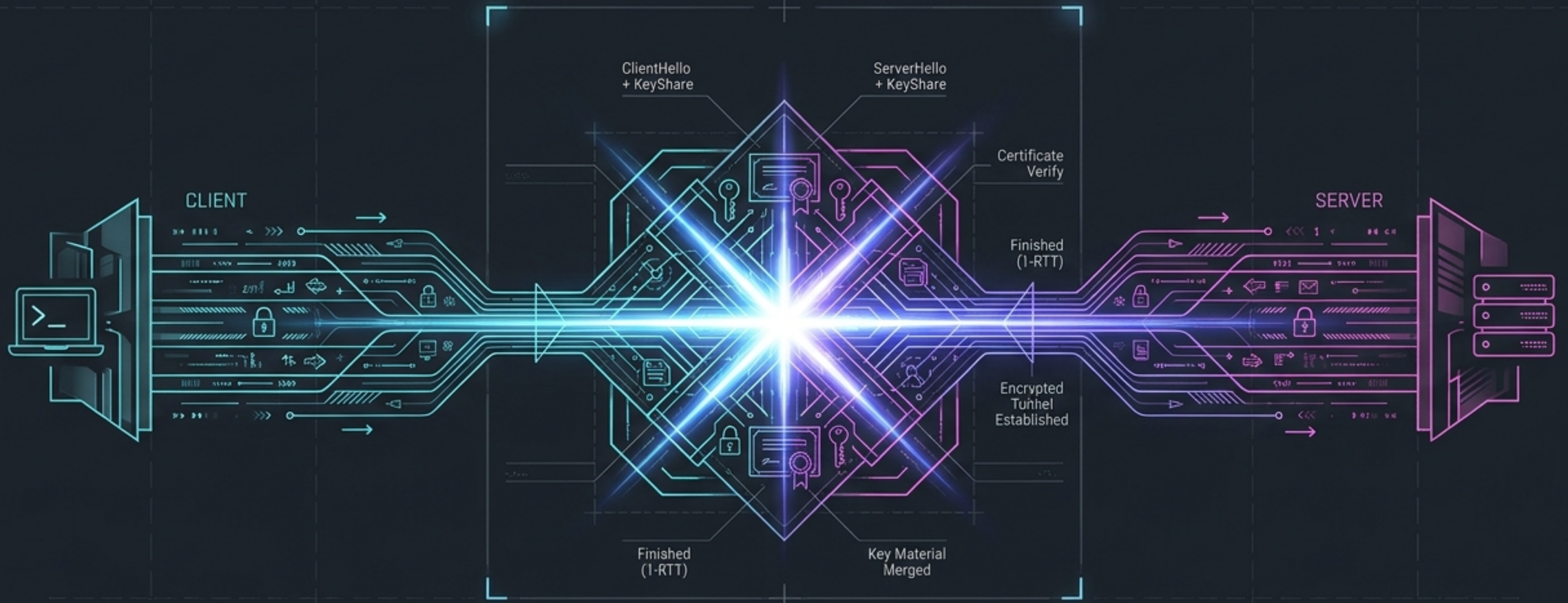
Web Security — S03E01: Transport Cryptography

