TM911: Secure Password Reset (Security Use Case)

Actors: User, MenuMap System, Email Service (IdP/SMTP)

Description: A user securely resets their password via email-based multi-factor verification and strong password policy, mitigating account takeover.

Priority: High

Complexity: High

Security Focus: Prevent misuse cases such as credential stuffing and reset-link hijacking.

Trigger: User clicks “Forgot Password.”

Preconditions:

- User has a registered email.
- Email service operational; throttling and rate limits active.

Main Success Scenario:

1. User submits email on the reset form.
2. System validates rate limits and existence of the account without disclosing whether the email is registered (“If that email exists, we’ll send a link”).
3. System generates a signed, single-use, short-lived token with IP/device binding.
4. Email Service delivers a reset link and out-of-band 6-digit code.
5. User opens link, provides out-of-band code, and sets a new password meeting policy.
6. System invalidates all active sessions and stores password hash with pepper/salt.

7. System confirms success and notifies the user via email of the change.

Extensions / Exceptions:

- 2a. **Rate limit exceeded:** System shows generic delay message and logs event.
- 3a. **Token reuse/expiry:** System rejects with generic error; offers to request a new link.
- 4a. **Email not received:** User can resend after cooldown.
- 5a. **Weak password:** System rejects with policy hints; requires strong password.

Postconditions:

- Password updated; sessions rotated; audit trail written; impossible-travel checks enabled on next login.

NFRs:

- **Security:** OWASP ASVS 2.1/2.2; signed tokens (JWE/JWS), TLS, CSRF protection on forms.
- **Privacy:** No account enumeration; minimal PII in emails.
- **Availability:** Reset service resilient; queued email retries (exponential backoff).
- **Auditability:** All steps logged with user-visible security log.