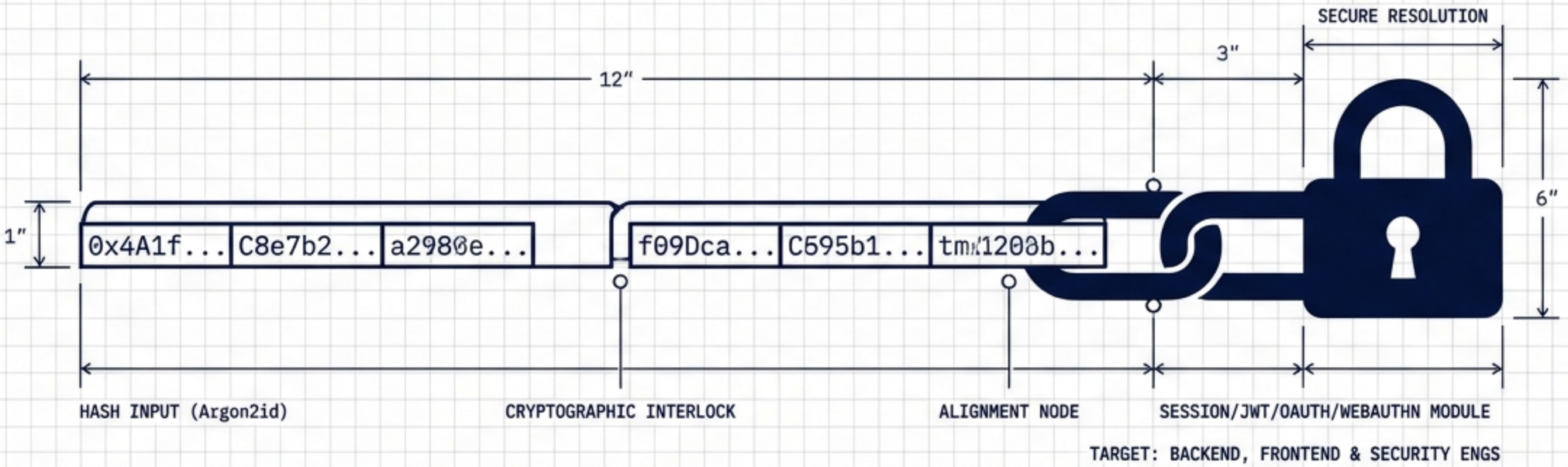


Web Security — S03E04: Modern Authentication

Argon2id, Session Cookies vs. JWTs, OAuth 2.0 / OIDC & WebAuthn Passkeys.

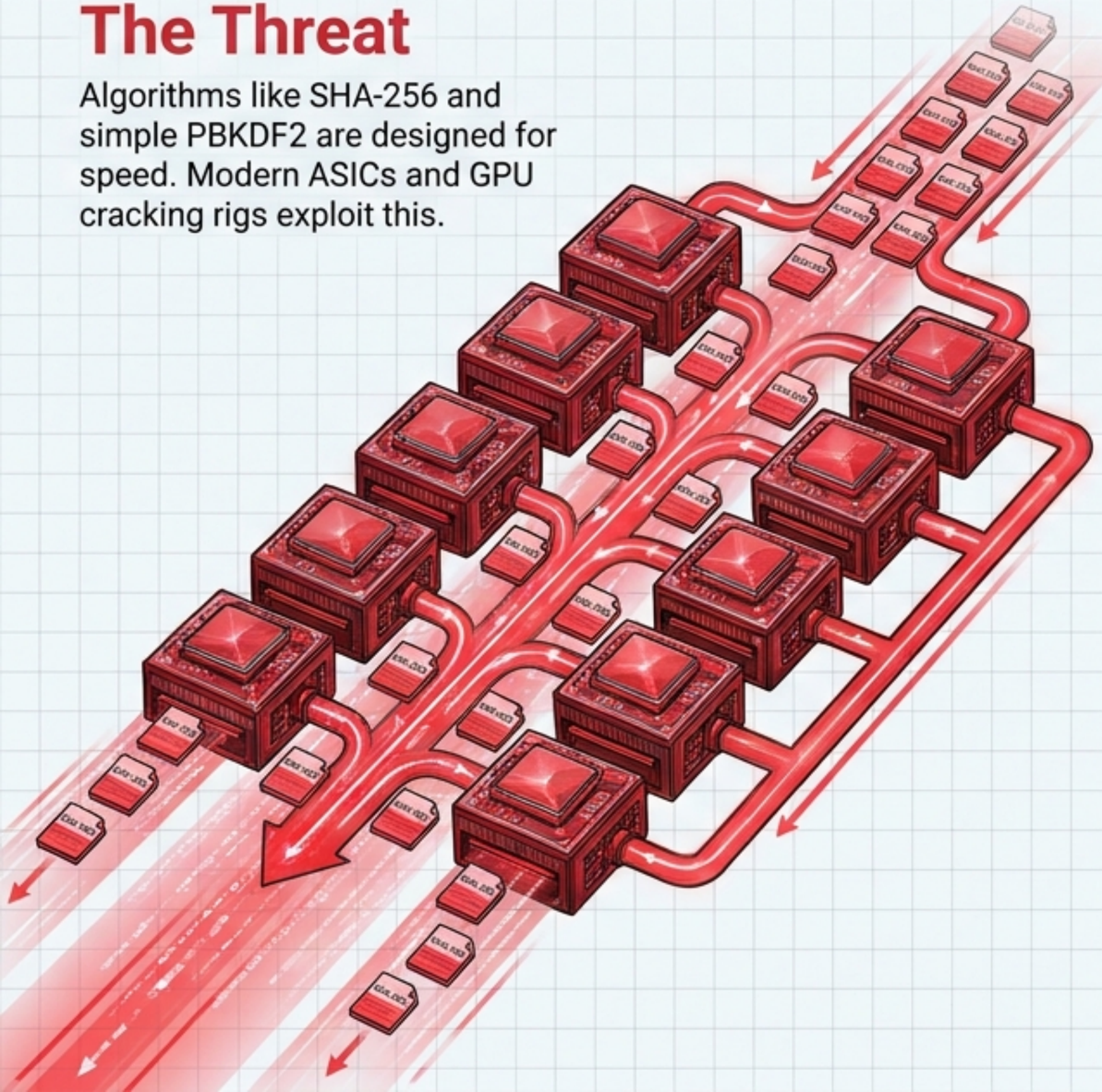
[ARCHITECTURE SCHEMATIC // TARGET: BACKEND, FRONTEND & SECURITY ENGS]