TLS 1.3 Internals, X.509 PKI, HSTS & Mutual TLS



Gemini Notebook

The Baggage of TLS 1.2

Structural flaws in a modern threat landscape



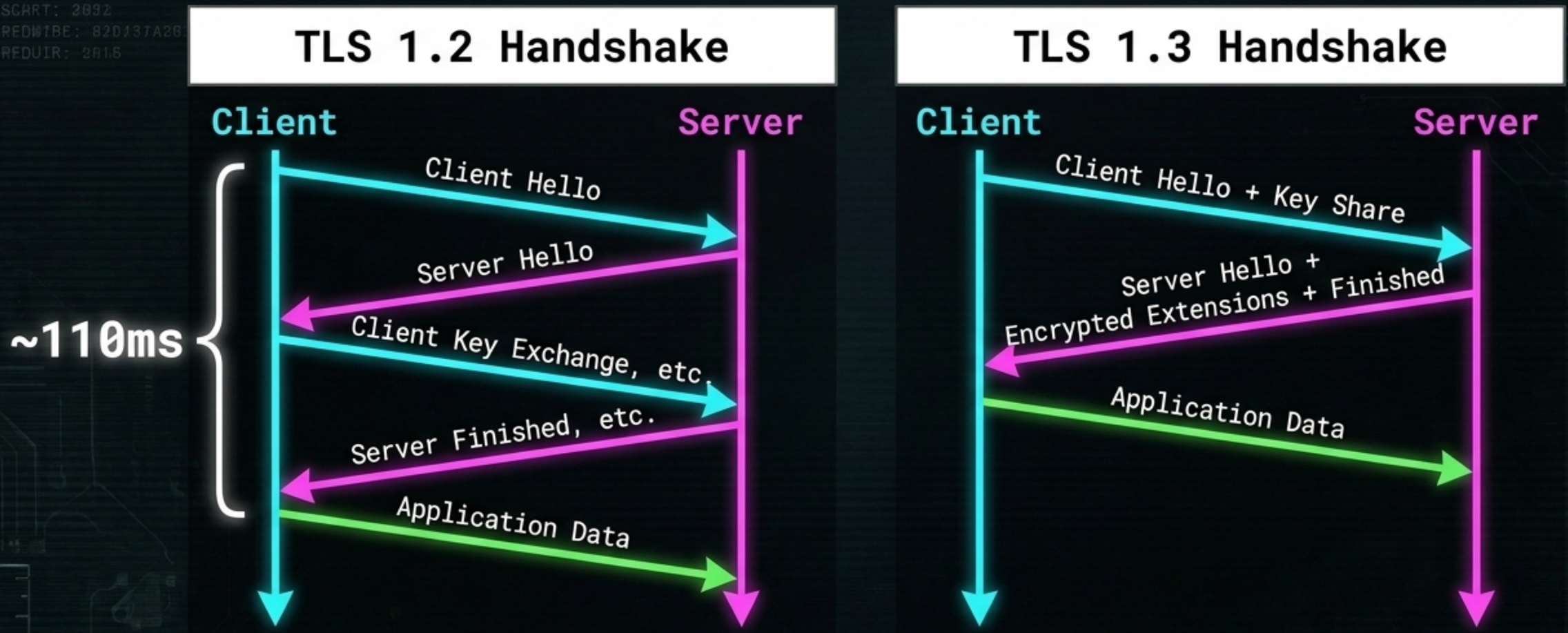
Gemini Notebook

The Vulnerability Matrix

Cryptographic Flaw	Exploit / Vulnerability	The Consequence
Static RSA Key Transport	Retroactive Decryption	Lack of Forward Secrecy
Block Cipher Padding	POODLE / Lucky13	Plaintext Recovery via CBC Oracles
MAC-then-Encrypt	Downgrade Attacks	Forced negotiation to weak legacy ciphers

Gemini Notebook

The Latency Tax



TCP Handshake (~50ms) happens first for both protocols.
TLS 1.2: Demands 2 Round Trips before API data moves.
TLS 1.3: Slashes cryptographic negotiation to 1 Round Trip.

Gemini Notebook

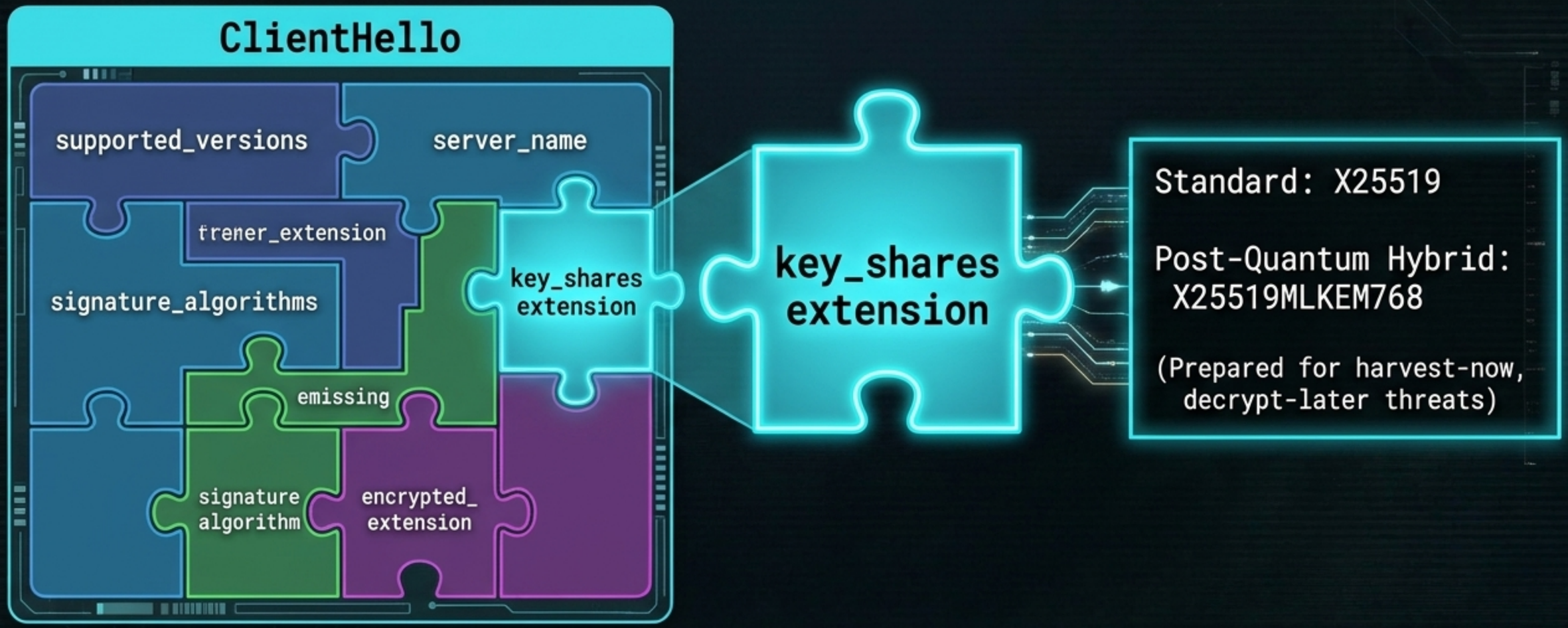
The 1-RTT Handshake Architecture (RFC 8446)



