

The background features white circuit board patterns in the corners, consisting of various lines, dots, and circular shapes representing components and traces.

# Reimagining Authentication: Modern Security Practices for Enterprise Applications

Why authentication and authorization is no longer a  
nice-to-have, but imperative

Julian Lyndon-Smith

# The Security Landscape

- 80% of breaches involve stolen/weak credentials (Verizon DBIR)
- \$4.45M average breach cost (IBM Report, 2023)
- Attackers automate credential stuffing
- Breaches are routine headlines

# It's Not Just the Other Guy

- Okta breach (2023) – MFA provider hacked
- Uber (2022) – MFA fatigue attack
- Colonial Pipeline (2021) – VPN creds stolen
- Breaches now happen weekly

# It's Not Just the Other Guy

03:52  
Cyber-crime News • The Register - Google Chrome

theregister.com/security/cyber\_crime/

Build.One | Inbox | Slack | BBC | The Register | OSNews | Ars Technica | 9to5Google | Electrek | The New Sta... | Boston | Google Mes... | Gemini | The Stack | HP OfficeJet... | Suno | Download a... | All Bookmarks

SIGN IN / UP The Register

No coach asks for only 55%  
Keep PCs at max performance when unplugged. [See how](#)

## CYBER-CRIME

**One line of malicious npm code led to massive Postmark email helix**  
MCP plus open source plus typosquatting equals trouble  
CYBER-CRIME 6 hrs | 2

**Asahi runs dry as online attackers take down Japanese brewer**  
No personal info gulped as yet, but don't call for help  
CYBER-CRIME 6 hrs | 4

**Harrods blames its supplier after crims steal 430k customers' data in fresh attack**  
Attackers make contact but negotiations fall on deaf ears  
CYBER-CRIME 16 hrs | 11

**Jaguar Land Rover gets £1.5B government jump-start after cyber breakdown**  
Hundreds of thousands of workers in financial despair supported with landmark loan  
CYBER-CRIME 17 hrs | 28

55% performance won't cut it  
Keep max PC performance when unplugged. [See how](#)

**Salesforce facing multiple lawsuits after Salesloft breach**  
UPDATED CRM giant denies security shortcomings as claims allege stolen data used for ID theft  
CYBER-CRIME 3 days | 9

**LockBit's new variant is 'most dangerous yet,' hitting Windows, Linux and VMware ESXi**  
Operator Cronos didn't kill LockBit - 6 just came back meaner  
CYBER-CRIME 4 days | 48

**Volvo North America confirms staff data stolen following ransomware attack on IT supplier**  
The downstream consequences of Mirai's ransomware attack continue to affect major organizations  
CYBER-CRIME 4 days | 5

**UK and US security agencies order urgent fixes as Cisco firewall bugs exploited in wild**  
CISA gives feds 24 hours to patch, NCSC urges rapid action as flaws linked to ArcaneDoor spies  
PATCHES 4 days | 13

# Authentication



# Authentication Fatigue is Real

- Too many logins frustrate users
- Developers reinvent auth wheels repeatedly
- CIOs dread compliance failures
- Attackers exploit weakest links

# Why This Matters Now

- Regulations: GDPR, PCI-DSS, HIPAA
- Cloud-native & microservices expansion
- Cyber insurance mandates MFA
- Security now = survival, not luxury

# Hard-Coded Passwords

- Database creds in config files
- API keys in GitHub repos
- Secrets shared in Slack/Teams
- Impossible to rotate safely

# Default Credentials

- Common defaults: admin/admin, root/toor
- Exploited by Mirai botnet (2016)
- Still common in IoT devices
- Disable defaults in audits

# Shared Accounts

- Everyone logs in as 'admin'
- No individual accountability
- Audit logs are meaningless
- Revoking access is difficult

# Password Reuse

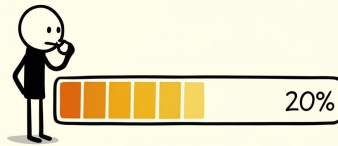
- Common across work and personal accounts
- Credential stuffing automation at scale
- 65% of users admit reusing passwords
- One breach compromises many services

# Password Policies: The Wrong Fight

- Forced resets frustrate users
- XKCD 936: correct horse battery staple
- Complexity  $\neq$  security
- Attackers bypass policies easily

