What is key-based authentication, and why do stolen keys grant lasting access?

Short answer: Key-based authentication proves identity with a cryptographic private key instead of a password — used by SSH, many VPNs, and file transfer clients. A stolen private key grants access without any password or MFA prompt, and because keys are rarely rotated, that access can persist for a very long time.

How it works

You hold a private key; the server holds the matching public key. At connection time the server issues a challenge only the private key can answer. The key itself never crosses the network.

This is genuinely stronger than passwords — it resists guessing, phishing, and reuse. Its weakness is different: **everything depends on the private key file staying private.**

Why a stolen key is so durable

- **No password prompt.** The key *is* the credential.
- **Frequently no MFA.** Key auth often stands alone, particularly for automated systems.
- **Rarely rotated.** Passwords expire on a schedule; keys commonly live for years.
- **Predictable storage.** Standard directories and VPN client configuration paths.

A stolen key is a quiet, durable back door that produces no failed logins and looks entirely legitimate.

Protection

VPN and key-based authentication material are explicitly among the protected identity categories. Access is evaluated at the kernel level, so a program harvesting key files is stopped — denied or fed fake data if it is a trusted program overreaching, rejected or suspended if it is unknown or compromised — before the key leaves the machine.

Revision #3
Created 2026-07-20 19:24:29 UTC by Dennis Underwood
Updated 2026-07-21 19:32:42 UTC by Dennis Underwood