Gemini Notebook

The Fall of Fast Hashes to GPU Parallelization

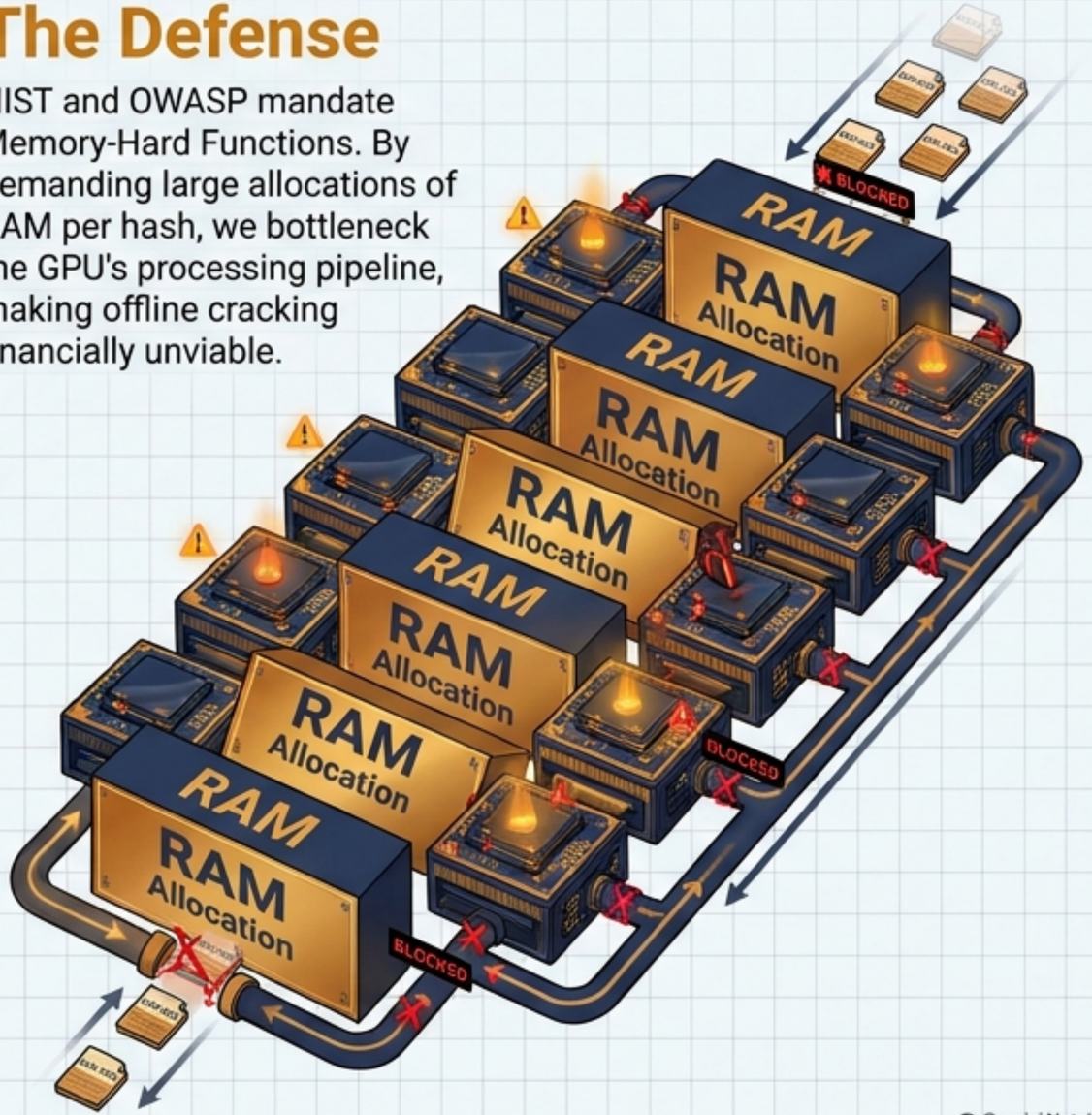
The Threat

Algorithms like SHA-256 and simple PBKDF2 are designed for speed. Modern ASICs and GPU cracking rigs exploit this.



The Defense

NIST and OWASP mandate Memory-Hard Functions. By demanding large allocations of RAM per hash, we bottleneck the GPU's processing pipeline, making offline cracking financially unviable.



Gemini Notebook

The Cryptographic Hash Selection Matrix

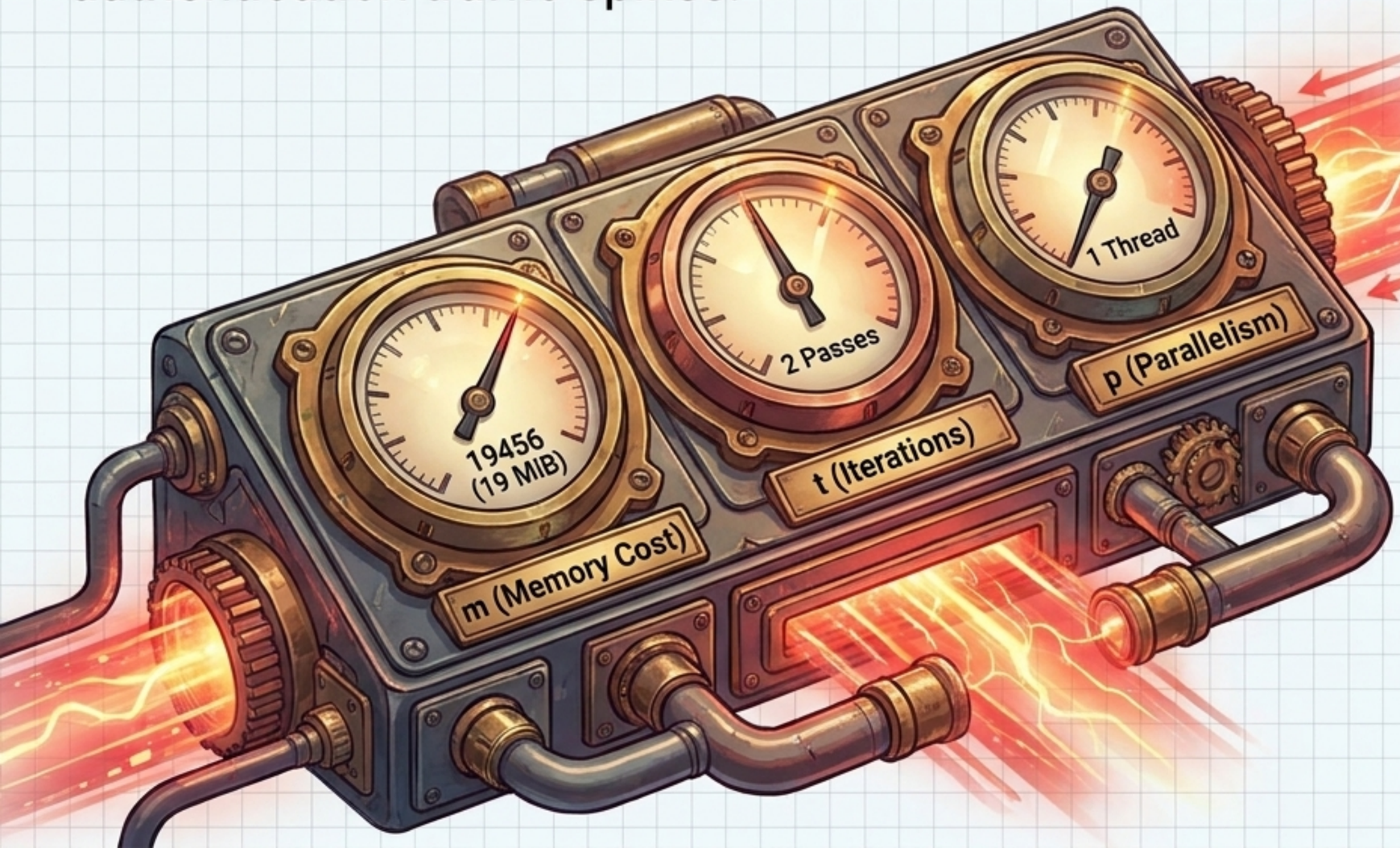
Argon2id (Winner)	scrypt (Fallback)	PBKDF2 (Legacy)
High Memory Hardness	High Memory Hardness	Low Memory Hardness
High GPU Resistance	High GPU Resistance	Low GPU Resistance
Modern Default (RFC 9106)	N=2^17, r=8	FIPS-140 Compliant (HMAC-SHA-256)

The bcrypt Footgun: bcrypt silently truncates inputs at exactly 72 bytes. Long passphrases or multi-byte unicode characters are cut off, creating a dangerous false sense of security.

