STRIDE threat model for an authentication flow

Captured 2026-07-02T04:52:00Z · company tier · claude-fable-5 · https://gateway.ansvar.eu

Scenario

You are designing a new B2B authentication flow using OAuth 2.1 + OIDC + Keycloak. Your security architect wants a fast STRIDE narrative grounded in OWASP and STRIDE-patterns before committing to a full workflow run.

What was asked

```
Build a STRIDE threat model for the following authentication architecture: user → Keycloak → resource server → PostgreSQL. For each STRIDE category list threats and attack techniques, verification requirements, and control mappings; cite STRIDE patterns, MITRE CAPEC, OWASP, NIST 800-53 where available, and any EU product-security duties (CRA).
```

Answer

STRIDE threat model — OAuth 2.1 + OIDC + Keycloak authentication flow

Four components in scope: **user agent → Keycloak (auth server) → resource server → PostgreSQL**. Each STRIDE category below is grounded in one of five gateway searches from this run — the STRIDE threat-pattern library, MITRE CAPEC attack patterns (publisher: The MITRE Corporation, served with capec.mitre.org source links), OWASP verification requirements, the security-controls catalog, and EU product law. A category with no fetched evidence is marked unresolved instead of being filled from model memory.

Spoofing

- **Authentication mechanism abuse.** [CAPEC-114](https://capec.mitre.org/data/definitions/114.html): an attacker "obtains unauthorized access to an application, service or device either through knowledge of the inherent weaknesses of an authentication mechanism" or by exploiting a flaw in it — the umbrella threat over every login path Keycloak exposes.
- **Authentication bypass.** [CAPEC-115](https://capec.mitre.org/data/definitions/115.html): the attacker "gains access to application, service, or device with the privileges of an authorized or privileged user by evading or circumventing an authentication mechanism". This row also grounds Elevation of privilege below.
- **Forged session credential.** [CAPEC-196](https://capec.mitre.org/data/definitions/196.html): "An attacker creates a false but functional session credential in order to gain or usurp access to a service."
- **Predictable token generation.** [Predictable Token Generation via Weak Random Number Generators (STRIDE-CRYPTO-RANDOM-001)](https://ansvar.eu/stride-patterns/patterns/STRIDE-CRYPTO-RANDOM-001): a weak random number generator lets an attacker "predict future values and forge authentication tokens. This allows complete account takeover". The matching test objective is [OWASP WSTG — Testing for Session Management Schema, Objective 2] (https://github.com/OWASP/wstg/blob/v4.2/document/4-Web_Application_Security_Testing/06-Session_Management_Testing/01-Testing_for_Session_Management_Schema.md): "Analyze and ensure that enough randomness exists to stop session forging attacks."
- **Default or weak credentials.** [Medical Device Identity Spoofing via Default Credentials and Weak Authentication (STRIDE-MEDDEV-SPOOF-005)](https://ansvar.eu/stride-patterns/patterns/STRIDE-MEDDEV-SPOOF-005): spoofing by "exploiting hardcoded default credentials, weak authentication mechanisms, or lack of device identity". A medical-device pattern by origin, but the mechanism applies to any service or client identity in this flow.
- **Email-channel spoofing.** [Email Spoofing via SPF/DKIM/DMARC Bypass (STRIDE-EMAIL-SPF-001)] (https://ansvar.eu/stride-patterns/patterns/STRIDE-EMAIL-SPF-001): "Business Email Compromise (BEC) attacks exploiting weak or misconfigured email authentication protocols". In scope wherever this flow sends password-reset or verification mail.
- **Login verification requirement.** [OWASP ASVS 4.0.3, V3.2.1] (https://github.com/OWASP/ASVS/blob/v4.0.3_release/4.0/docs_en/OWASP%20Application%20Security%20Verification%20Sta en.flat.json): "Verify the application generates a new session token on user authentication. (C6)" — the check that kills fixated pre-authentication sessions at the Keycloak login.

Tampering

- **Token replay.** [Tokenization Bypass and Token Reuse Attacks (STRIDE-PAYMENT-TOKEN-001)](https://ansvar.eu/stride-patterns/patterns/STRIDE-PAYMENT-TOKEN-001): where tokens lack binding restrictions, "attackers can replay them for fraudulent transactions". A payments-domain pattern; the replay mechanics transfer to any bearer token the resource server accepts.
- **Multi-step flow bypass.** [CAPEC-140](https://capec.mitre.org/data/definitions/140.html): applications that "require users to submit information through an ordered sequence of web forms" can have intermediate steps skipped — relevant if login, MFA enrolment, or consent is a multi-step sequence.
- **Unresolved:** no fetched row in this run covers input tampering at the PostgreSQL hop (for example SQL injection). Re-query before sign-off; nothing cited from memory.