Gemini Notebook

Immediate Ephemeral Key Shares

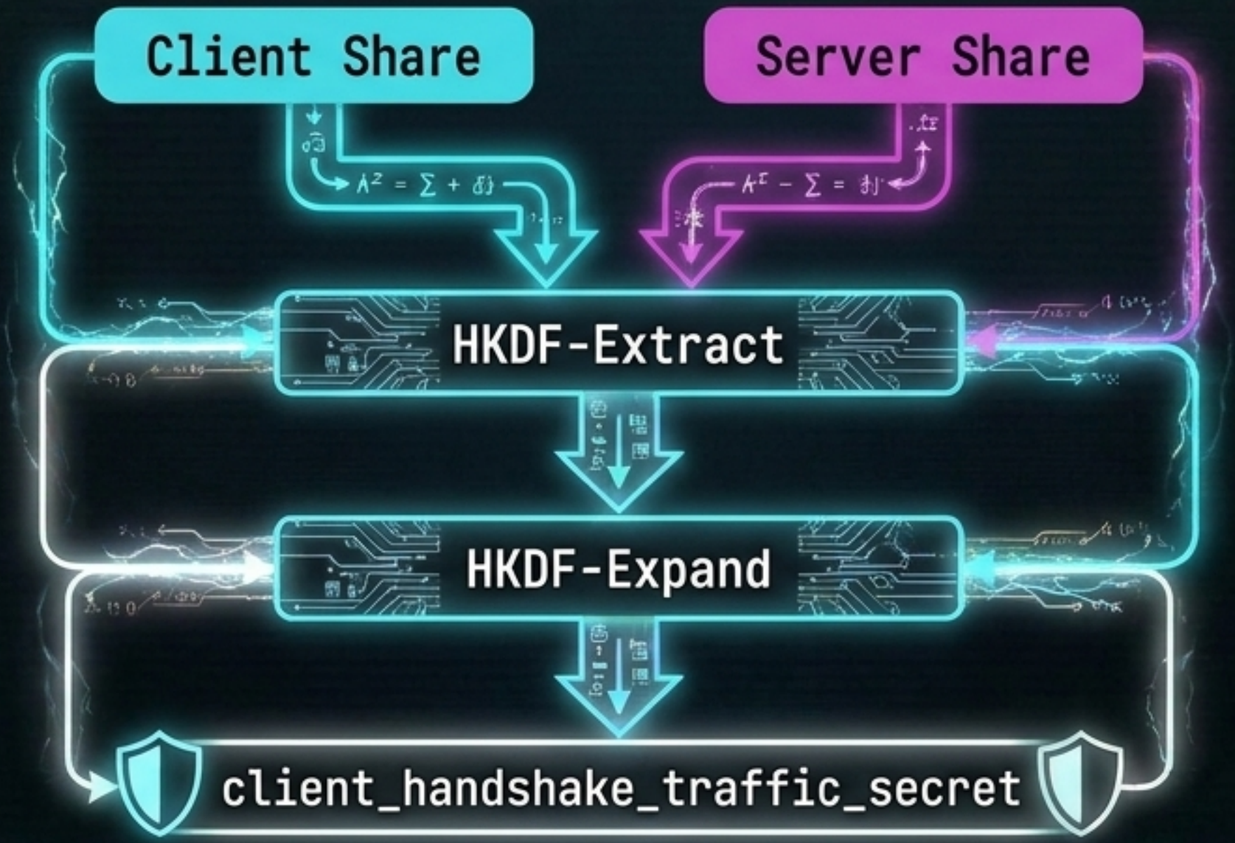
Client initiates by guessing the server's preferred cryptographic group and generates the ephemeral key share instantly.



Gemini Notebook

HKDF & The Key Schedule Waterfall

TLS 1.3 guarantees confidentiality during the handshake.



Handshake traffic secrets derive instantly following ServerHello.
Certificate and CertificateVerify signatures traverse the wire fully encrypted.

Gemini Notebook

AEAD-Only Symmetric Encryption

TLS 1.3 purges vulnerable generic block ciphers.

MAC-then-Encrypt



Encrypt-then-MAC (AEAD)



Authorized Primitives:
- AES-128-GCM
- AES-256-GCM
- ChaCha20-Poly1305

Gemini Notebook

The Power of Perfect Forward Secrecy

Ephemeral Diffie-Hellman (ECDHE) isolates cryptographic compromise.



Session keys are destroyed upon connection termination.
A leaked server private key cannot decrypt historical packet captures.

Gemini Notebook

0-RTT Early Data & PSK Resumption

Maximum performance for global mobile networks.

