CS-009 · Foundations

Core Security Principles

The design principles, like least privilege and fail secure, behind good security decisions.

Executive Summary

Core security principles are time-tested design ideas that guide sound security decisions, such as least privilege, separation of duties, fail secure, and keeping designs simple. They are not tools or products but rules of thumb that help teams build systems that are resilient by design. Understanding them helps professionals reason about security consistently across any technology.

What It Is

Core security principles are a set of foundational ideas, refined over decades, that describe how to design and operate secure systems. Least privilege means giving each user, process, or system only the access it truly needs. Separation of duties splits sensitive actions across people so no one person can act alone. Defense in depth layers controls so no single failure is fatal. Fail secure means a system defaults to a safe, closed state when something goes wrong. Other widely cited principles include keeping designs simple, avoiding reliance on secrecy of design, minimizing the attack surface, and complete mediation, which means checking every access rather than trusting a past check.

Why It Matters

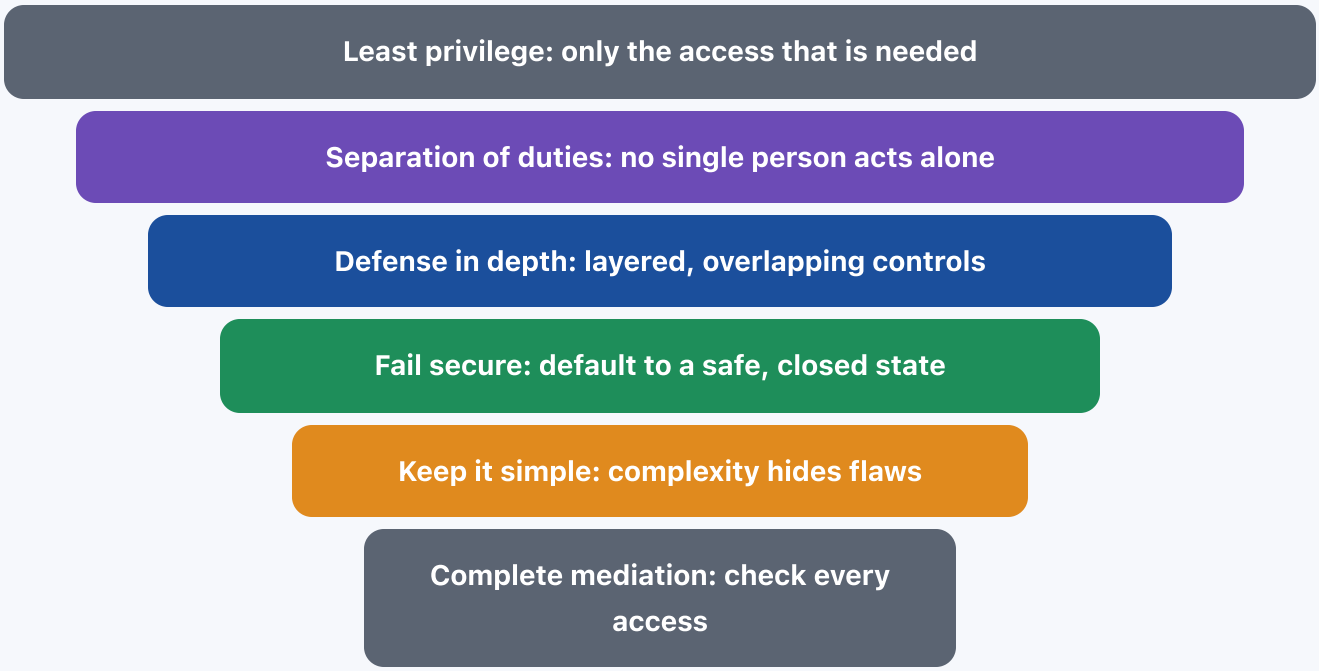
Technologies change constantly, but these principles endure, which makes them a durable way to reason about security. A professional who internalizes them can evaluate an unfamiliar system quickly by asking whether it grants least privilege, whether it fails safely, and whether its design is needlessly complex. Applying principles early, during design, is far cheaper than bolting on security later. For organizations, principled design reduces the number and severity of

weaknesses. For careers, these principles appear throughout certifications and interviews and underpin the entire practice of secure design.

