected device platforms' toggle is set to 'Yes'.

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
User Agent Bypass ✓

Assignments

Users ○  
All users

Target resources ○  
All cloud apps

Network | NEW ○  
Not configured

Conditions ○  
1 condition selected

Access controls

Grant ○  
1 control selected

Session ○  
0 controls selected

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ○  
User risk level is the likelihood that the user account is compromised.  
Not configured

Sign-in risk ○  
Sign-in risk level is the likelihood that the sign-in session is compromised.  
Not configured

Insider risk ○  
Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management.  
Not configured

Device platforms ○  
1 included

Locations ○  
Not configured

Client apps ○  
Not configured

Filter for devices ○  
Not configured

Authentication flows (Preview) ○  
Not configured

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure ⓘ  
Yes No

Include Exclude

Any device

Select device platforms

Android

iOS

Windows Phone

Windows

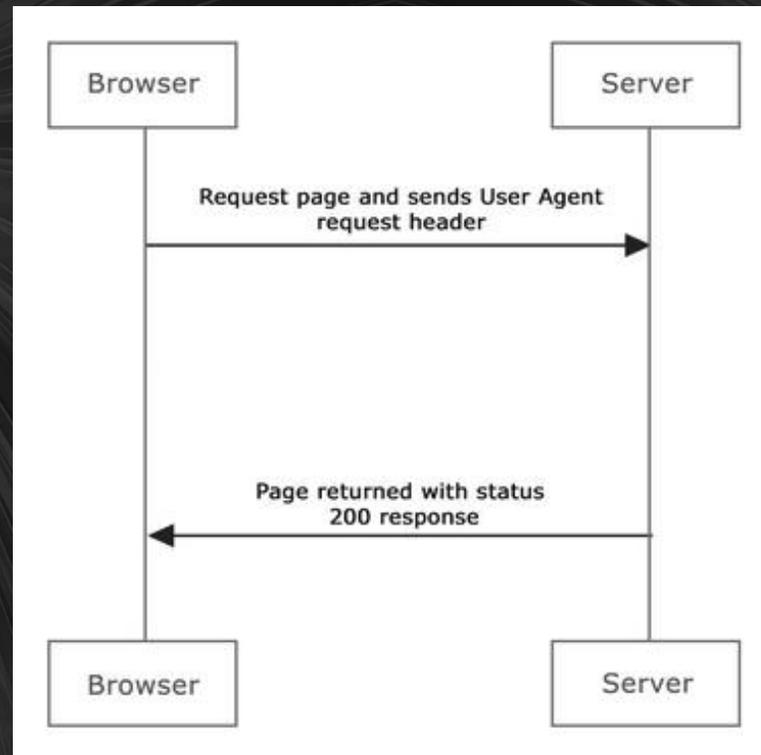
macOS

Linux



# 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
```



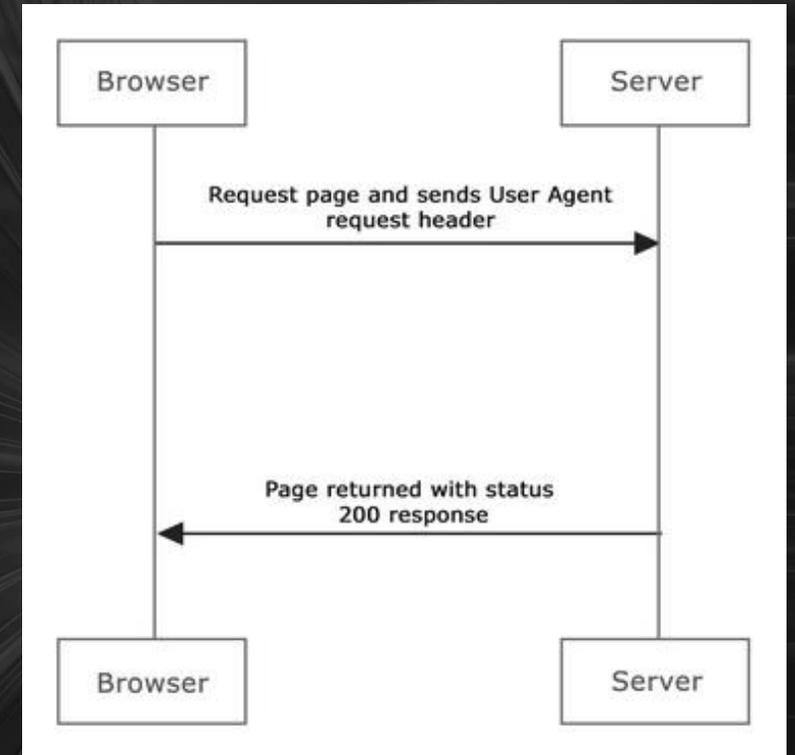
# Abusing the misconfiguration

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

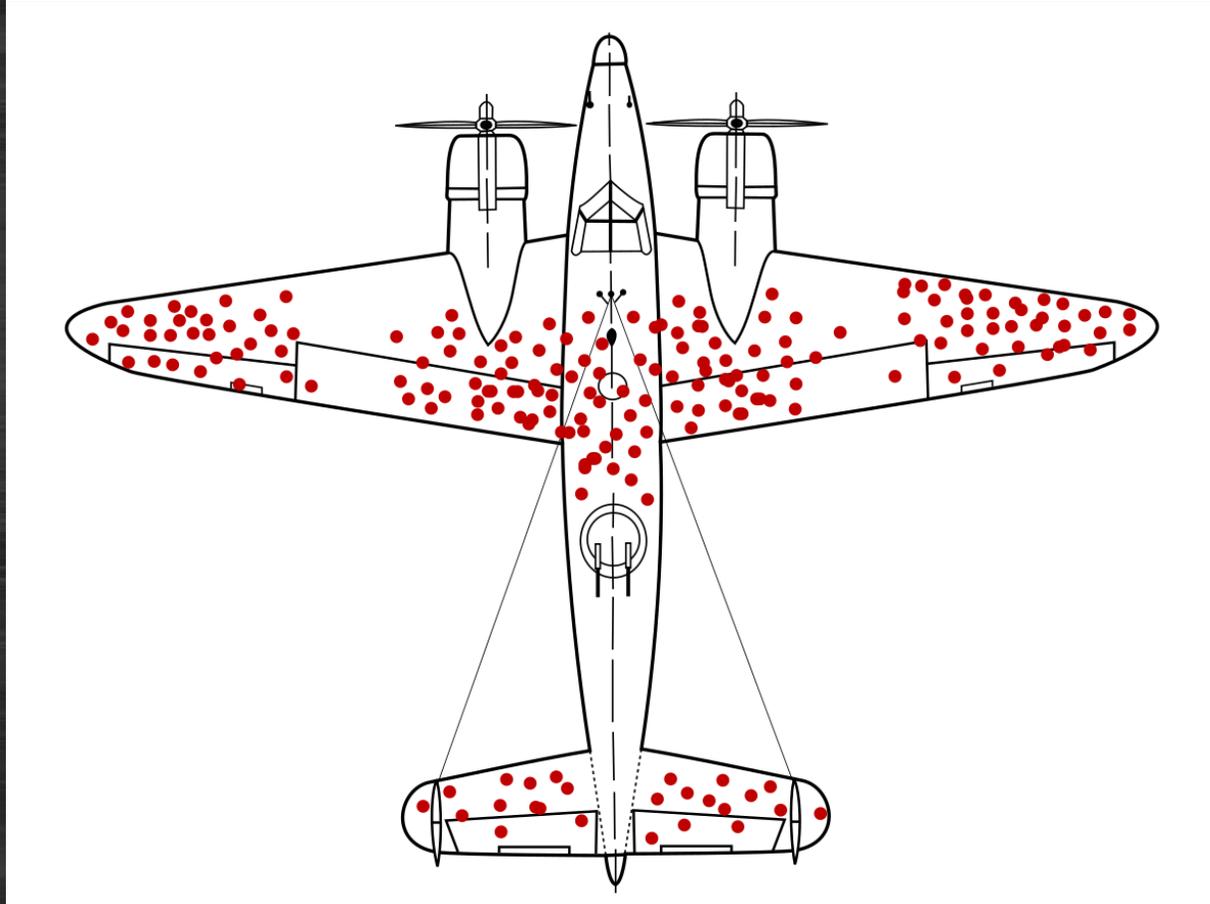
Let's make a change to our "user agent"

- 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 screenshot displays the 'Conditional Access policy' configuration page in Microsoft Entra ID. The policy is named 'User Agent Bypass'. The 'Assignments' section shows it is applied to 'All users' and 'All cloud apps'. The 'Conditions' section shows '1 condition selected'. The 'Access controls' section shows '1 control selected'. The 'Device platforms' section is expanded, showing '1 included' device platform. The 'Device platforms' list includes: Any device, Select device platforms, Android, iOS, Windows Phone, Windows (checked), macOS, and Linux. The 'Apply policy to selected device platforms' section is set to 'Yes'.