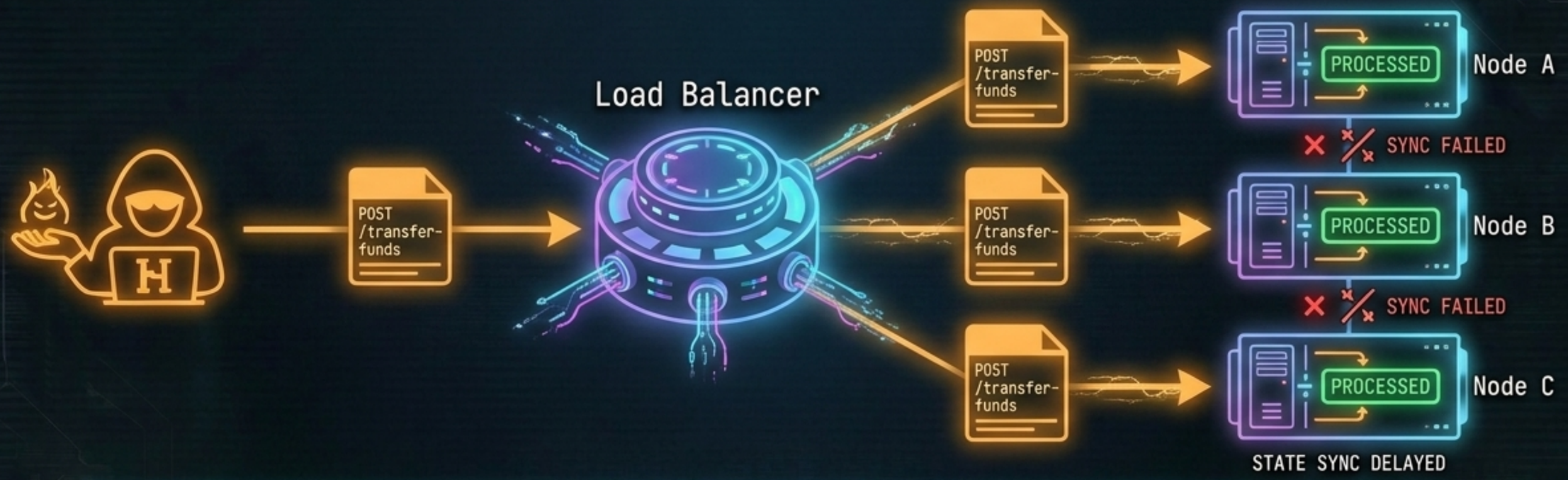


Pre-Shared Key (PSK) identities permit zero round-trip latency. Clients resume previous TLS 1.3 sessions by transmitting encrypted application data concurrently with the ClientHello.

Gemini Notebook

The 0-RTT Replay Hazard

0-RTT explicitly trades forward secrecy for speed and is vulnerable to network-level replay attacks.



0-RTT explicitly trades forward secrecy for speed and is vulnerable to network-level replay attacks.
Architectural Mandate: Never transmit non-idempotent mutations (e.g., database writes, financial transactions) inside early data.

Gemini Notebook

X.509 PKI & The Chain of Trust

Cryptographic identity is established via verifiable signature chains.



Gemini Notebook

The Failure of Traditional Revocation



CRLs: Bloated, unscalable lists dragging down client performance.
Live OCSP: Introduced unacceptable latency and severe privacy compromises by revealing user navigation paths directly to Certificate Authorities.

Gemini Notebook

OCSP Stapling & ACME Automation

Cryptographic identity is established via verifiable signature chains.

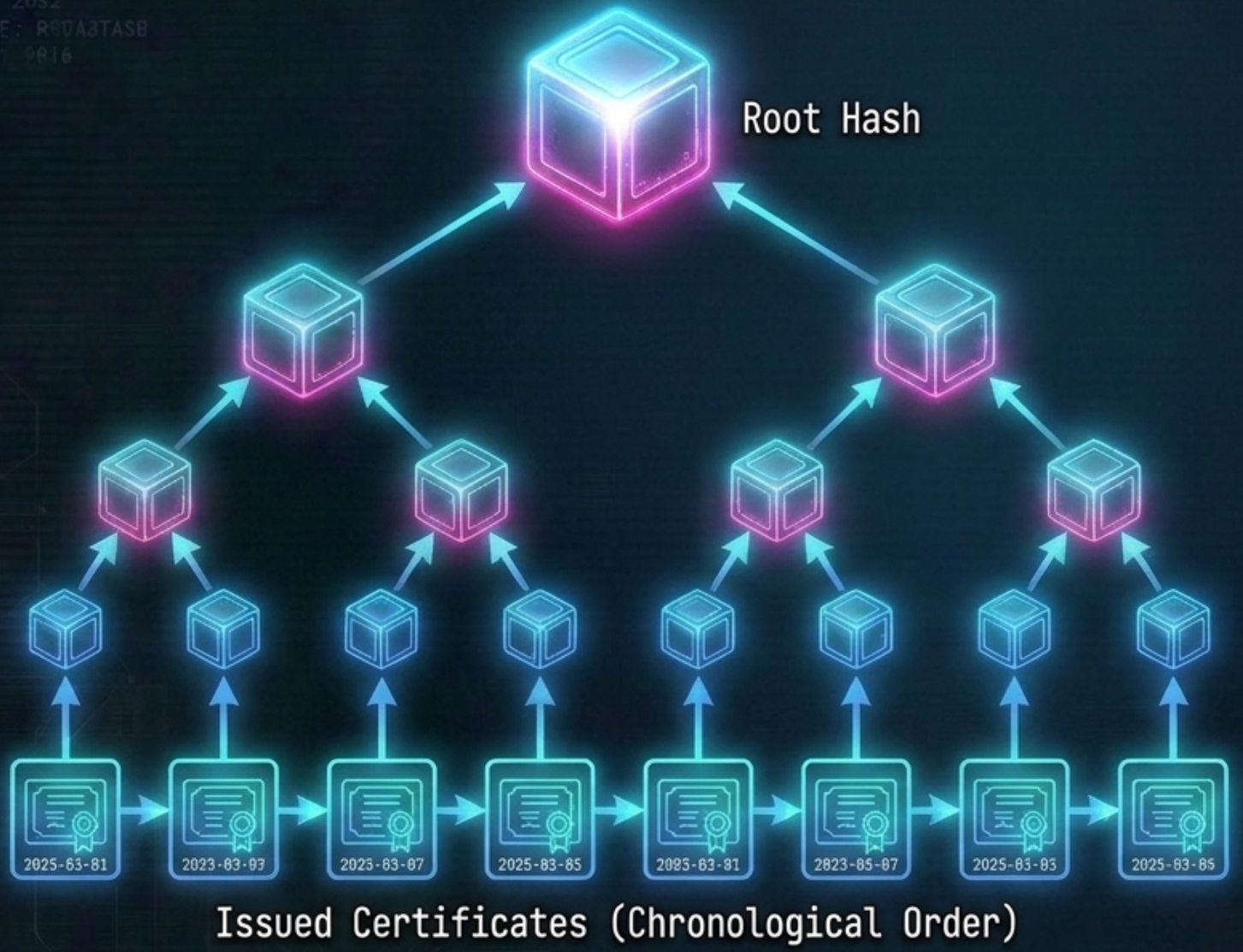


OCSP Stapling: The server bears the latency burden, delivering proof of validity directly in the handshake without breaking client privacy.

