API Keys and Privacy

Rich Salz, Mike Bishop, Marius Kleidl
IETF 123, 23 July 2025

draft-ietf-httpapi-privacy

API key leakage over HTTP

- Scenario:
    - Misconfigured client sends API keys over unencrypted HTTP
    - Server redirects to HTTPS and client follows
    - Client receives successful response
- But API keys were exposed over plain HTTP
- Client didn’t notice this problem

→ How can this be prevented/mitigated?

Server recommendations

- Use HSTS and HTTPS DNS records to prevent unencrypted HTTP requests
- Use `Secure` attribute in Cookies to only transmit them over HTTPS
- Block traffic on port 80 entirely
- Respond with 403 to unencrypted HTTP requests without redirect
- Revoke credentials that were sent over unencrypted HTTP (*)

Server recommendations

- Use HSTS and HTTPS DNS records to prevent unencrypted HTTP requests
- Use `Secure` attribute in Cookies to only transmit them over HTTPS
- Block traffic on port 80 entirely
- Respond with 403 to unencrypted HTTP requests without redirect
- Revoke credentials that were sent over unencrypted HTTP (*)
- (*) not necessary if the request only included digital signatures or message authentication codes (MACs) derived from credentials but not the credentials themselves (**new in -02**)

Client recommendations

- Query and follow HTTPS DNS records
- Respect HSTS header
- Respect `Secure` Cookie attribute
- Disallow unencrypted HTTP by default (*)
- (*) unless explicitly configured to do so

Next steps

- WGLC