Gemini Notebook

Tuning Argon2id for Production Environments

Balancing brute-force defense against server CPU/RAM exhaustion during authentication traffic spikes.



OWASP Minimum Baselines for Argon2id

Gemini Notebook

Unique Salts vs. Hardware-Backed Peppers

Application Database



Salt: Unique per user. Defeats precomputed rainbow tables.

Network Security Boundary

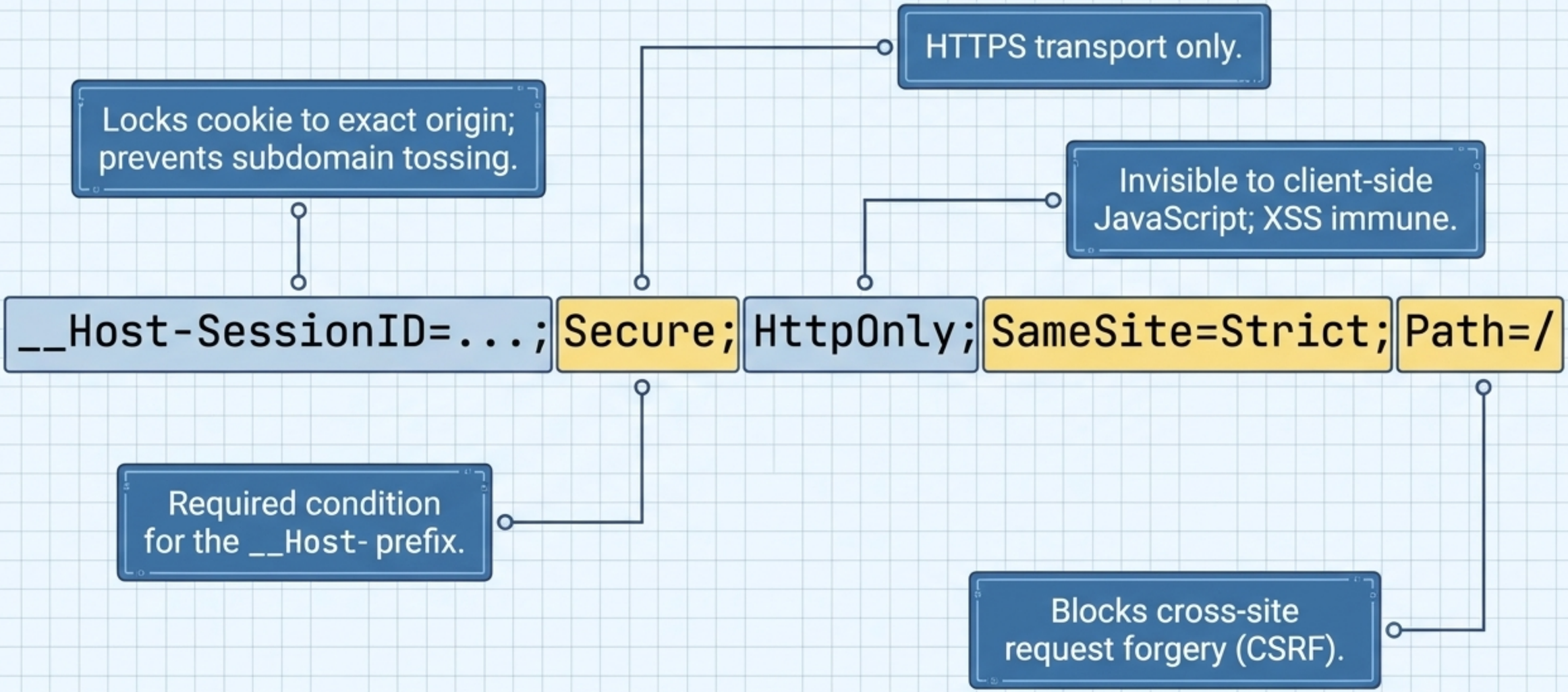
Hardware Security Module (HSM) / KMS



Pepper: Cryptographic secret applied via HMAC post-hashing. An attacker who exfiltrates the entire database still cannot crack passwords offline without compromising this physical hardware.

Gemini Notebook

Anatomy of the Hardened Session Cookie

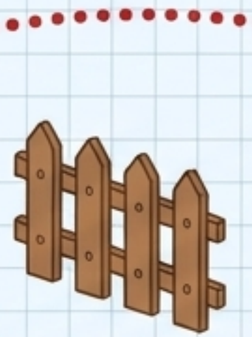


Gemini Notebook

Defeating Sibling-Subdomain Cookie Fixation

The Exploit

attacker.app.com
(Compromised Sibling)



`Domain=.app.com`

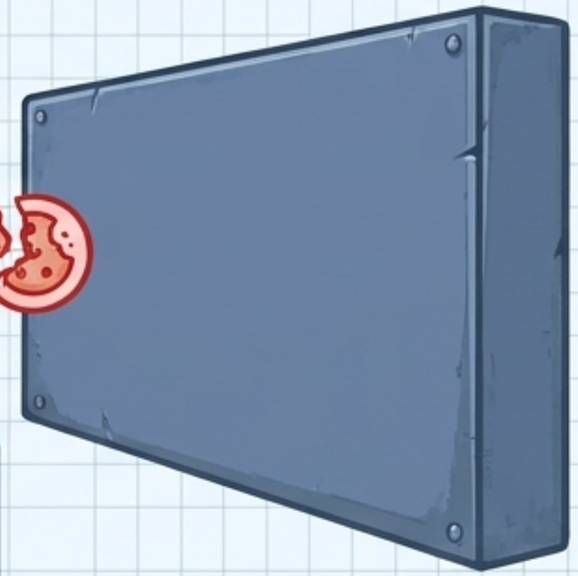
app.com

Without prefix: Sibling subdomain successfully overwrites the top-level session.

With RFC 6265bis Defense

attacker.app.com
(Compromised Sibling)

`__Host-SessionID`

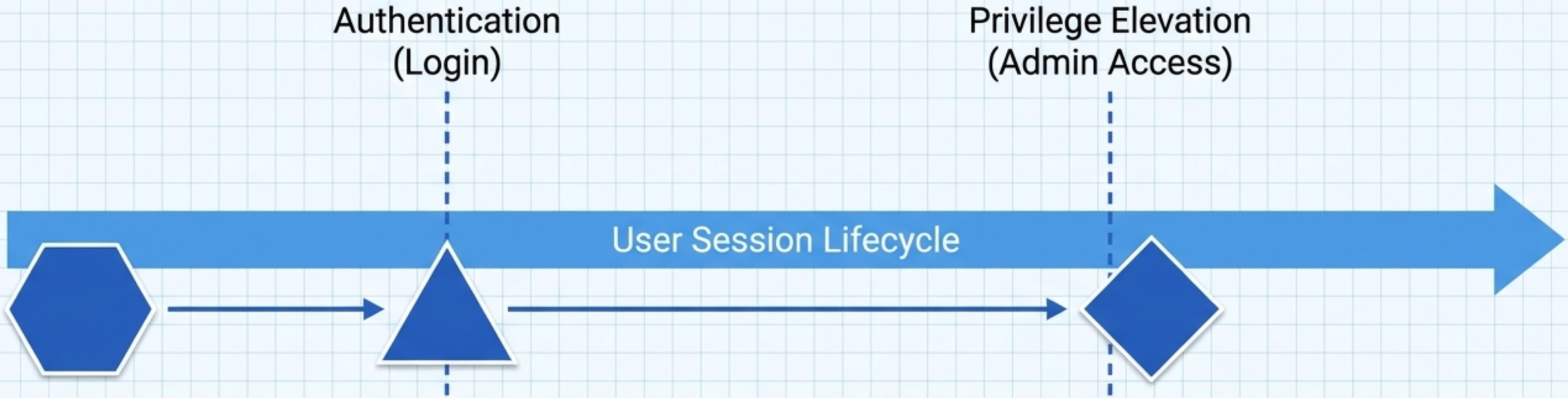


With `__Host-` prefix: The browser strictly rejects the cookie because the attribute is explicitly forbidden. The session is *locked* to the exact host.