ACME Protocol: Shrinks the compromise window by enforcing short-lived automated certificates, rendering manual rotation obsolete.

Gemini Notebook

Certificate Transparency (CT) Logs

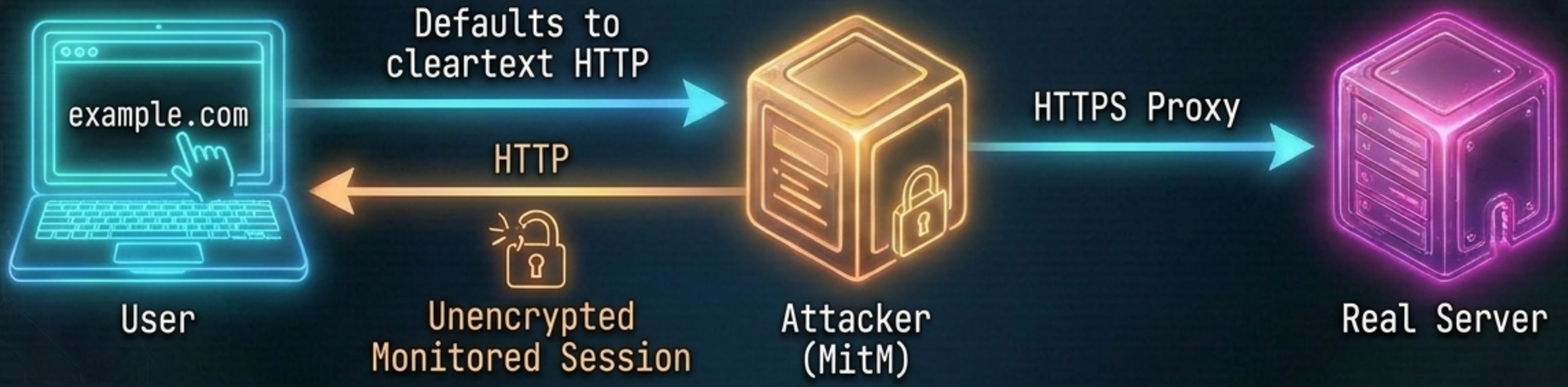


- A decentralized, cryptographically verifiable, append-only ledger.
- Eliminates the threat of rogue CAs silently issuing valid certificates for domains they do not control.
- Clients reject certificates lacking valid Signed Certificate Timestamps (SCTs).

Gemini Notebook

The Bootstrap Gap & SSL Stripping

The first request vulnerability (RFC 6797).

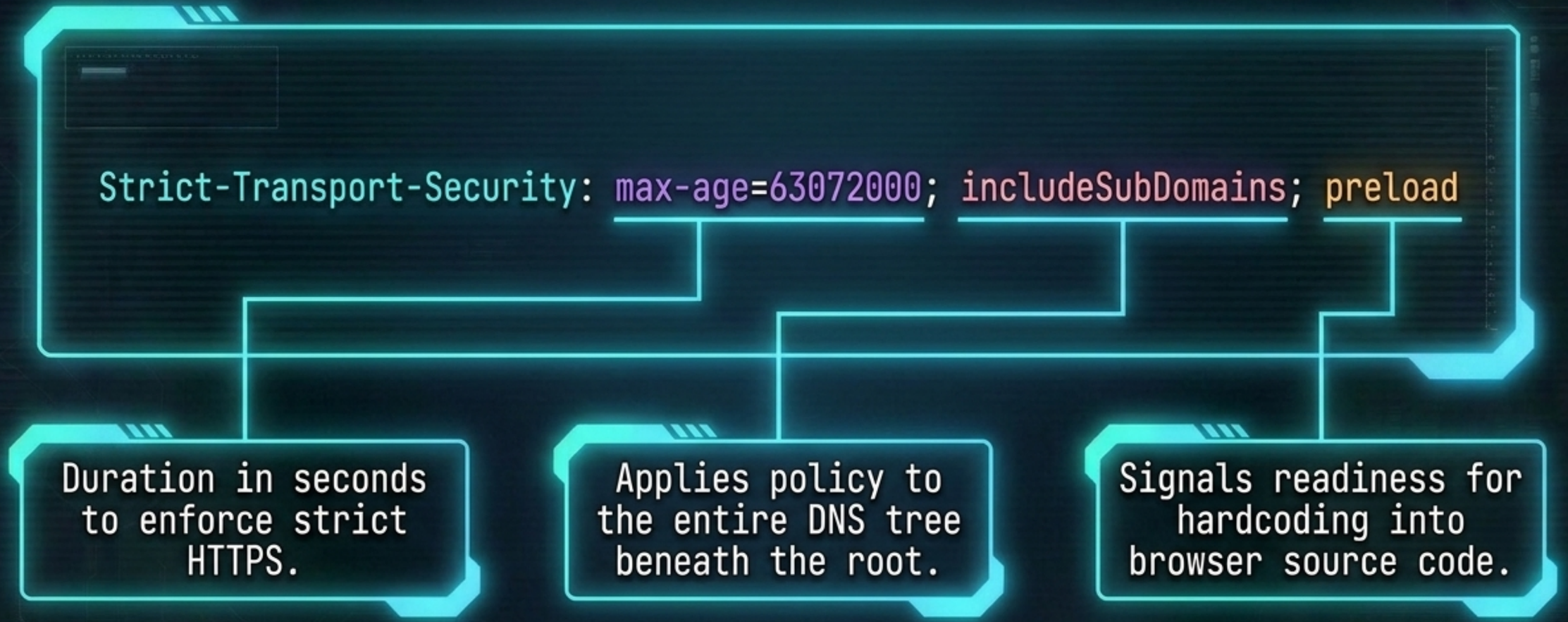


Attackers strip the HTTPS upgrade, locking the user into a monitored cleartext session.

