Secure Systems Design and Implementation

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

Policy types

- Confidentiality
- Integrity Policy
- Availability Policy

Secure Systems - Principles

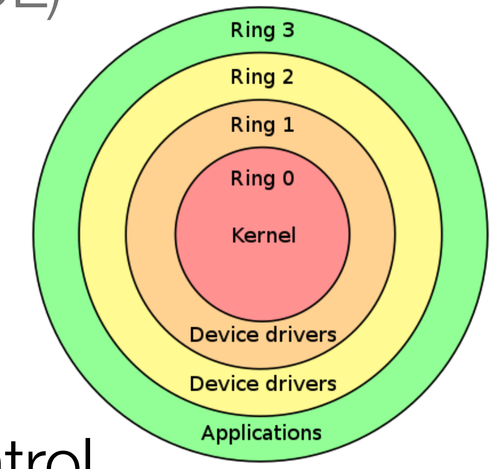
- Principle of Least Privilege
- Principle of Fail-Safe Defaults
- Principle of Economy of Mechanism
- Principle of Complete Mediation
- Principle of Open Design
- Principle of Separation of Privilege
- Principle of Least Common Mechanism
- Principle of Least Astonishment

Secure Systems - Entities

- What Is Identity?
- Files and Objects
- Users
- Groups and Roles
- Naming and Certificates

Secure Systems - Access Control

- Access Control Lists (ACL)
- Capabilities
- Locks and Keys
- Ring-Based Access Control
- Propagated Access Control