Gemini Notebook

Session Fixation Defense & Identifier Rotation

Lifecycles require both Absolute Timeouts (max lifespan) and Idle Timeouts (inactivity).

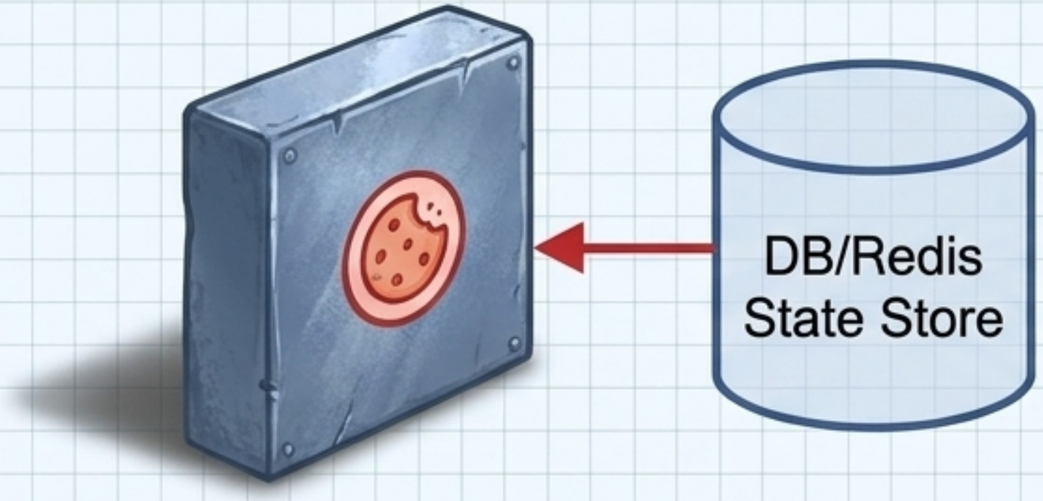


Rotation Mandate: To defeat Session Fixation, web applications must issue a completely new cryptographic identifier immediately upon any authentication state change.

Gemini Notebook

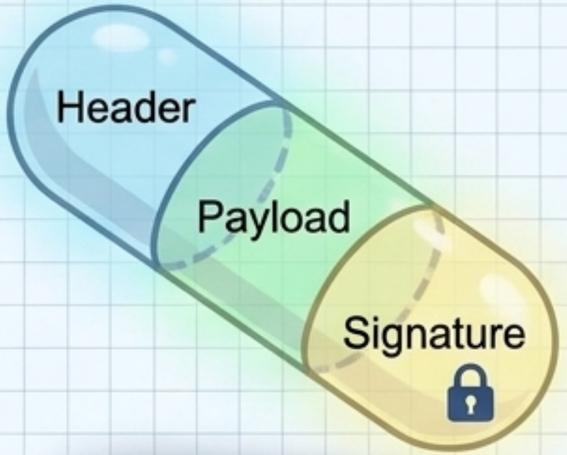
The Great Debate: Opaque Sessions vs. Stateless JWTs

Stateful Opaque Cookie



- Requires server-side state (DB/Redis lookup per request).
- Trivial to revoke instantly.
- Extremely small payload size.

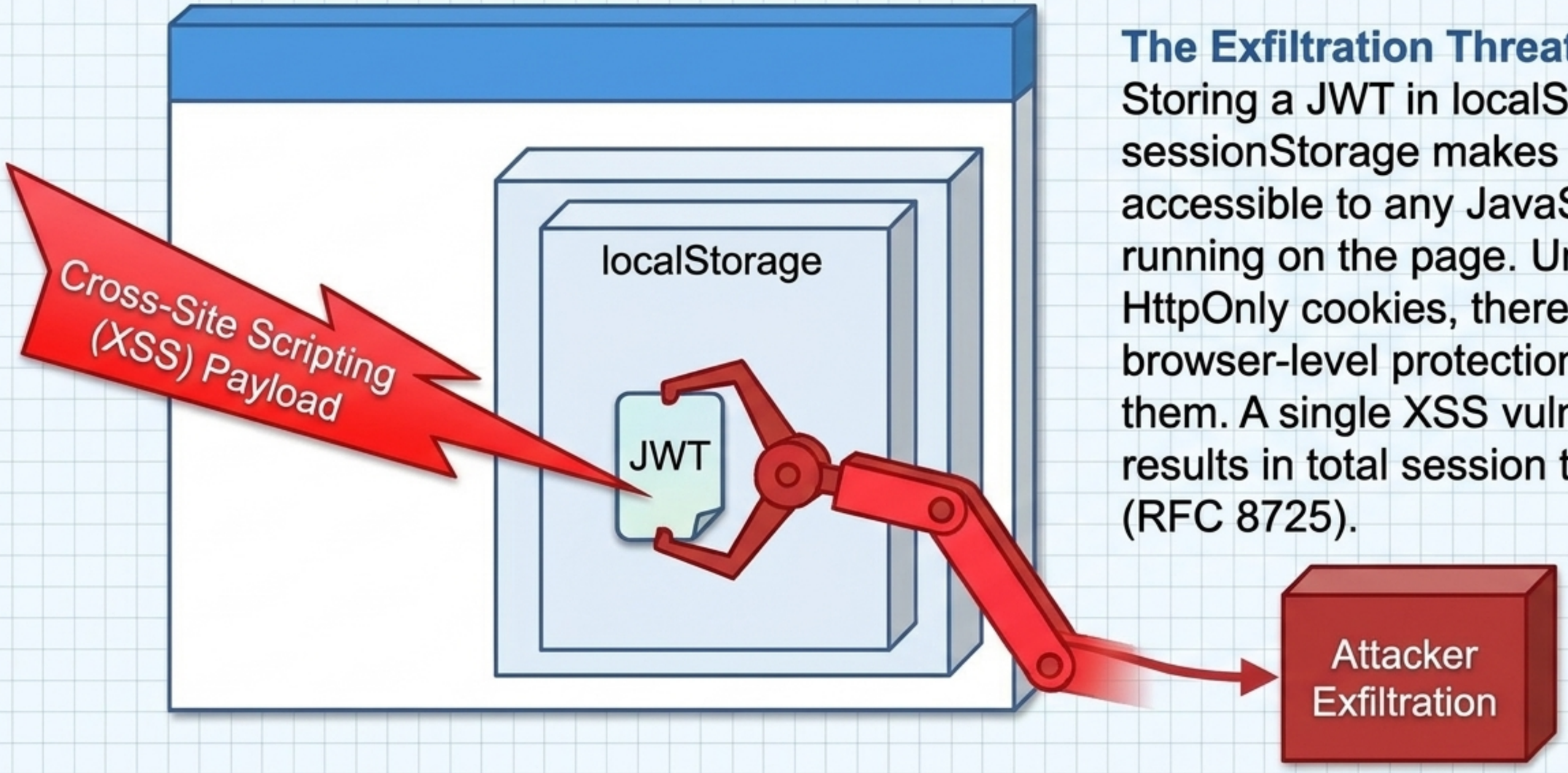
Stateless JWT



- Cryptographically verifiable without DB lookups.
- The infinite scalability myth.
- Extremely difficult to revoke without re-introducing state (deny-lists), defeating the purpose.