Repudiation

- **Unresolved:** none of the five searches returned a repudiation pattern, verification requirement, or audit-logging control. Flagged rather than improvised.

Information disclosure

- **Access-token theft.** [OAuth 2.0 Access Token Theft and Replay in Spring Boot and Express.js Applications (STRIDE-API-OAUTH-001)](https://ansvar.eu/stride-patterns/patterns/STRIDE-API-OAUTH-001): tokens exposed through insecure "storage, insufficient encryption, lack of token binding, and compromised service accounts".
- **Session sidejacking.** [CAPEC-102](https://capec.mitre.org/data/definitions/102.html): "Session sidejacking takes advantage of an unencrypted communication channel between a victim and target system" — the attacker "sniffs traffic on a network looking for session tokens". Forces TLS on every hop, including resource server → PostgreSQL.

Denial of service

- **Unresolved:** no fetched row addresses denial of service (rate limiting, lockout, resource exhaustion) in this run. Flagged rather than improvised.

Elevation of privilege

- **Operating as a privileged user.** [CAPEC-115](https://capec.mitre.org/data/definitions/115.html) again: a successful bypass ends "with the privileges of an authorized or privileged user".
- **Cited controls** from the security-controls catalog:

- [IAC-20 — Least-privilege logical access](https://ansvar.eu/security-controls/iac/IAC-20): every grant kept "aligned with the least-privilege principle". - [IAC-21 — Least privilege for processes](https://ansvar.eu/security-controls/iac/IAC-21): "Access is held to the minimum required, permitting only the processes needed" — the shape of the resource server's PostgreSQL role. - [IAC-16.3 — Step-up authentication for privilege changes](https://ansvar.eu/security-controls/iac/IAC-16.3): "Asking to alter a privilege level triggers an extra authentication check" — the control on the Keycloak-admin and role-change boundary.

Product-security duties (CRA)

If this authentication flow ships inside a product with digital elements, the threat model above is input evidence for the [Cyber Resilience Act, Annex I, Part I](https://eur-lex.europa.eu/eli/reg/2024/2847/oj#anx_I) — "ESSENTIAL CYBERSECURITY REQUIREMENTS … Cybersecurity requirements relating to the properties of products with digital elements". The premium guidance fan-out also returned [MDCG 2025-6](https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en) ("What cybersecurity measures are required by the AIA and MDR/IVDR?"), which ties medical-device cybersecurity duties to those horizontal requirements — relevant only if the product is a medical device.

Run notes — what did not resolve

- **NIST 800-53.** The prompt asked for NIST 800-53 citations. The security-controls corpus returned five catalog controls (IAC-20, CPL-03.3, IAC-21, IAC-16.3, AAT-29.2) — none carrying a NIST 800-53 control identifier in this run. Same gap as the 2026-05-14 capture: still unresolved, and no 800-53 IDs were cited from model memory.
- **Repudiation and Denial of service.** Zero on-point fetched rows; both categories are marked unresolved above.
- **Returned but excluded as off-scope** (not cited as grounding): an assessor-access control (CPL-03.3), an AI-agent scoping control (AAT-29.2), a batteries-regulation recital on digital product passports, and an automotive repair-access guidance note.

From the fetched evidence, the load-bearing checks for this architecture are: regenerate the session token on authentication (ASVS V3.2.1), generate tokens from a strong random source (WSTG Objective 2 + STRIDE-

CRYPTO-RANDOM-001), bind and encrypt stored tokens (STRIDE-API-OAUTH-001), TLS on every hop (CAPEC-102), and least privilege plus step-up authentication at the privilege boundary (IAC-20, IAC-21, IAC-16.3).