# 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

The screenshot shows the configuration page for a Conditional Access policy. The policy name is 'Guest WiFi Bypass'. Under 'Assignments', 'All users' is selected. Under 'Target resources', 'All cloud apps' is selected. Under 'Network', 'Any network or location and 1 excluded' is selected. Under 'Conditions', '1 condition selected' is shown. Under 'Access controls', '1 control selected' is shown. On the right side, the 'Exclude' tab is active, and 'Selected networks and locations' is chosen. The 'Multifactor authentication trusted IPs' control is visible at the bottom right.

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control user access based on their network or physical location. [Learn more](#)

Configure ⓘ

**Yes** No

Name \*  
Guest WiFi Bypass ✓

Assignments

Users ⓘ  
All users

Target resources ⓘ  
All cloud apps

Network **NEW** ⓘ  
Any network or location and 1 excluded

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
1 control selected

Session ⓘ  
0 controls selected

Include **Exclude**

Select the locations to exempt from the policy

All trusted networks and locations

All Compliant Network locations

Selected networks and locations

Select

Multifactor authentication trusted IPs

Multifactor authentication trusted IPs \*\*\*

# 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

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on all or specific network access traffic, cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

**Include** Exclude

None

All cloud apps

Select apps

Edit filter

None

Select

Microsoft Admin Portals

Microsoft Admin Portals

Name \*

Azure Management Bypass

Assignments

Users

All users

Target resources

1 app included

Network **NEW**

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

# Why is this an issue?

- “Microsoft Admin Portals” cloud app, does not cover

## ① Note

The Microsoft Admin Portals app applies to interacting with the underlying resources or services like Microsoft Graph. Those resources are not covered by this application. Those resources are covered by the [Microsoft Management API](#) app. This enables customers to move their automation that relies on APIs and PowerShell to the [Microsoft Management API](#) app. [Administrators performing operations](#)