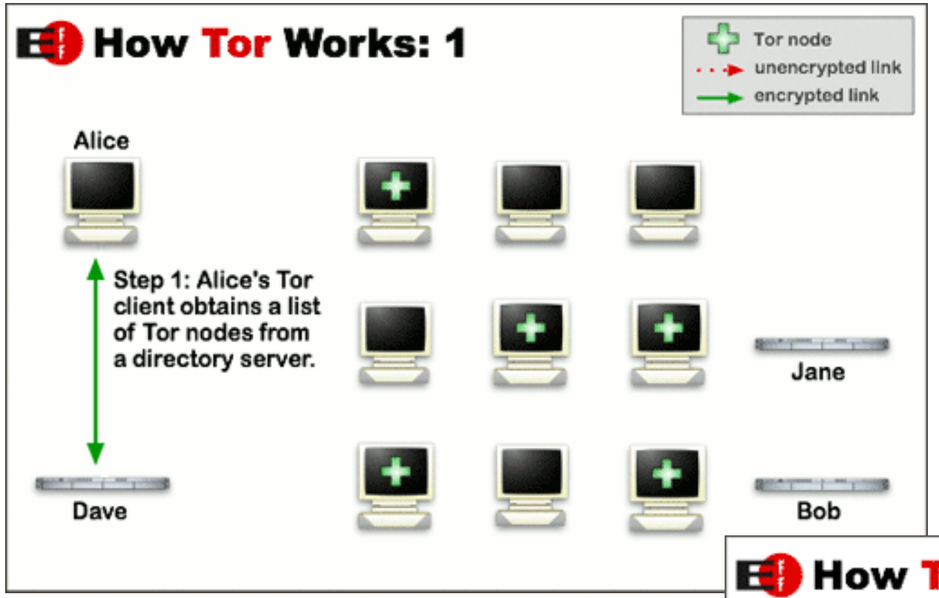


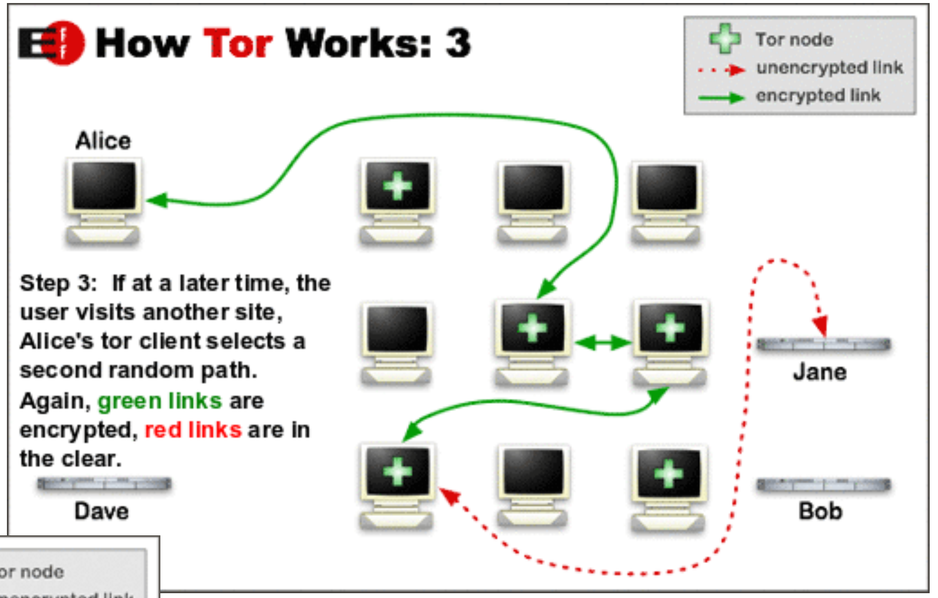
Secure Systems - In practice

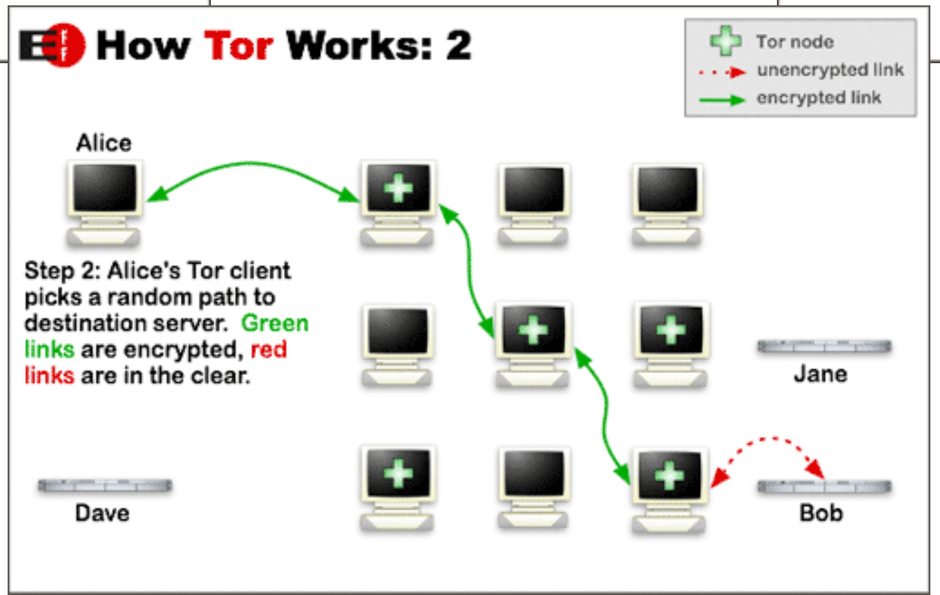
3 principles for developers

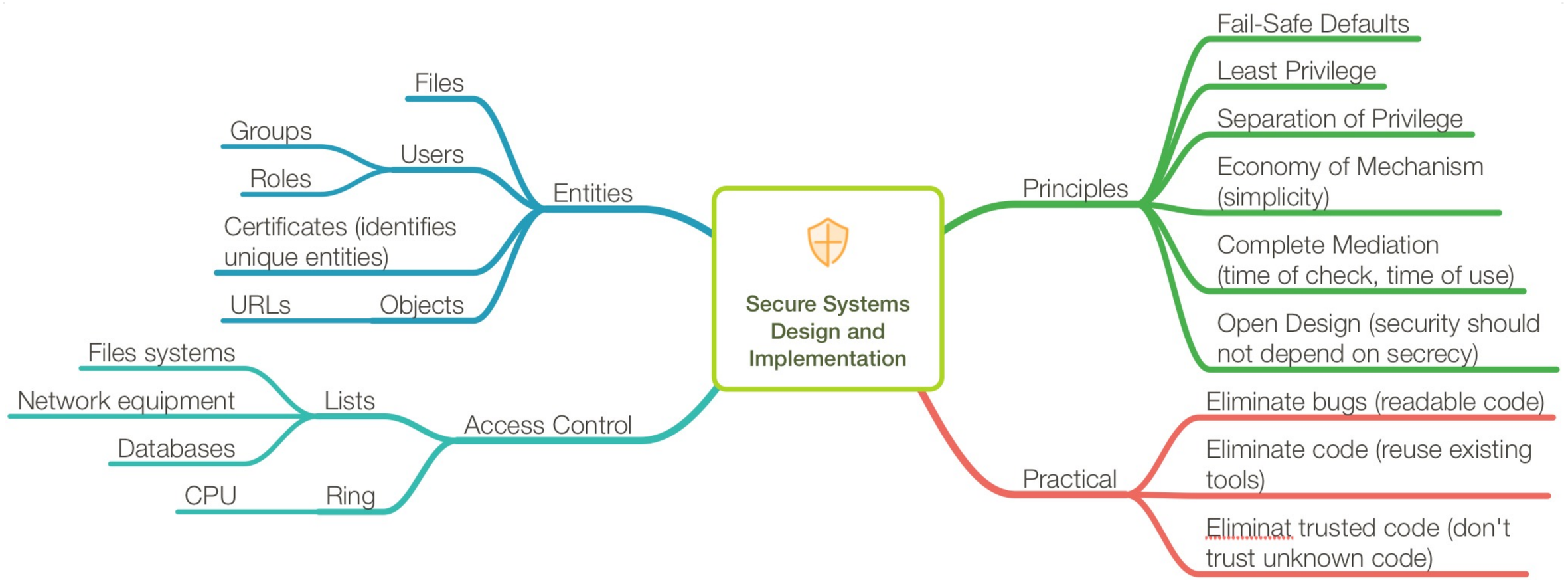
- Eliminate bugs
- Eliminate code
- Eliminate trusted code

Secure Systems - Tor








Secure Systems Design and Implementation
Entities
Files
Users
Groups
Roles
Certificates (identifies unique entities)
Objects
URLs
Access Control
Lists
Files systems
Network equipment
Databases
Ring
CPU
Principles
Fail-Safe Defaults
Least Privilege
Separation of Privilege
Economy of Mechanism (simplicity)
Complete Mediation (time of check, time of use)
Open Design (security should not depend on secrecy)
Practical
Eliminate bugs (readable code)
Eliminate code (reuse existing tools)
Eliminat trusted code (don't trust unknown code)