Gemini Notebook

Why Browser-Side JWTs Fail Security Audits



The Exfiltration Threat:
Storing a JWT in localStorage or sessionStorage makes it accessible to any JavaScript running on the page. Unlike HttpOnly cookies, there is no browser-level protection shielding them. A single XSS vulnerability results in total session theft (RFC 8725).

Gemini Notebook

JWT Cryptographic Vulnerabilities (RFC 8725)

The **Core Flaw**: JWT headers are unauthenticated attacker input. Libraries must not blindly trust the header to determine verification rules.

Signature Bypass

```
{"alg": "RS256"}
~~{"alg": "none"}~~
```

Forces the server to skip signature validation.

Public-Key Confusion

```
{"alg": "RS256"}
~~{"alg": "HS256"}~~
```

Swaps asymmetric RS256 for symmetric HS256, tricking the server into using its public key as an HMAC secret.

Server-Side Request Forgery

```
{"jku": "[trusted_url]"}
{"jku": "https://attacker.com/key.json"}
```

Injects an unvalidated JSON Web Key URL, forcing the server to fetch and trust a malicious key.

Cross-Service Replay

```
{"aud": "[Service A]"}
~~aud: [REMOVED]~~
```

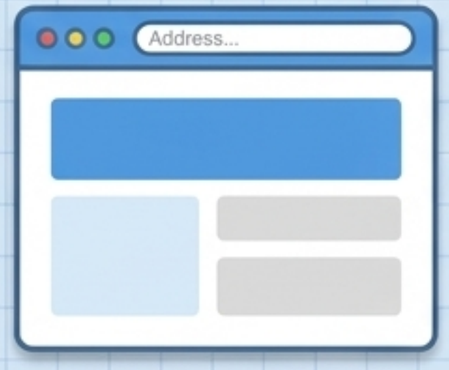
Removing audience claims allows a token minted for Service A to be replayed against Service B.

Gemini Notebook

Resolving the Debate: The Backend-for-Frontend (BFF)

Do not choose between Cookies and JWTs—use both exactly where they belong. The BFF acts as a secure translation layer.

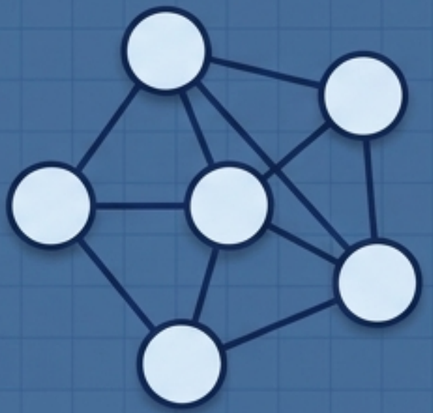
The Untrusted Client
(Browser)



The Gateway
(BFF)



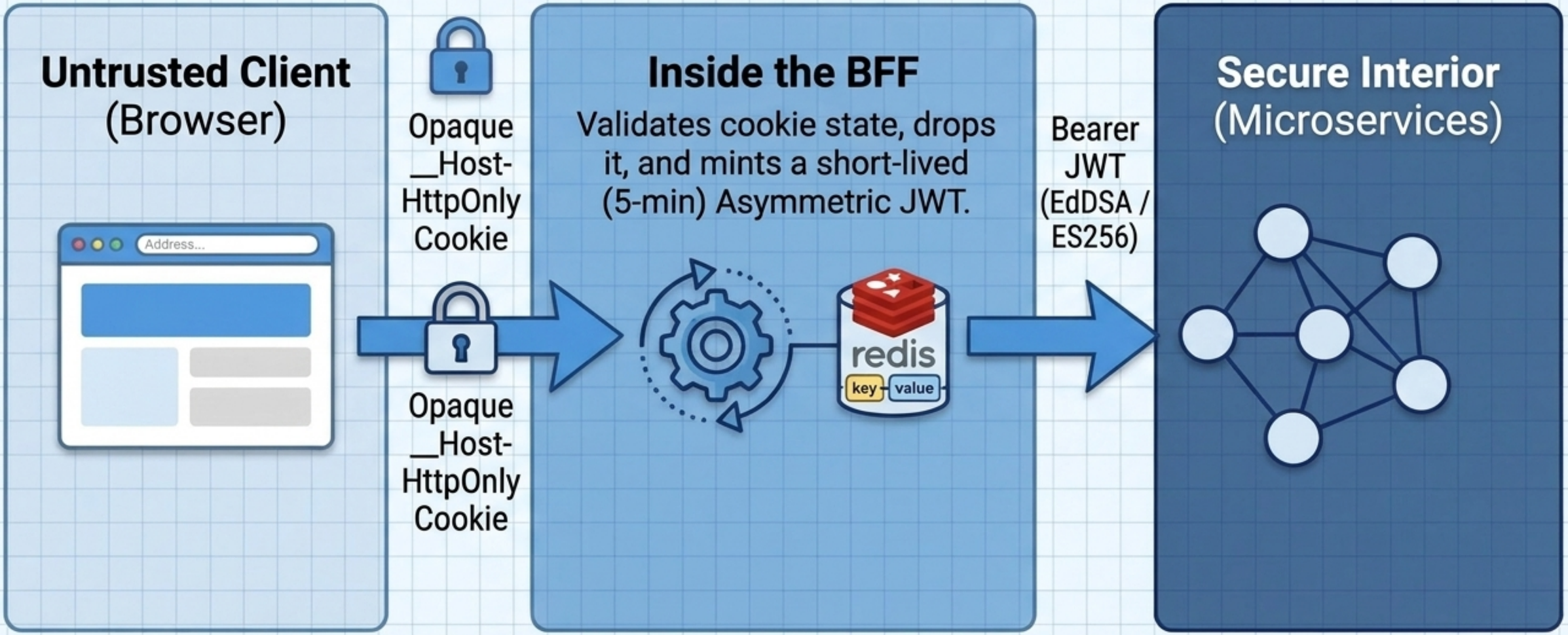
The Secure Interior
(Microservices)