Sign-ins to the [Microsoft Management API](#) app are not covered by this application. [Administrators performing operations](#) without impacting automation recommends using a [policy requiring](#) [Microsoft Management API](#) app.

## ① Note

When you use the Microsoft Graph API, you agree to the [Microsoft APIs Terms of Use](#) and the [Microsoft Privacy Statement](#).

The [Microsoft Management API](#) application applies to [Azure PowerShell](#), which calls the [Azure Management API](#). This application does not apply to [Microsoft Graph PowerShell](#), which calls the [Microsoft Graph API](#).



# 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 administrative “cloud” apps are included in the policy
  - Microsoft Admin Portals
- Understand the limitations of security defaults – this starting point.
  - Azure Resource Manager
  - Azure Credential Config
  - Azure AD Identity Governance
  - AAD Reporting
- \*\*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

The screenshot shows the configuration page for a new Conditional Access policy named "Trusted Device Bypass". The policy is assigned to "All users" and "All cloud apps". The "Conditions" section shows "1 condition selected". The "Access controls" section shows "1 control selected". The "Filter for devices" section is set to "Include filtered devices". The "Authentication flows (Preview)" section is "Not configured".

The "Filter for devices" section is expanded, showing the configuration for a filter to apply policy to specific devices. The "Configure" toggle is set to "Yes". The "Devices matching the rule" section shows "Exclude filtered devices from policy" selected. The filter rule is configured as follows:

And/Or	Property	Operator	Value
And	TrustType	Equals	Microsoft Entra registered
And	trustType	Equals	Microsoft Entra joined

The rule syntax is displayed as: `device.trustType -eq "Workplace" -and device.trustType -eq "AzureAD"`



# How does our CAP know if our device is enrolled?

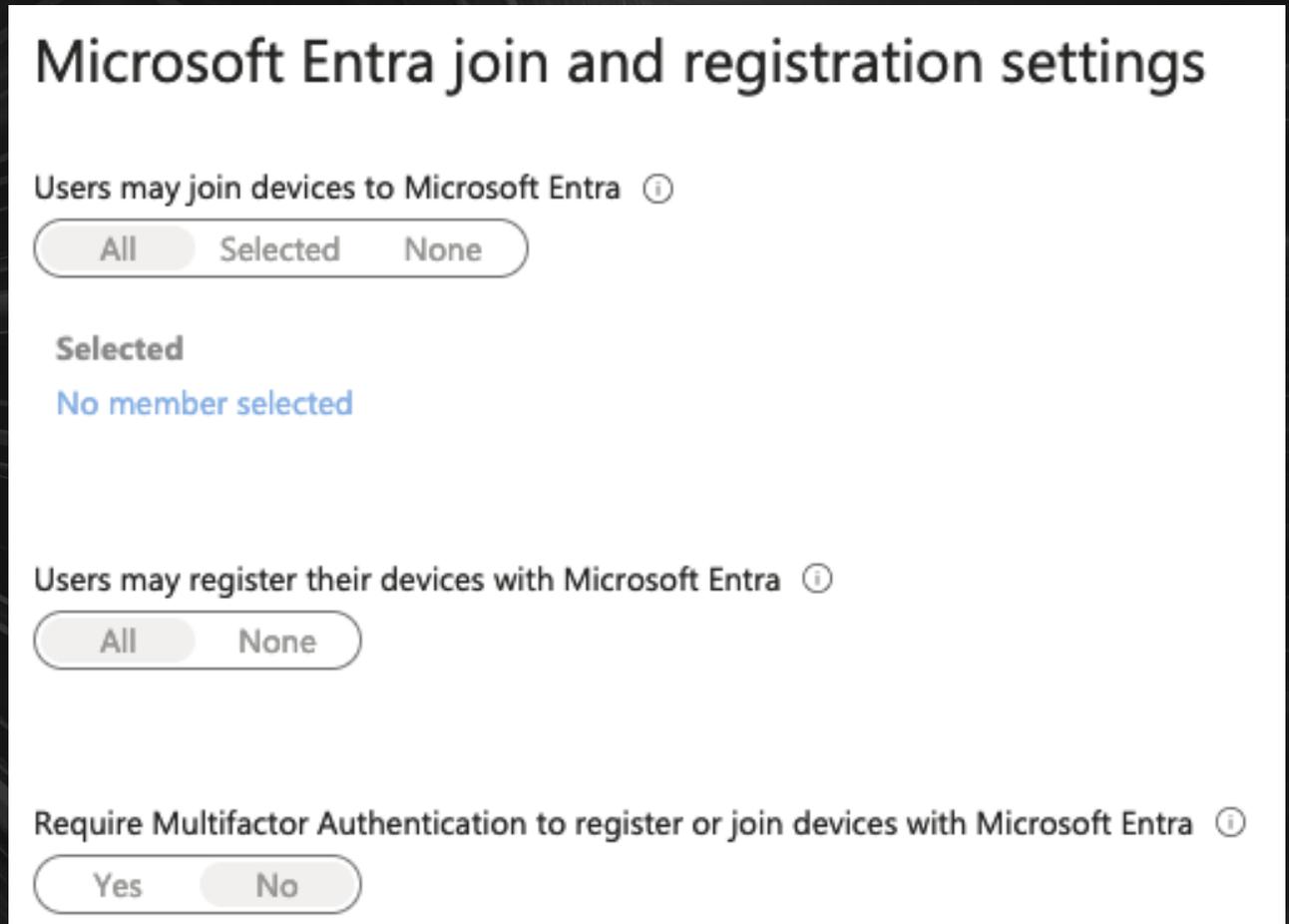
- Following certain sign in flows with our organisation credentials on a device will register or join that device to the Entra domain.
- Registered and Joined devices are different

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...



