IA.L2-3.5.4

Identification & Authentication

Replay-Resistant Authentication

"Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts."

Objectives

[a]
Replay-resistant authentication mechanisms are implemented for network access to privileged and non-privileged accounts.

Key Discussion Points

What Is Replay?:
An attacker captures authentication traffic and replays it later to gain access — static passwords sent in cleartext are vulnerable.

Nonces and Challenges:
Kerberos, TLS, and TOTP all resist replay because each session uses a unique token — the captured credential cannot be reused.

MFA Helps:
MFA with TOTP (3.5.3) often satisfies 3.5.4 simultaneously — 30-second tokens expire too fast to replay.

Insecure Protocols:
NTLM, Telnet, and basic HTTP do not resist replay — their use on CUI systems is a direct finding under this control.

Assessment Methods

EXAMINE

Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings; system audit logs; list of privileged system accounts.

INTERVIEW

Personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system or network administrators; system developers.

TEST

Mechanisms supporting or implementing identification and authentication capability or replay-resistant authentication mechanisms.

IA.L2-3.5.4

IDENTIFICATION & AUTHENTICATION — Replay-Resistant Authentication

Plain English

What this control is really saying:

If an attacker intercepts your authentication traffic and can replay it — send it again later to get in — your authentication mechanism is not replay-resistant. This control requires protocols that make captured credentials useless: Kerberos, TLS, and time-based tokens all qualify. Static passwords over unencrypted protocols do not.

How it is used:

- All Windows domain authentication uses Kerberos — NTLM is disabled via Group Policy on all CUI systems.
- All web-based CUI applications require HTTPS/TLS — plain HTTP connections are rejected at the reverse proxy.
- VPN and remote access use MFA with time-based OTP — each session token expires in 30 seconds and cannot be replayed.
- The SSP documents the authentication protocols in use and confirms that insecure protocols (NTLM, Telnet, basic HTTP) are prohibited.

Real World Example

The Scenario

Acme Defense uses Windows Active Directory for authentication. NTLM is allowed as a fallback on all domain systems. An internal web app used for project tracking runs on HTTP with basic authentication — no HTTPS has been configured.

What the assessor finds

NTLM is enabled and in use on three systems — captured NTLM hashes could enable pass-the-hash attacks. The project tracking app transmits credentials in cleartext over HTTP. Neither mechanism resists replay attacks.

SPRS Score Impact

3.5.4 carries a point value of 5. NTLM and cleartext protocols remain in widespread use in DIB environments — and pass-the-hash attacks exploiting NTLM are a well-documented APT technique targeting defense contractors.

What Good Looks Like

Kerberos enforced for domain auth with NTLM disabled, all web apps require TLS, remote access uses time-based tokens, insecure protocols blocked at network and host level, replay-resistant mechanisms documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ NTLM not disabled

Windows authentication falls back to NTLM — captured NTLM hashes can be passed or cracked, not truly replay-resistant.

✗ Plain HTTP in use

Internal web applications use HTTP — basic auth credentials are transmitted in clear text and can be captured and replayed.

✗ Static session tokens

Web applications issue non-expiring session cookies — a stolen token grants access indefinitely without re-authentication.

✗ Telnet or FTP still used

Legacy protocols transmit credentials in cleartext — every session is replayable by anyone with access to the network.

✗ VPN using pre-shared keys

Site-to-site VPN uses a static pre-shared key — it is not time-based and does not provide replay resistance.