How It Works

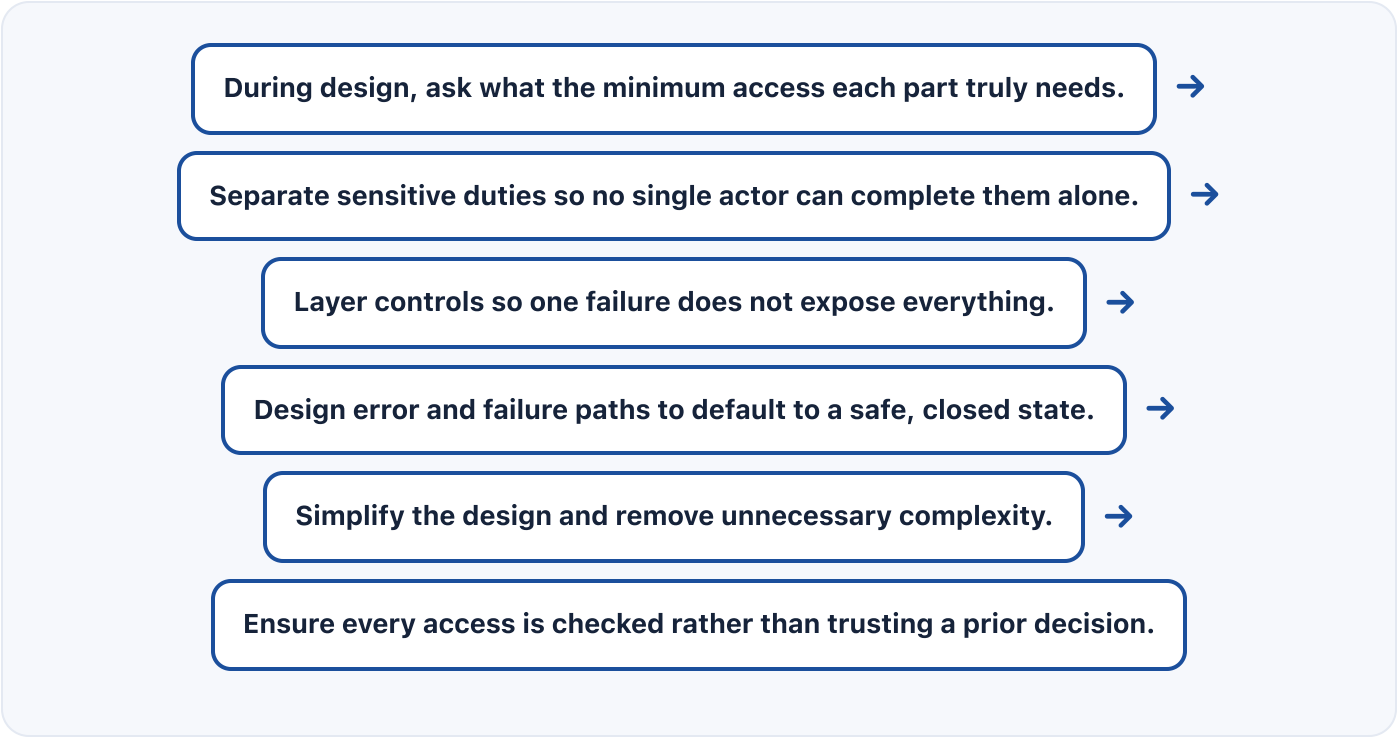
Principles are applied as questions and constraints during design, review, and operation. When granting access, teams ask what the minimum needed is and grant only that. When designing a sensitive workflow, they separate duties so approval and execution are not the same person. When handling errors, they ensure failures leave the system closed rather than open. When reviewing an architecture, they look for unnecessary complexity that hides flaws. These principles reinforce one another: least privilege limits the damage of a breach, defense in depth ensures a single failure is survivable, and complete mediation ensures access is always checked. Together they form a consistent way of thinking rather than a checklist to complete once.

