When authn breaks: Real world failures

BSidesSeattle 2025 | Apr 18, 2025

Maya Kaczorowski

Maya Kaczorowski

Founder

OBLIQUE

Agenda

- Types of authentication failures
- Real world failures
- Common vulns in authn protocols
- Avoiding & mitigating issues

Kinds of authn failures

Authentication failures

Credential compromise

MFA & recovery

Session management

Authentication protocols

Infrastructure

Authentication failures

~~Credential compromise~~ No MFA

MFA & recovery

Session management

Authentication protocols

Infrastructure

The last 5 years of authn failures

Jul 2020

Twitter account hijacking

Twitter employees phished

- Widespread internal access to admin tool
- Scraped LinkedIn for employees and their phone numbers
- Pretended to be IT & contacted employees to log in to portal & share 2FA code

Impact: ~45 accounts promoted Bitcoin scam, netting ~$120k

https://en.wikipedia.org/wiki/2020_Twitter_account_hijacking

Jun 2021

Azure AD Seamless Sign-on

Brute-force attacks without sign-in logs

Impact: None

- Seamless Single Sign-On features automatically logs users into AD if their device is joined to the tenant
- Returns error code if the login fails, confirming a user exists
- No logging or rate limiting on these sign-on attempts

https://www.secureworks.com/research/undetected-azure-active-directory-brute-force-attacks

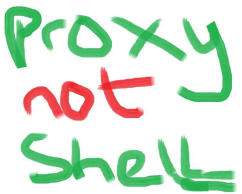
Sep 2021

ProxyShell

Microsoft Exchange auth bypass
CVE-2021-34473

Impact: 10k+ Exchange servers

- Issue with URL normalization in “Explicit Logon” feature to directly link to a user’s inbox
- Chained 3 vulns to bypass auth on Exchange servers to get RCE
- These patches were still vulnerable to SSRF



https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell

Jan 2022

Okta LAPSUS$

Compromise of third party support engineer's laptop

Impact: access to 366 Okta tenants

- Disclosed on Twitter, in screenshots from LAPSUS$, months after the breach
- Probably stolen creds
- Okta called it an "unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider"

https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/

Mar 2022

GitLab static passwords

Hardcoded passwords for certain auth providers
CVE-2022-1162

Impact: None

- When registering a user account, a password was also automatically generated
- Passwords followed a predictable pattern

https://about.gitlab.com/releases/2022/03/31/critical-security-release-gitlab-14-9-2-released/

Apr 2022

GitHub OAuth token theft

Heroku & TravisCI

Impact: copying private repos & downloading npm packages

- GitHub OAuth tokens issues to Heroku and Travis CI compromised
- Enumerated users' organizations and repos, including copying private repositories
- Compromised npm infra, including private packages

https://github.blog/news-insights/company-news/security-alert-stolen-oauth-user-tokens/

May 2022

Cisco VPN MFA bypass

Corp password synced to personal account

Impact: Access to Cisco corp IT

- Cisco employee synced password to personal Google Chrome profile
- After compromising personal account, brute forced MFA bypass: vishing & MFA fatigue
- Successfully enrolled their own MFA devices
- Escalated to admin privileges

https://blog.talosintelligence.com/recent-cyber-attack/

Sep 2022

Uber MFA fatigue

External contractor VPN account compromised

- LAPSUS$, again
- Bought external contractor VPN credentials on dark web
- MFA fatigue
- Reached out to contractor on WhatsApp posing as IT
- Gained access to Uber's internal systems

Impact: elevated permissions to internal Uber systems

https://www.uber.com/newsroom/security-update/

Oct 2022

FortiOS firewall

Auth bypass to admin interface
CVE-2022-40684

Impact: Was exploited

- FortiOS (firewall) and FortiProxy (web proxy) vulnerable to auth bypass
- HTTP/S request to gain access to admin interface
- Exploited to add malicious super admin account **`fortigate-tech-support`**

https://www.fortiguard.com/psirt/FG-IR-22-377

Oct 2022

LastPass

Eng credentials used to access dev environment

- First incident: engineer's work laptop, with creds for dev environment
- Second incident: engineer's home computer, with access to master LastPass vault
- Accessed backups including API keys, encrypted user vaults, MFA database

Impact: users' password vaults, including bitcoin wallet creds

https://blog.lastpass.com/posts/security-incident-update-recommended-actions

Jan 2023

CircleCI AWS tokens

Employee cookie theft

- Malware on an engineer's laptop used to steal a "valid, 2FA-backed SSO session"
- Generated prod access tokens
- Stole customer environment variables, tokens, and keys

Impact: OAuth tokens, API keys, & other secrets compromised

https://circleci.com/blog/jan-4-2023-incident-report/

Oct 2023

Okta support system

Compromised support employee's credentials

Impact: 5 customers with hijacked Okta sessions

- Customer support employee's account saved to personal Chrome profile
- Stole valid session tokens from support tickets
- 1Password reported the issue to Okta first
- Downloaded a report of all of Okta's customers

https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause/

Nov 2024

Okta bcrypt

Checked partial password

Impact: Okta's reputation

- Used bcrypt (which limits input size) to hash `userId + username + password`
- Okta usernames with more than 52 characters didn't check passwords
- User could log in with username and previously stored cache key

https://trust.okta.com/security-advisories/okta-ad-ldap-delegated-authentication-username/

Sep 2024

Snowflake customers

Credential stuffing accounts with no MFA

- Stolen credentials obtained via infostealer malware
- Authenticated to accounts with no MFA
- Leaked or collected ransoms for stolen data

Impact: 165+ Snowflake customers, including AT&T

https://www.404media.co/the-walls-are-closing-in-on-the-snowflake-hacker/

Examples we discussed

Credential compromise i.e. **no MFA**	Okta LAPSUS$, Okta support system, Snowflake customers
MFA & recovery	Twitter, Cisco VPN, Uber
Session management	GitHub OAuth, CircleCI
Authentication protocol	Azure AD Seamless Sign-on, ProxyShell, GitLab static passwords, FortiOS, Okta bcrypt
Infrastructure	n/a

Vulns in authn protocols

Authentication protocol failures

JWT validation	No verification of signature algorithm or allow `none`
OAuth state parameters	Missing or improperly validated state parameters allow for CSRF
OIDC ID tokens	Missing or improperly validated `aud` claim in `id_token`
SAML signature wrapping	Only validating the XML document signature

Check out this talk: https://www.youtube.com/watch?v=yX8hyMmoVMo

Lessons learned

Lessons learned: implementing auth

- Check for common implementation mistakes
- Use the right algorithms
- Implement session timeouts
- Prevent brute force attacks
- Provide users with more than basic auth: MFA

Implement phishing-resistant MFA

Lessons learned: using auth

- Implement MFA
- Require strong MFA
- Educate users on MFA fatigue
- Alert on MFA events
- Rotate OAuth tokens
- Provide a corporate password manager
- Pay attention to support employee auth

Authentication will fail

Compensating controls

- Defense in depth
- Network segmentation
- Proper authorization
- Strong authorization

Respond to compromise

- Logging
- Monitoring
- Invalidate sessions
- Rotate credentials
- Communicate

Thank you

Get the slides: https://tinyurl.com/authn-failures

More resources

- BSidesSF talk on insecurity protocols: https://www.youtube.com/watch?v=yX8hyMmoVMo
- BSidesSF talk on LAPSUS$ playbook: https://www.youtube.com/watch?v=9wpBaXcXQSM