

Patterns of failure in modern authz

Daniel “*phrawzty*” Maher
Sr. DevRel Manager; Cerbos

OWASP™

SNOWFROC 2025

Context: About Me

- Recovering system administrator
- Secretly French (🤫 don't tell anybody)
- Frequently ate lunch with the security folks at Datadog
- Oh! I work at a start-up called Cerbos

Context: About Cerbos

- *"Externalized, policy-based, runtime authorization for your applications"*
- It's literally a self-hosted binary with an HTTP API
- There's also a hub with a bunch of neat features



What is Authorization?

» *"Is this entity allowed to perform this action on this resource?"*

» Related to, but distinct from, authentication

Early Days: POSIX Permissions

- User/Group/World model
- Read/Write/Execute primitives

The Middle Ages: ACLs & RBAC

» Access Control Lists

» Role-Based Access Control frameworks

Modern Authorization

- Token-based approaches (JWT, OIDC)
- Federated systems
- PBAC, ABAC, ReBAC...

When it all goes wrong

(and it will)

Facebook "Privacy bug"

Overview

- 📅 May 2018
- Audience selector default changed to public
- 14 million users affected
- Policy enforcement failure during feature update

Facebook "Privacy bug"

Key Authorization Failures

- Default permission setting changed without user consent
- Policy enforcement layer failed during UI update
- Inadequate permission state validation

Okta "Support System breach"

Overview

- 📅 2023
- HAR file exfiltration exposed session tokens
- Auth bypasses in support systems

Okta "Support System breach"

Key Authorization Failures

- Overly permissive access to production
- Insufficient isolation between support tiers
- Authorization checks bypassed through session token theft
- Inadequate token validation controls

Microsoft "Midnight Blizzard"

Overview

- 📅 2024
- Password spray attack led to tenant compromise
- Legacy tenants, basic auth, and privilege escalation

Microsoft "Midnight Blizzard"

Key Authorization Failures

- Excessive privileges in legacy tenant configurations
- Inadequate role separation
- Authorization boundaries between tenants insufficiently enforced
- Lack of just-in-time access controls for privileged operations

How to stop it from all going wrong

(or at least give yourself a fighting chance)

Token Security

- Validation best practices (signature, expiry, issuer)
- Secure storage and transport
- Avoiding common token vulnerabilities

Permission Management

- Role explosion 💥
- Just-in-time access patterns
- Principle of least privilege

Externalizing Authorization

- Clear separation between business logic and authz rules
- Update policies without updating code
- Enhanced auditability and compliance reporting

Testing Authorization Systems

- Policy unit testing
- Automated access review

Critical Path Patterns

- High-availability authorization
- Graceful degradation strategies
- When in doubt, deny by default

Conclusion

- Authorization fails at boundaries and transitions
- *Externalize your authorization decisions*
- Tokens require rigorous validation
- Use just-in-time access and live the principle of least privilege
- Test continuously and review access regularly



← play this game!

(no really, it's fun)