Secure Design Principles

SAND2014-18623C

Build it Right

- Be Explicit
- Work Factor
- Understand Attack Surfaces
- Compromise Recording
- Fail-safe Defaults
- Embrace Change

Know What You're Doing

- Effectiveness
- Encrypt Correctly

Be Flexible

- Continuous Improvement
- Design for Iteration
- Open Design

Keep it Simple

- Adopt Simplifications
- Economy of Mechanism

Keep it Running

- Availability
- Appropriate Resources

Have Trust Issues

- Trustworthy Authentication
- Never Assume Trust
- Authorize after Authentication
- Defense in Depth
- Chain of Control
- Deny by Default
- Transitive Trust
- Complete Mediation
- Accountability
- Non-repudiation
- Least Privilege

Don't Tell the Whole Story

- Separation of Duty
- Separation of Privilege
- Least Common Mechanism

Be a Control Freak

- Access Controls
- Flow Controls
- Inference Controls

Manage Your Assets

- Manage Sensitive Data
- Reduce Sensitivity
- Anonymization
- Separate Data and Control
- Reduce Exposure
- Validate Information
- Minimize Secrets
- Encryption

Users Come First

- ConsiderYour Users
- Psychological Acceptability
- Least Astonishment

Protect as Little as Necessary

- Timeliness
- Adequate Protection

Protect End-to-End

- Weakest Link
- Easiest Penetration

Secure By Design