The screenshot shows the 'Microsoft Entra join and registration settings' interface. It contains three sections, each with an information icon (i) to its right:

- Users may join devices to Microsoft Entra**: A radio button group with three options: 'All' (selected), 'Selected', and 'None'.
- Selected**: A sub-section with the text 'No member selected' in blue.
- Users may register their devices with Microsoft Entra**: A radio button group with two options: 'All' (selected) and 'None'.
- Require Multifactor Authentication to register or join devices with Microsoft Entra**: A radio button group with two options: 'Yes' and 'No' (selected).

# 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 allow users to reset their own passwords
- We create a SSPR policy:
  - Number of methods required to reset: 1
  - Methods available:
    - Email
    - Mobile phone

**Password reset | Authentication methods** ...

Jacob Hawthorne

Save Discard

- Diagnose and solve problems
- Manage
  - Properties
  - Authentication methods**
  - Registration
  - Notifications
  - Customization
  - On-premises integration
  - Administrator Policy
- Activity
- Troubleshooting + Support

**Authentication Methods for SSPR and Signin**

Number of methods required to reset ⓘ

1 2

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone (SMS only)
- Office phone ⓘ
- Security questions

# 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.

Number of methods required to reset ⓘ

1

2



# 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
<a href="#">Adobe Acrobat Pro</a>	\$23.99	\$27.99	17%	<a href="#">🔗</a>	2023-07-18
<a href="#">Adobe Creative Cloud</a>	\$84.99	\$140.99	66%	<a href="#">🔗</a>	2023-07-18
<a href="#">Airtable</a>	\$10 per u/m	\$60 per u/m	500%	<a href="#">🔗</a> Quote	2019-10-19
<a href="#">Asana</a>	\$25 per u/m	\$60 per u/m <sup>1</sup>	140%	<a href="#">🔗</a> Quote	2020-12-09
<a href="#">Atlassian (Jira Cloud)</a>	\$7.75 per u/m	\$11.75 per u/m <sup>2</sup>	51%	<a href="#">🔗</a>	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

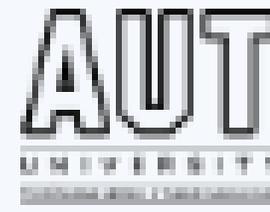


# Thanks

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



Thank You to Our Sponsors and Hosts!



# BASTION

SECURITY GROUP



DATACOM



PentesterLab

plexure



Without them, this Conference couldn't happen.

Questions?