Gemini Notebook

Closing the Gap: Strict-Transport-Security (HSTS)

Instructs the browser to forcefully upgrade all future insecure links to HTTPS internally before packets ever leave the client machine.



Gemini Notebook

Preload Lists & The includeSubDomains Blast Radius

The first request vulnerability (RFC 6797).



The Preload Fix:
Hardcoding domains into browser source code secures the very first visit.

The Operational Hazard:
Applying includeSubDomains indiscriminately can instantly brick legacy internal dev environments that lack valid TLS infrastructure.

Gemini Notebook

Mutual TLS (mTLS) Handshake Mechanics

Moving from unilateral trust to bilateral cryptographic proof.

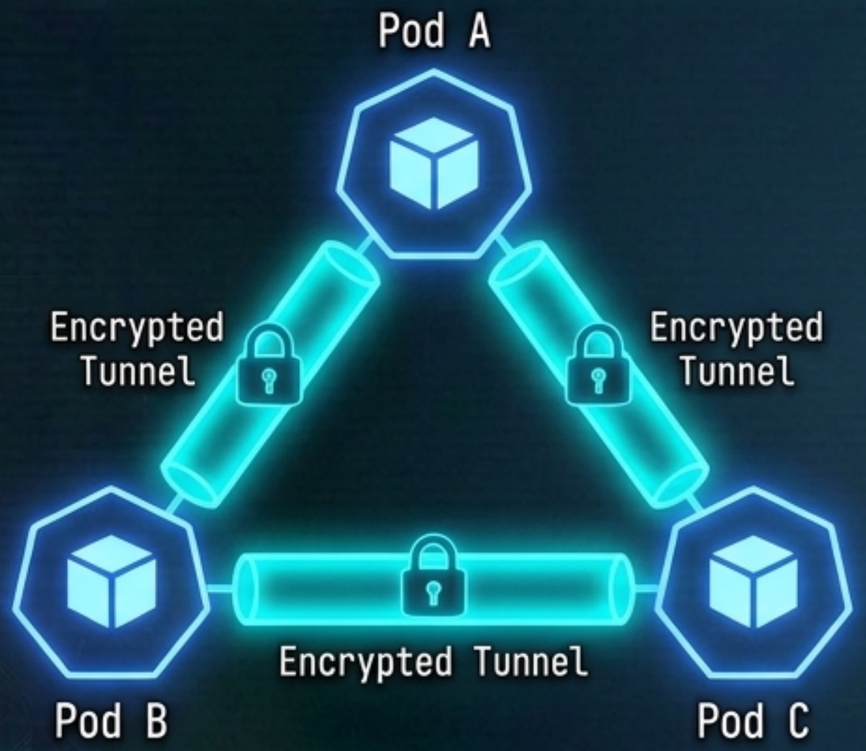


The server demands client authentication at the transport layer before processing any application logic.

Gemini Notebook

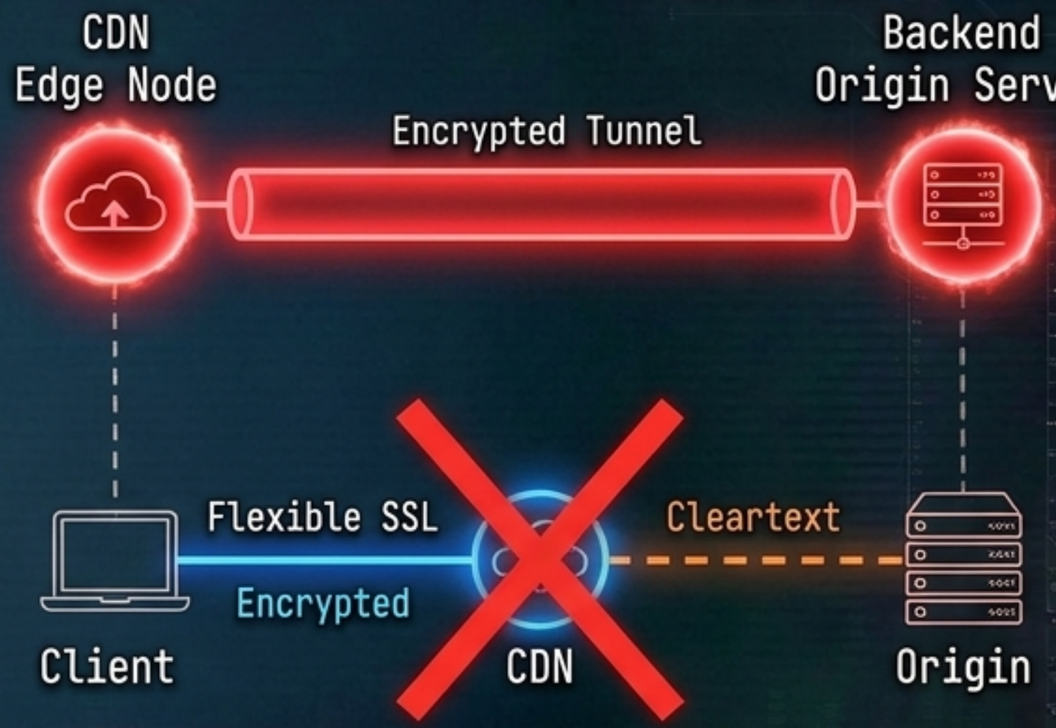
Workload Identity & CDN Origin Pulls

Service Mesh (SPIFFE/SPIRE)



Issues short-lived workload identities, removing static API keys between microservices.

