1 Security Engineering

Security has many factors/attributes:

1. secure architecture: security concerns are part of the architecture.
2. threat modeling: with threat mitigation
3. eliminate vulnerabilities: no known security issues during deployment
4. future improvement: deprecate protocols, etc., that may become insecure.
5. least priviledge: run everything under the last priviledged roles
6. conservative default settings
7. avoidance of risky default settings: application does not bypass operating system security.
8. minimize attack surface: turn off services that are not used.
9. redunduncy: multiple threat mitigation—multiple layers.
10. deployment guidelines: how to securely deploy software. how to ensure what is deployed/running is secure.
11. deployment tools that allow patching securely.
12. analysis/administration tools to enable easier security cofiguration.
13. quick response to security reports.
14. monitor public channels for mentions of security vulnerabilities
15. engage with users to enable secure use of the system
16. train users to be midnful of security.
17. threat models:
    (a) spoofing: fooling authentication
    (b) tampering; comprimising integrity of system
    (c) disclosure: information leaking
    (d) denial of service.
    (e) elevation of priviledge; authroization
18. coding guidelines:

(a) validate input (size, values, etc.)

(b) keep it simple

(c) default deny (access based on permissions, not on exclusion).

(d) least priveledge

(e) sanitize data on output: be very careful with strings that to go to other systems, such as shells or relational database.