Architecture Diagram



Core principles wrap around a system, each shaping design decisions from access to failure behavior.

Visual Workflow



Common Attacks

- Privilege abuse when accounts have more access than needed
- Fraud enabled when one person controls an entire sensitive process
- Exploitation of a single control with no depth behind it
- Systems failing open and granting access during an error
- Bypasses hidden inside overly complex, hard-to-review designs

Common Mistakes

- Granting broad access for convenience and never trimming it
- Letting one person both request and approve sensitive actions
- Relying on secrecy of the design instead of sound controls
- Designing systems that fail open when something breaks
- Adding complexity that no one fully understands or can review

Best Practices

- Grant least privilege and review access regularly
- Separate duties for sensitive or high-value actions

- Layer controls so no single failure is catastrophic
- Design failure paths to fail secure by default
- Prefer simple, reviewable designs over clever complexity
- Check every access instead of trusting a previous decision

Quick Checklist

- [x] Access granted at least privilege and reviewed periodically
- [x] Separation of duties enforced for sensitive processes
- [x] Overlapping controls in place, no single point of failure
- [x] Error and failure states default to closed, not open
- [x] Design reviewed for unnecessary complexity
- [x] Access checks applied consistently, not skipped after first grant

Recommended Tools

Identity and access management (IAM)
Enforces least privilege and access reviews

Privileged access management (PAM)
Controls and separates high-risk administrative access

Workflow and approval systems
Support separation of duties for sensitive actions

Configuration and policy-as-code tools
Encode fail-secure defaults and consistent checks

Industry Standards

NIST SP 800-53
Controls reflecting least privilege, separation of duties, and more

NIST SP 800-160
Guidance on engineering trustworthy, principled systems

ISO/IEC 27001
Management system reflecting principled

access and control design

Career Relevance

Security design principles are foundational for security engineers, architects, developers practicing secure coding, and GRC analysts who assess whether designs are sound. They appear throughout entry and advanced certifications and are common interview material because they reveal whether a candidate can reason about security rather than only operate tools. AI governance professionals apply the same principles to how AI systems are accessed and controlled.

Interview Questions

- What does least privilege mean, and why is it so effective?
- Explain separation of duties with a practical example.
- What does it mean for a system to fail secure rather than fail open?
- Why is simplicity considered a security principle?
- What is complete mediation and why does it matter?

Related Certifications

CompTIA Security+ | **ISC2 CISSP** | **ISC2 Certified in Cybersecurity (CC)**

Further Reading

- NIST SP 800-53 Control Catalog
- NIST SP 800-160 Systems Security Engineering
- CISA: Secure by Design

Key Takeaways

- Core principles are enduring design ideas, not tools or products.
- Least privilege and separation of duties limit the damage of any compromise.
- Fail secure means defaulting to a safe, closed state on error.

- Simplicity and complete mediation make systems easier to secure and review.
- Applying principles at design time is far cheaper than fixing flaws later.

FAQ

What is the difference between least privilege and zero trust?

What does fail secure mean in plain terms?

Why is simplicity a security principle?

Related Careers

RELATED ROLES

Security Engineer | Security Architect | Grc Analyst

RELATED CERTIFICATIONS

CompTIA Security+ | ISC2 CISSP | ISC2 Certified in Cybersecurity (CC)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Core Security Principles**
3. Go deeper: Cybersecurity
4. Go deeper: The CIA Triad
5. Validate it: work toward **CompTIA Security+**

6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-002 The CIA Triad | CS-003 Defense in Depth | CS-004 Zero Trust | CS-010 Cyber Hygiene