Authenticated Origin Pulls

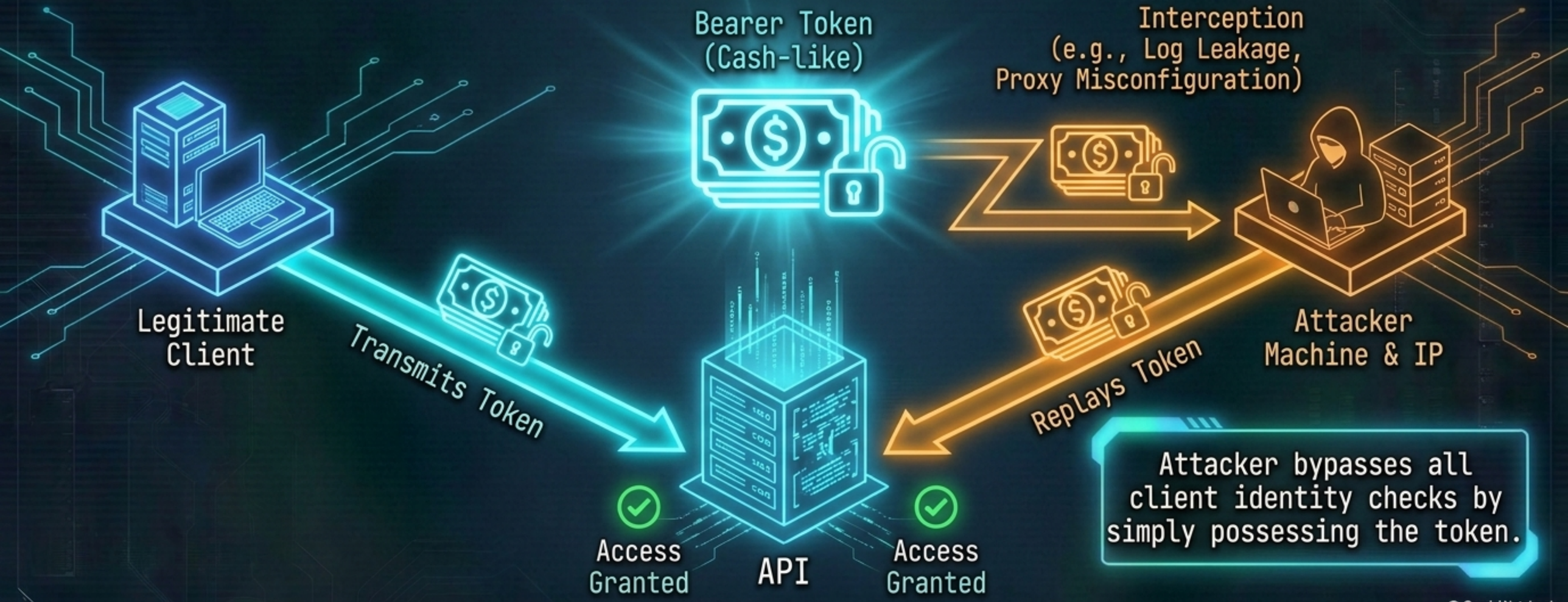


Eliminates the Flexible SSL trap.

Gemini Notebook

The Bearer Token Problem

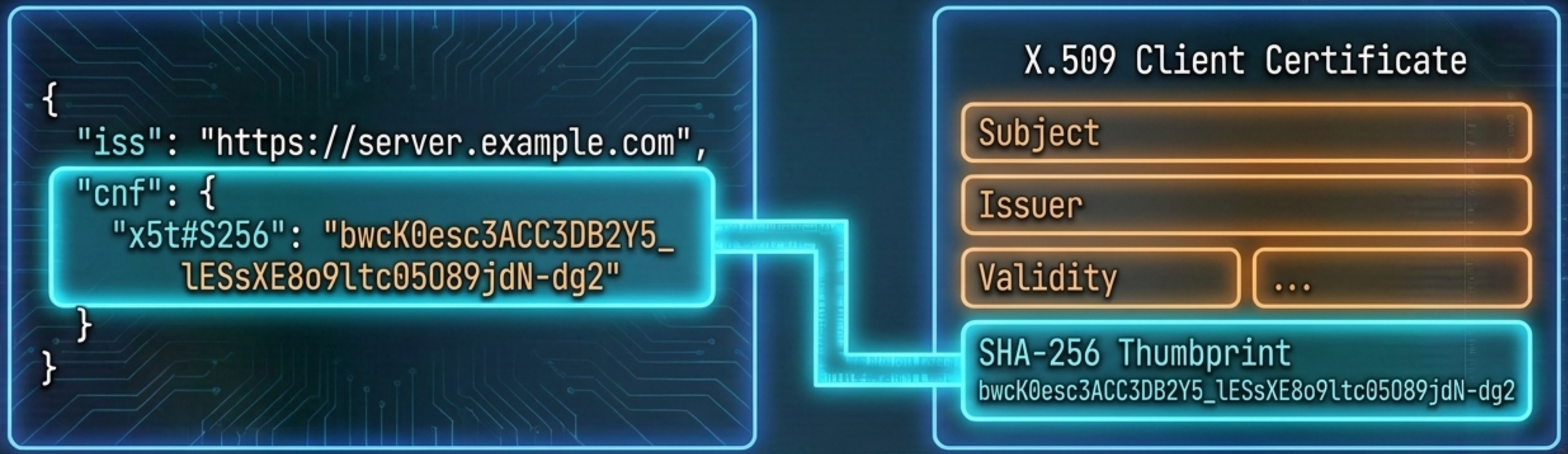
Traditional OAuth 2.0 Bearer tokens function exactly like cash.
Possession equals authorization.