Gemini Notebook

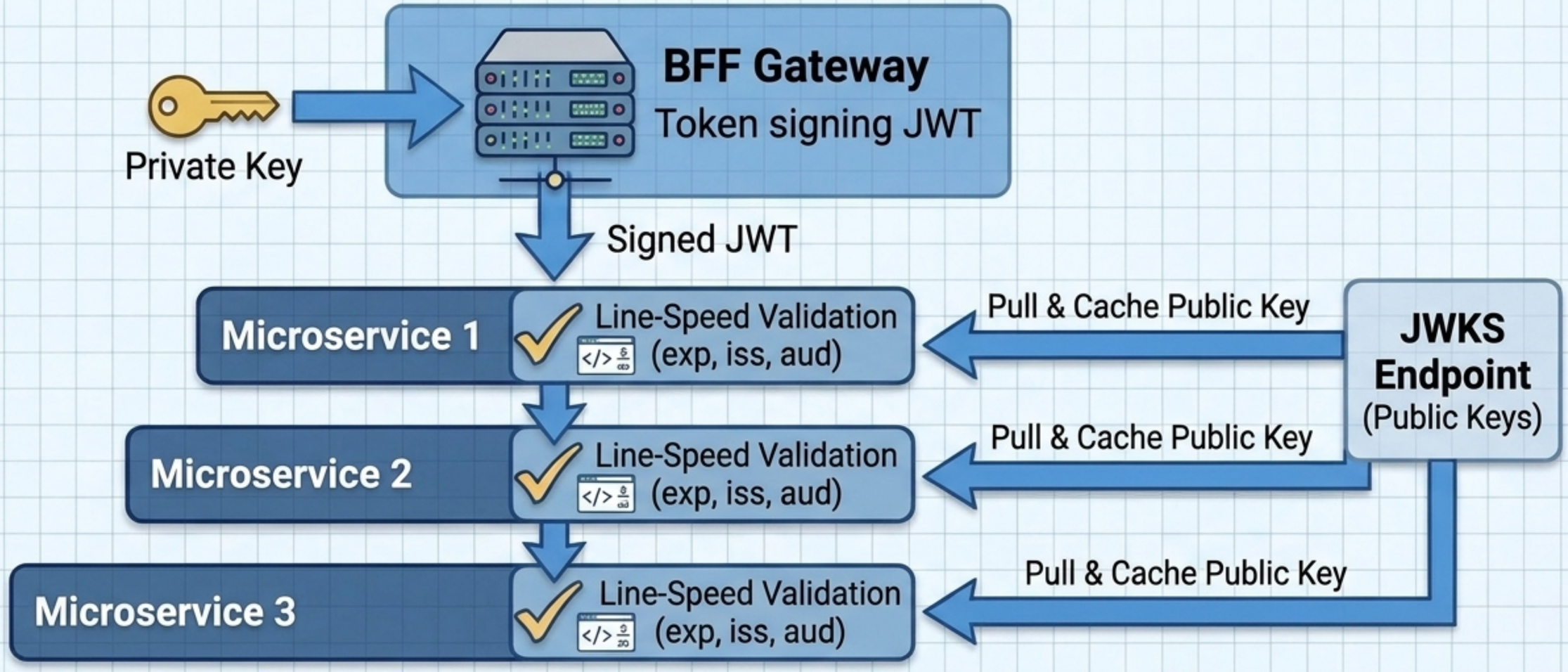
The Translation Architecture Gold-Standard

The browser never sees the JWT. Microservices never touch a database. Total decoupling.



Gemini Notebook

High-Speed Microservice JWT Propagation



Decentralized Validation: Downstream services locally cache the BFF's public key. Tokens are validated mathematically at line-speed (checking exp, iss, and aud claims) without bottlenecking a central authorization server.

Gemini Notebook

OAuth 2.0 vs. OpenID Connect (OIDC)

Never use an OAuth Access Token for client-side identity proofing.

OAuth 2.0



Delegated Authorization

OpenID Connect

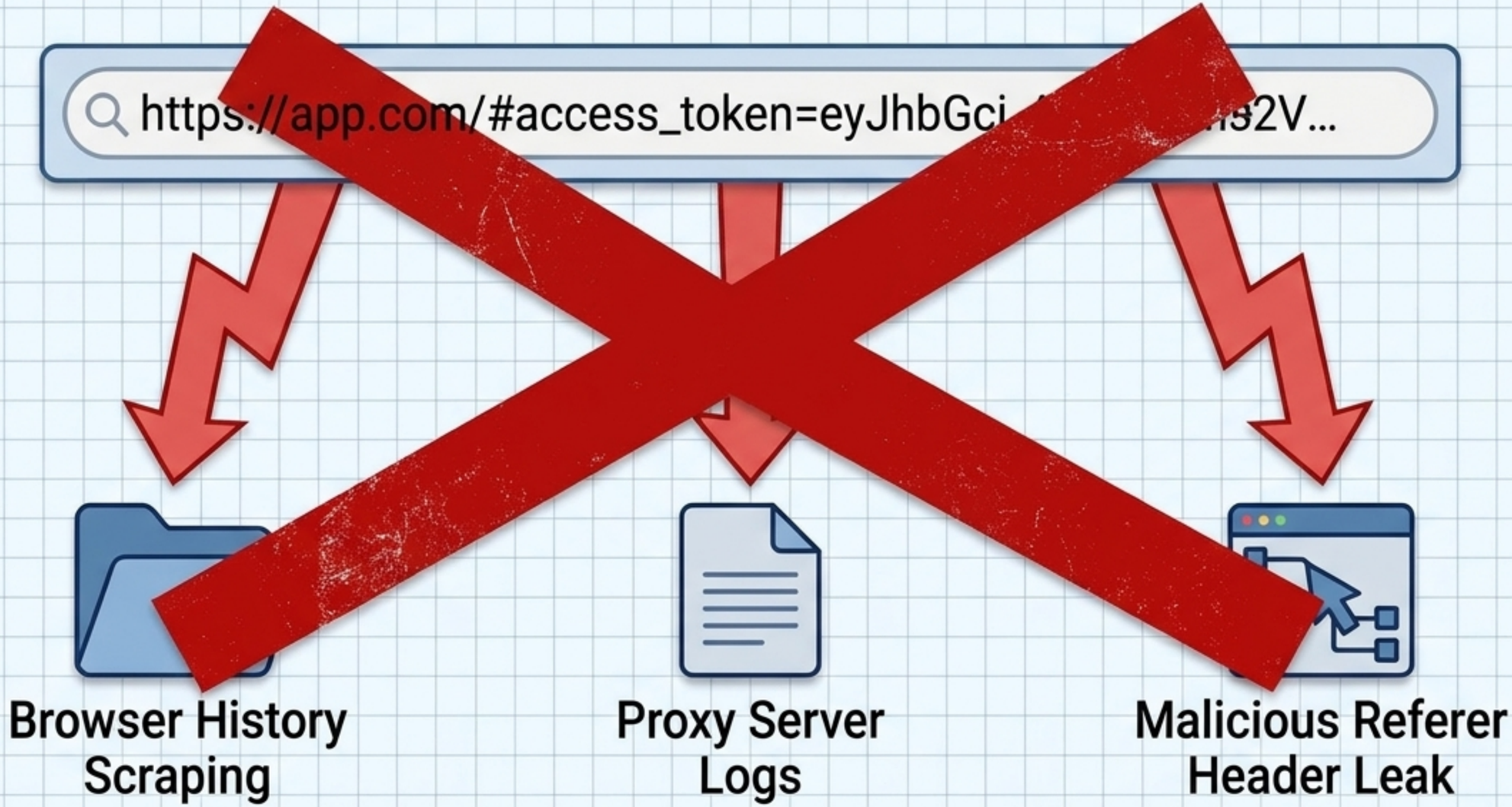


Federated Authentication

Gemini Notebook

The Death of the Implicit Flow (RFC 9700)

The Implicit Flow is officially obsolete for all clients (including Single Page Apps).



Gemini Notebook

Step-by-Step: Auth Code + PKCE (RFC 7636)

An intercepted Auth Code is useless without the original verifier.



