IA.L2-3.5.11

Identification & Authentication

Obscure Feedback

"Obscure feedback of authentication information."

Objectives

[a]
Authentication information is obscured during the authentication process.

Key Discussion Points

Mask the Input:
Displaying asterisks or dots as each character is typed is the standard — this is the default behavior on most modern login screens.

Shoulder Surfing:
The threat this control addresses is an observer watching as someone types their password — a real risk in shared office environments.

Mobile Devices:
Small device keyboards increase typo risk — briefly displaying the character before masking it is acceptable on mobile per the guide.

All Auth Mechanisms:
Applies to any authentication input field — not just Windows login, but web apps, VPN portals, and application login screens too.

Assessment Methods

EXAMINE

Identification and authentication policy; procedures addressing authenticator feedback; system security plan; system design documentation; system configuration settings; system audit logs.

INTERVIEW

Personnel with information security responsibilities; system or network administrators; system developers.

TEST

Mechanisms supporting or implementing the obscuring of feedback of authentication information during authentication.

IA.L2-3.5.11

IDENTIFICATION & AUTHENTICATION — Obscure Feedback

Plain English

What this control is really saying:

When someone types a password, the characters should not be visible on screen. An observer walking by, a security camera, or someone intentionally looking over a shoulder could capture the password just by watching. This control requires that all authentication input fields mask what is being typed — the classic asterisk or dot substitution.

How it is used:

- All Windows login screens and application login forms display asterisks as characters are typed — plaintext password entry is not available.
- Web applications are tested annually to confirm that all authentication fields obscure input — any field that displays plaintext is flagged immediately.
- Mobile device apps briefly display each character for one second then mask it — consistent with the guide's exception for small-keyboard devices.
- The SSP documents the obscuring mechanism used for each system and application type, including the mobile device exception.

Real World Example

The Scenario

Acme Defense uses an older CNC machine configuration utility that was installed five years ago. Nobody has ever verified whether the application's login screen obscures password entry. The utility is used in a shared workspace where multiple operators work at the same station.

What the assessor finds

The CNC utility login screen displays the password in plaintext as it is typed. The IT admin was unaware — the application has been in use for years. Multiple operators share the workstation, creating a direct shoulder-surfing risk in a physically accessible production environment.

SPRS Score Impact

3.5.11 carries a point value of 1. While low-weighted, this control is often where assessors find legacy application gaps — a login field that displays plaintext is a visible, demonstrable finding with no remediation complexity.

What Good Looks Like

All authentication input fields mask entry with asterisks or dots, web apps tested for obscuring behavior, mobile exception applied consistently, legacy systems evaluated and documented, SSP reflects obscuring mechanism for all authentication interfaces.

Common Gaps

What assessors actually find in the field:

✗ Password visible on entry

An application login field displays the password in plaintext as the user types — visible to anyone nearby.

✗ Show/hide toggle defaults to show

A web app has a 'show password' toggle that defaults to visible — users frequently leave it on in shared environments.

✗ Terminal/CLI tools display input

A command-line configuration tool echoes password characters to the terminal during entry — visible in the scrollback buffer.

✗ Legacy app not evaluated

An older industrial control system login screen has not been reviewed — nobody knows if it obscures authentication input.

✗ Screen recording captures creds

Remote support sessions use screen sharing without masking authentication fields — password entry is recorded in the session log.