Gemini Notebook

Certificate-Bound Access Tokens (RFC 8705)

Bind OAuth tokens to the client's mutual-TLS certificate.



A stolen token is instantly useless to an attacker because they do not possess the client's private TLS key.

Gemini Notebook

The Modern Configuration Matrix

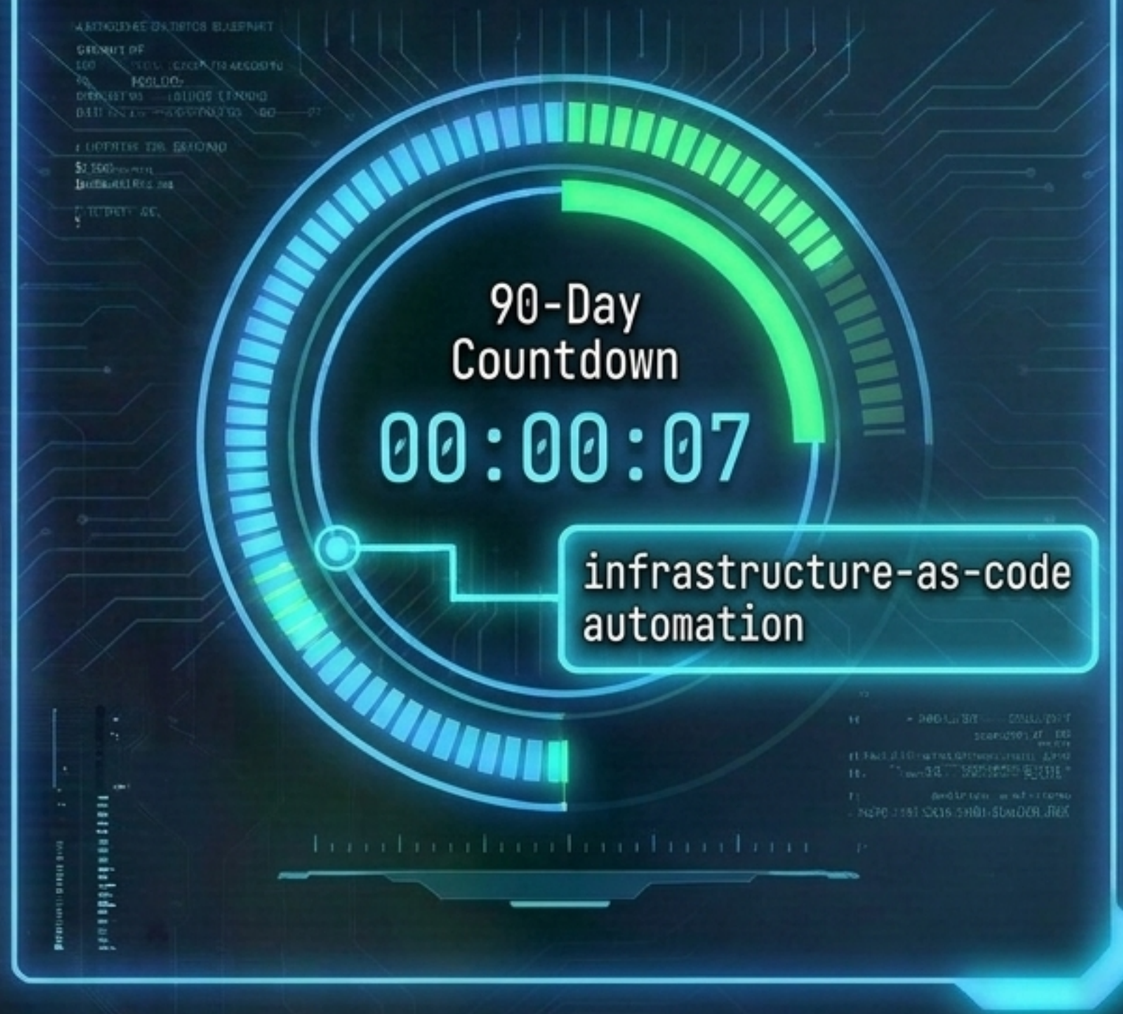
[DENY] ✗	[ALLOW] ✓
[✗] TLS 1.0 / TLS 1.1 / SSLv3	[✓] TLS 1.3 (Enforce as primary)
[✗] Static RSA Key Exchange & Cipher Suites	[✓] TLS 1.2 (Restricted strictly to AEAD ciphers)
[✗] CBC Block Ciphers (e.g., AES-CBC)	

Middlebox Note: Use RFC 8446 Appendix D.4 compatibility mode for legacy proxy traversal.

Gemini Notebook

Operational Rigor & Post-Quantum Readiness

Automated Rotation Observability



Threat: Shor's Algorithm against classical cryptography

Remediation Blueprint:

Post-Quantum Reality:

- Begin phasing in Kyber-based hybrid key exchanges

X25519MLKEM768

- Defend against retroactive decryption by quantum adversaries.

Gemini Notebook

Master Architecture Synthesis

Trust Nothing. Authenticate Everything.

Security is not achieved via a single protocol.



HSTS
(Forced HTTPS Upgrade)

TLS 1.3
(1-RTT Ephemeral Exchange)

X.509
(Verified against CT Logs)

mTLS
(RFC 8705 Token Binding)

It is a layered, interdependent cryptographic mesh.

Every layer compensates for the threat model of the layer beneath it.

Gemini Notebook