Gemini Notebook

Hardening the OAuth Exchange



Prevents Cross-Site Request Forgery, replay attacks, and forged logins.

Stops authorization codes from leaking via open-redirectors.

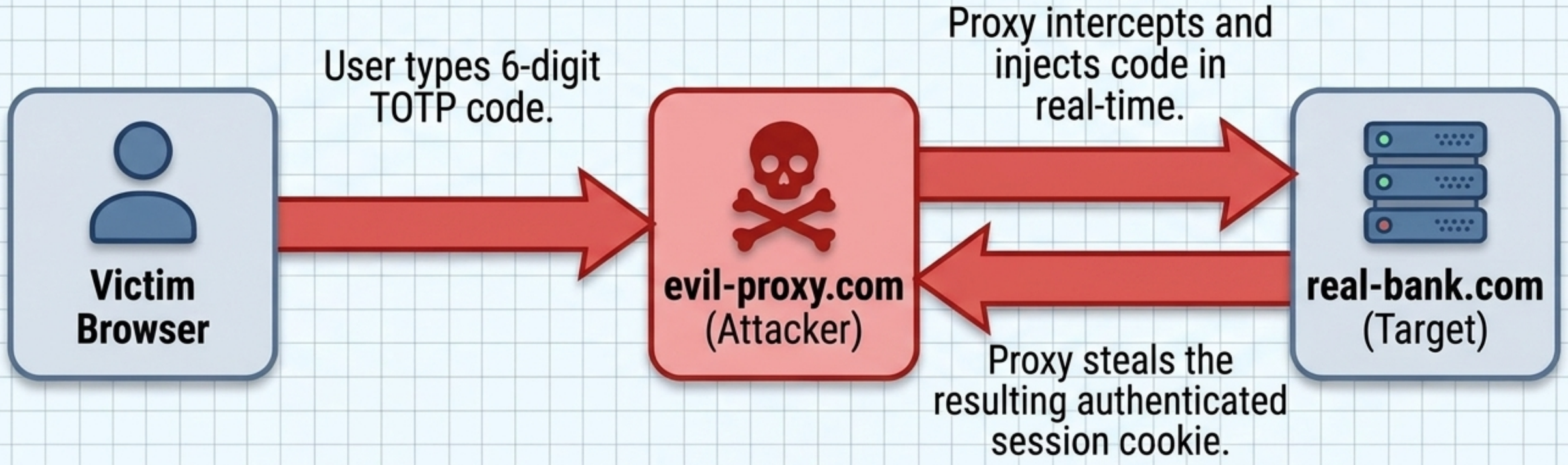


Automatic reuse revocation. If a stolen refresh token is replayed, the server instantly nukes the entire token family, killing persistent access.

Gemini Notebook

The Real-Time AitM Phishing Threat

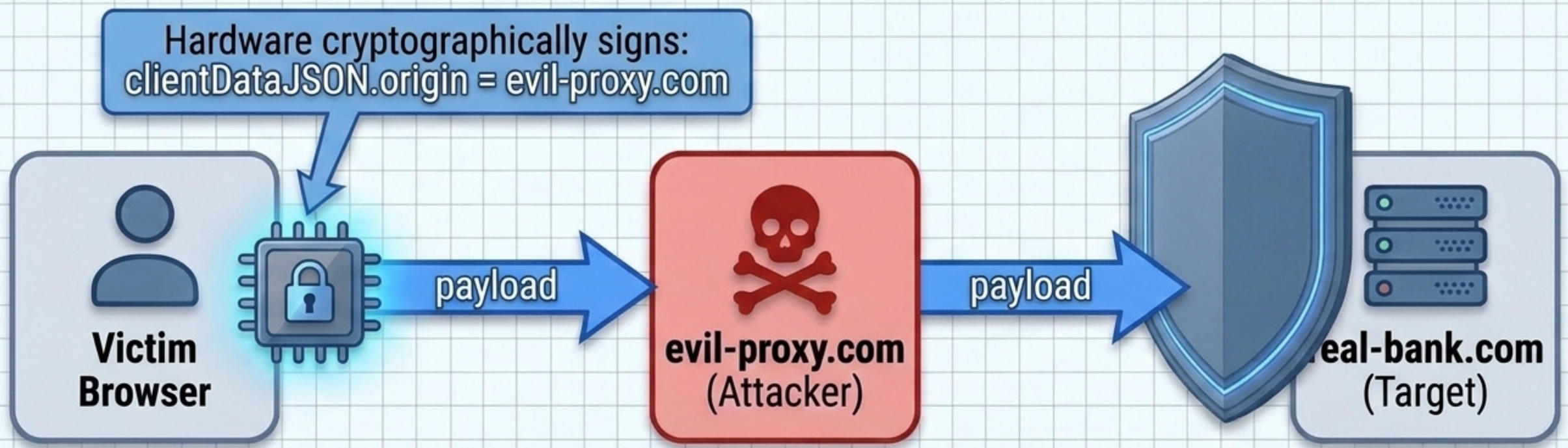
Why 6-digit TOTP codes are failing: Adversary-in-the-Middle kits seamlessly bypass traditional MFA.



Gemini Notebook

Phishing-Resistant Auth: The WebAuthn Shield

Level 3 Phishing Resistance: Proxies cannot forge hardware signatures.



Server mathematically
rejects signature.
Expected origin "real-bank.com",
received "evil-proxy.com".

Gemini Notebook

Passkeys & Hardware-Backed Key Storage

Private keys are generated and guarded by the operating system's secure key manager.

Platform Authenticators
(Synced Passkeys)



Roaming Authenticators
(Hardware Keys)