# Password Policies: The Wrong Fight

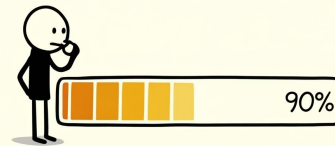
TRADITIONAL  
PASSWORD STRENGTH



Tr0ub4dor&3

Upper and lower case, numbers, symbols... but it's one word with substitutions, so it's guessable

XKCD #936:  
PASSWORD STRENGTH



correcthorsebatterystaple

Four common words concatenated.  
Hard to guess, easy to remember



# Password Policies: The Wrong Fight

- A password using any word , or combination of words has already been compromised
- Still bad advice out there - this was written in January 2025 (<https://www.defendedsolutions.com/defended-solutions-blog/a-guide-to-passwords-the-3-random-word-system>)
-

# Breach Costs

- Downtime, fines, brand damage
- Colonial Pipeline paid \$5M ransom
- Equifax settlement: \$700M
- Costs rising every year

# Equifax Breach

- Vulnerability discovered in Apache Struts March. Patched same day
- Equifax were aware , and instructed to apply patch
- Due to internal process failures, the patch was not applied to all of Equifax's vulnerable systems.
- 2 months later Equifax was exploited

# Takeaway: Passwords Broken

- Passwords alone are broken
- Breach costs are skyrocketing
- Regulators losing patience
- It's time to evolve

# SSO Benefits

- One login for many apps
- Stronger centralised policies
- Reduced credential sprawl
- Happier, more productive users

# SSO in Action

- Microsoft Entra ID (Azure AD)
- Okta for enterprise SaaS
- Google Workspace federation
- Industry adoption across sectors

# When SSO Goes Wrong

- Okta breach centralised risk
- Vendor dependency is high
- One compromise = many systems
- Centralised failure possible

# Multi-Factor Authentication

- SMS (weak, prone to SIM swap)
- Authenticator apps (better)
- Hardware keys (best)
- NIST guidance: avoid SMS

# MFA Fatigue

- Uber breach: MFA bombing
- Users overwhelmed by prompts
- Attackers exploit human behaviour
- Adaptive auth reduces fatigue

# Passwordless Authentication

- WebAuthn standards
- Passkeys across devices
- Hardware keys like YubiKey
- Adoption by Apple, Google, Microsoft

# Federated Identity

- Trust established between providers
- SAML for legacy systems
- OAuth2 for delegated access
- OIDC for modern identity

# Delegated Access (OAuth)

- OAuth scopes grant granular access
- Users often over-authorise
- Example: full Google Drive access
- Careful scope design = safer apps

# Centralised vs Decentralised Identity

- Centralised IdPs practical today
- Decentralised (DID/SSI) emerging
- Promises stronger user control
- Still maturing, watch closely

# Modern Auth Takeaway

- Passwords ≠ modern security
- SSO + MFA reduce risk
- Passwordless improves UX + security
- Balance centralisation with resilience

# Secrets



# Why Secrets Management?

- API keys, DB creds, TLS certs = prime targets
- Attackers actively scan repos
- Insider risk reduced with proper tools
- Compliance requires proper handling

# Bad Practices with Secrets

- .env files in repos
- Keys in Docker images
- Credentials in Jira/Confluence
- 'Private' repos aren't safe

# Secrets Management Tools

- HashiCorp Vault / OpenBao
- AWS Secrets Manager
- Azure Key Vault
- Google Secret Manager

# Key Rotation Importance

- Stale creds = goldmine for attackers
- Frequent rotation limits blast radius
- Automate rotation with pipelines
- Rotating keys shortens the window for cracking a key

# Secrets in CI/CD

- Inject secrets at runtime
- Avoid commit history leaks
- Use pipeline integrations
- Prevent developer exposure

# Secrets Takeaway

- Secrets are like uranium: dangerous if mishandled
- Never store in code or tickets
- Automate storage and rotation
- Integrate into development lifecycle

# Authorization



# AuthN vs AuthZ

- AuthN = verifying who you are
- AuthZ = deciding what you can do
- Both are essential
- Don't confuse them (many still do!)