Tool calls

| # | Tool | Result | |---|------|--------| | 1 | `search` | 5 threat patterns — STRIDE-API-OAUTH-001, STRIDE-EMAIL-SPF-001, STRIDE-PAYMENT-TOKEN-001, STRIDE-MEDDEV-SPOOF-005, STRIDE-CRYPTO-RANDOM-001 | | 2 | `search` | 5 MITRE attack patterns via the search_capec_patterns fan-out — CAPEC-114, CAPEC-115, CAPEC-140, CAPEC-196, CAPEC-102 (capec.mitre.org, The MITRE Corporation) | | 3 | `search` | 2 results — ASVS V3.2.1 (new session token on authentication), WSTG-SESS-01 Objective 2 (session-ID randomness) | | 4 | `search` | 5 catalog controls — IAC-20, CPL-03.3, IAC-21, IAC-16.3, AAT-29.2; no NIST 800-53 identifiers in the returned rows | | 5 | `search` | 4 results via search + agency-guidance + case-law fan-out — CRA Annex I Part I, MDCG 2025-6, plus 2 off-scope rows (batteries-regulation recital, automotive repair-access guidance) |

Citations

| Type | Jurisdiction | Reference | URL | |------|--------------|-----------|-----| | threat-pattern | intl | STRIDE patterns — OAuth 2.0 Access Token Theft and Replay in Spring Boot and Express.js Applications (STRIDE-API-OAUTH-001) | <https://ansvar.eu/stride-patterns/patterns/STRIDE-API-OAUTH-001> | | threat-pattern | intl | STRIDE patterns — Email Spoofing via SPF/DKIM/DMARC Bypass (STRIDE-EMAIL-SPF-001) | <https://ansvar.eu/stride-patterns/patterns/STRIDE-EMAIL-SPF-001> | | threat-pattern | intl | STRIDE patterns — Tokenization Bypass and Token Reuse Attacks (STRIDE-PAYMENT-TOKEN-001) | <https://ansvar.eu/stride-patterns/patterns/STRIDE-PAYMENT-TOKEN-001> | | threat-pattern | intl | STRIDE patterns — Medical Device Identity Spoofing via Default Credentials and Weak Authentication (STRIDE-MEDDEV-SPOOF-005) | <https://ansvar.eu/stride-patterns/patterns/STRIDE-MEDDEV-SPOOF-005> | | threat-pattern | intl | STRIDE patterns — Predictable Token Generation via Weak Random Number Generators (STRIDE-CRYPTO-RANDOM-001) | <https://ansvar.eu/stride-patterns/patterns/STRIDE-CRYPTO-RANDOM-001> | | threat-pattern | intl | MITRE CAPEC-114 — abusing weaknesses of an authentication mechanism | <https://capec.mitre.org/data/definitions/114.html> | | threat-pattern | intl | MITRE CAPEC-115 — evading or circumventing an authentication mechanism | <https://capec.mitre.org/data/definitions/115.html> | | threat-pattern | intl | MITRE CAPEC-140 — bypassing an ordered sequence of web forms | <https://capec.mitre.org/data/definitions/140.html> | | threat-pattern | intl | MITRE CAPEC-196 — forging a false but functional session credential | <https://capec.mitre.org/data/definitions/196.html> | | threat-pattern | intl | MITRE CAPEC-102 — session sidejacking over unencrypted channels | <https://capec.mitre.org/data/definitions/102.html> | | guidance | intl | OWASP ASVS 4.0.3 — V3.2.1: new session token on user authentication | <https://github.com/OWASP/ASVS/blob/v4.0.3_release/4.0/docs_en/OWASP%20Application%20Security%20Verification%20Standaren.flat.json> | | guidance | intl | OWASP WSTG v4.2 — Testing for Session Management Schema, Objective 2 | <https://github.com/OWASP/wstg/blob/v4.2/document/4-Web_Application_Security_Testing/06-Session_Management_Testing/01-Testing_for_Session_Management_Schema.md> | | controls-catalog | intl | Security controls — IAC-20: Least-privilege logical access | <https://ansvar.eu/security-controls/iac/IAC-20> | | controls-catalog | intl | Security controls — IAC-21: Least privilege for processes | <https://ansvar.eu/security-controls/iac/IAC-21> | | controls-catalog | intl | Security controls — IAC-16.3: Step-up authentication for privilege changes | <https://ansvar.eu/security-controls/iac/IAC-16.3> | | regulation | eu | Cyber Resilience Act (Regulation (EU) 2024/2847), Annex I, Part I — Essential cybersecurity requirements | <https://eur-lex.europa.eu/eli/reg/2024/2847/oj#anx_I> | | guidance | eu | MDCG 2025-6 — cybersecurity measures required by the AIA and MDR/IVDR | <https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en> |

Generated by Ansvar AI Gateway. This is the same artifact a customer would receive.