



Non-Trusted

Majority of software
Operating system
Graphics
Applications
Data processing
etc

Trusted Software

Provision of security services
Small, well reviewed code

Trusted Software

- Crypto functions
- Key management
- Attack detection
- Sensitive data