# RBAC

- Assign permissions to roles
- Roles mapped to job functions
- Simple to implement
- Works well in static orgs

# RBAC Limitations

- Role explosion in complex systems
- Hard to manage dynamic needs
- Poor for fine-grained access
- Audits become messy

# ReBAC

- Relationship-based access
- Example: Google Docs sharing
- Dynamic and flexible
- Better for collaboration models

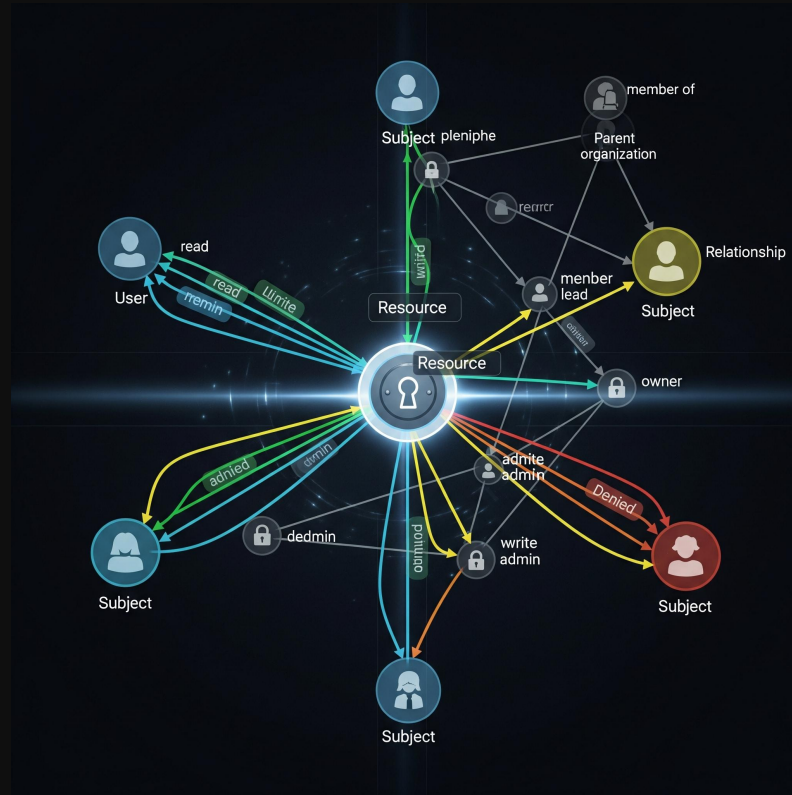
# ABAC

- Attribute-based policies
- Consider time, location, device
- More flexible than RBAC
- Powerful but complex

# Choosing a Model

- RBAC for simple/static orgs
- ABAC/ReBAC for dynamic environments
- Hybrid models often best
- Balance simplicity with flexibility

# Buy, Build, or Borrow?



# Buy, Build, or Borrow?

- Vendor SaaS (Okta/Auth0)
- Open source (Ory, Keycloak)
- Custom = last resort
- Consider skills + compliance

# Decoupling Auth

- Remove auth logic from apps
- Use API gateways for enforcement
- Leverage external IdPs
- Scales better across services

# Zero Trust

- Never trust, always verify
- Authenticate every request
- Inspired by Google BeyondCorp
- Applies to users and services

# Zero Trust

- HashiCorp Boundary
- Slack Nebula
- Teleport
- Tailscale

# Microservices Security

- JWT tokens for identity propagation
- Service-to-service auth with mTLS
- Service meshes handle authn/z
- Token expiry + rotation matter

# Legacy Modernisation

- Wrap old apps with reverse proxies
- Externalise authentication logic
- Integrate with IdPs gradually
- ‘Don’t rip, wrap’ strategy

# Auth Anti-Patterns

- Rolling your own crypto
- DIY login systems
- Storing plaintext passwords
- Relying on obscurity

# Migration Strategy

- Audit current systems
- Pilot with low-risk apps
- Iterate and expand coverage
- Train developers & users

# Key Takeaways

- Passwords alone  $\neq$  enough
- Centralised auth is essential
- Secrets must be managed properly
- Modern authZ models future-proof systems

# What To Do Tomorrow

- Enable MFA org-wide
- Audit repos for secrets
- Adopt a secrets manager
- Pilot modern auth in one app

# Resources

- NIST 800-63: digital identity
- OWASP ASVS: app security standards
- OAuth2 / OIDC specifications
- FIDO Alliance: passwordless resources

# Final Thought

- “Security is like an onion – lots of layers”
- Layers make you cry, but they protect you
- Without them, everything stinks
- Invest in strong authentication

# Q&A

- Keep calm and don't use password123
- Ask about practical adoption
- Challenge your current assumptions
- Now your turn: what's your biggest auth pain?