FIDO2 / CTAP Ceremony

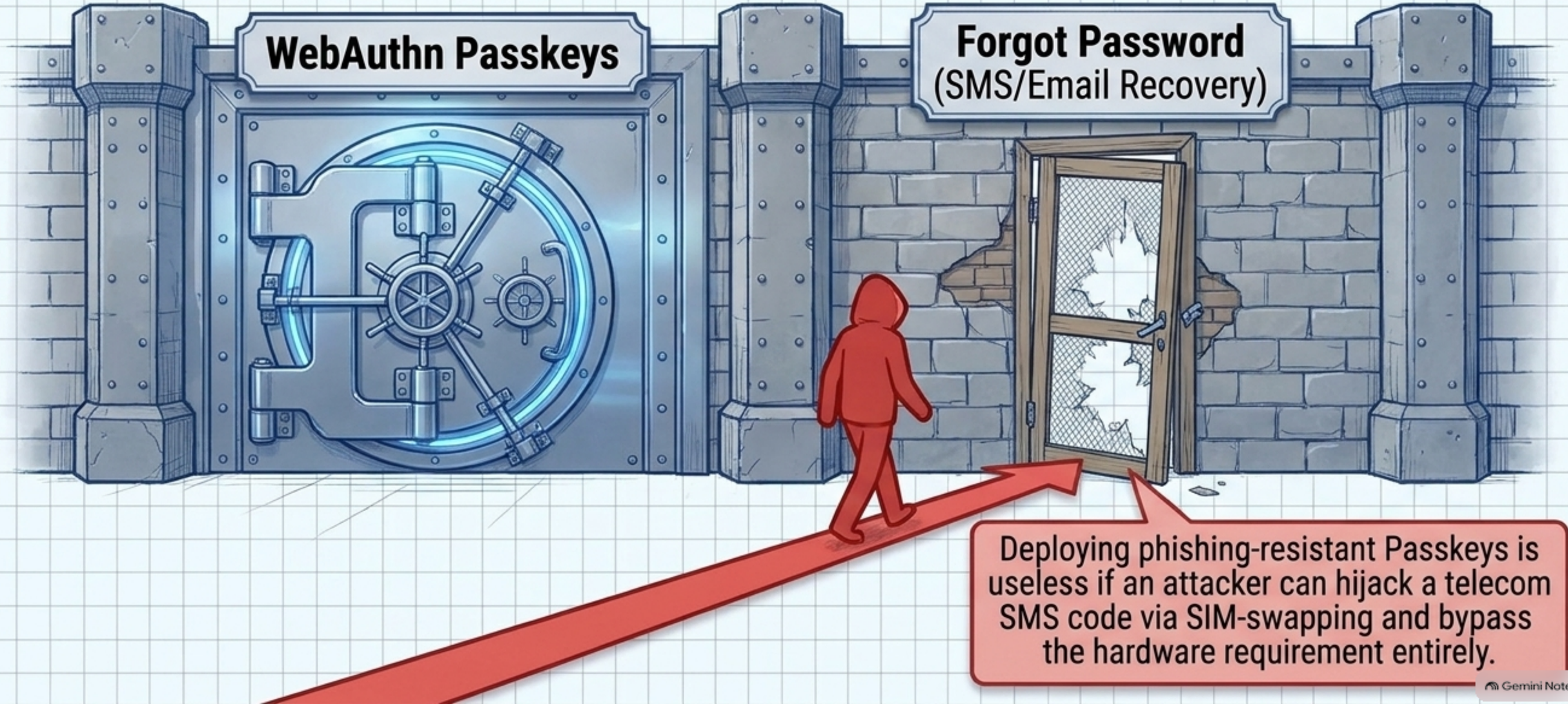
Non-exportable Private Key signs the server-provided Challenge.

The server only stores the Public Key. OS-level malware cannot extract the Private Key.

Gemini Notebook

The Account Recovery Downgrade Attack

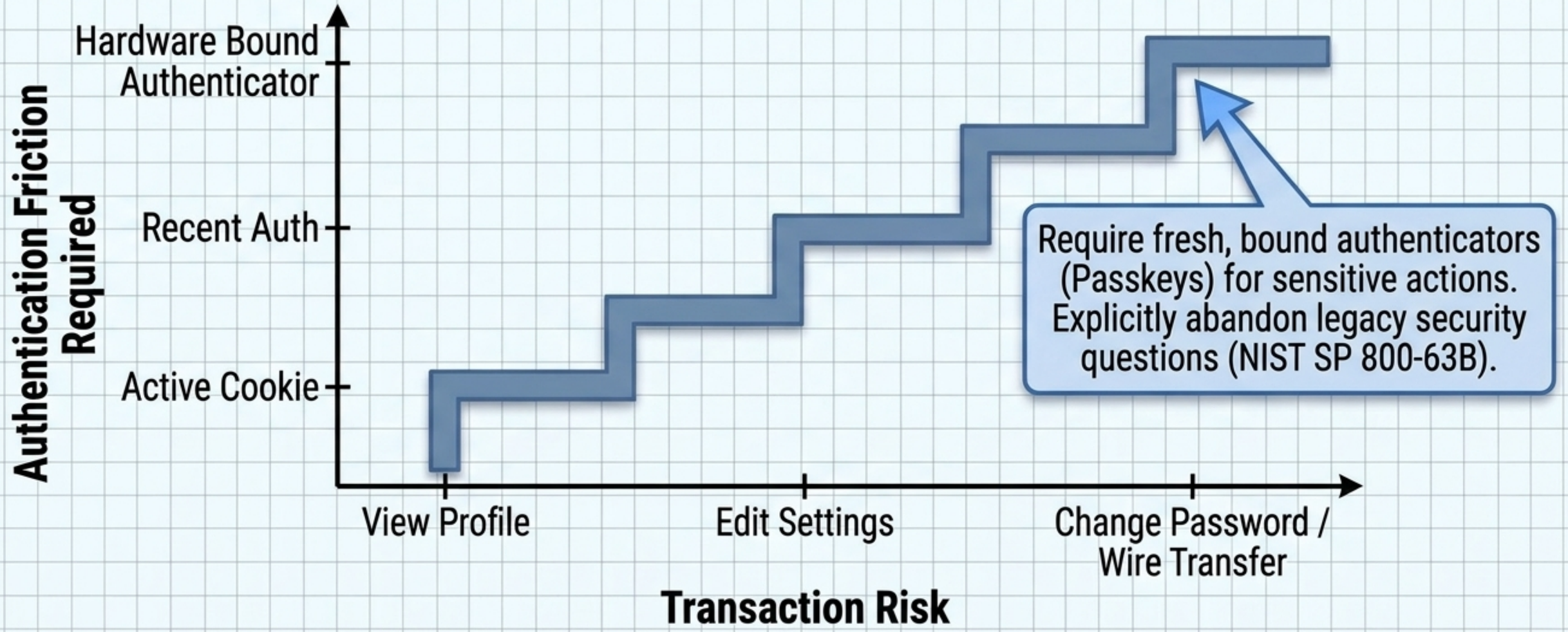
Your authentication system is only as secure as its recovery flow.



Gemini Notebook

Step-Up MFA & Context-Aware Auth

An active session cookie only proves the user authenticated in the past.
Authenticated session ≠ absolute trust.



Gemini Notebook

Synthesis: The Unified Auth Architecture Matrix

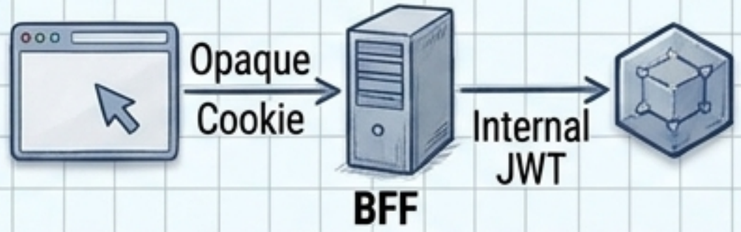
Secret Storage

- Argon2id (m=19456, t=2, p=1) + HSM-Backed HMAC Pepper.



Web App Sessions

- BFF Pattern translating opaque cookies to internal JWTs.



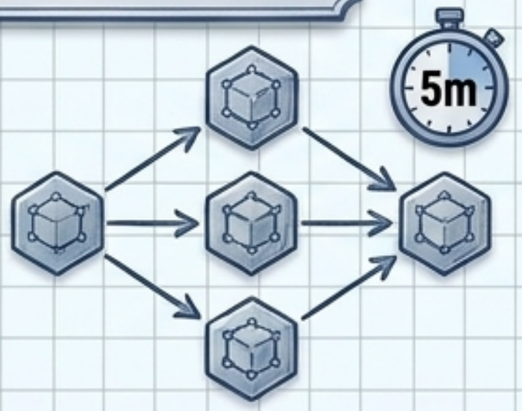
Browser Boundary



- __Host-prefixed, HttpOnly, SameSite=Strict session cookies.

Internal Microservice Auth

- Short-lived (5m) asymmetric EdDSA / ES256 JWTs.



Federation & MFA

- OAuth 2.0 Auth Code Flow + PKCE + Strict Redirect URIs.
- WebAuthn Passkeys (Phishing-Resistant Level 3). Zero SMS fallbacks.



Gemini Notebook