

Highlights : Memory Protection

- Virtual memory (pages and segmentation)
- Tagged architecture
- Data access rules
- Stack switching
- Access Control Matrix
- Capabilities

Highlights : Authentication

- Dictionary attacks
- Brute force attacks
- Salting
- One-time passwords
(S/Key)
- Hardware support

Highlights : Trust Models

- Discretionary Access Control
- Mandatory Access Control
- Bell LaPadula model
- Biba (Strict Integrity) model
- Information Transfer Path
- Separation of Duty

Highlights : Trusted OS Design

- Principle of least privilege
- Separation of privilege
- Reference Monitors
- Trusted Computing Base
- Virtualization
- TCSEC (Orange Book)
- Common Criteria
 - Protection profile
 - Assurance requirement
 - Evaluation classes

Highlights : Malware

- Zero-day attack
- Rootkits
- Virus, worms, and defenses
- Buffer overflow attack
- Cross-site scripting
- Penetration testing
- fuzzing

Highlights : Network Security Protocols

- SSL
- SSH
- IPsec
 - Transport/tunnel mode
 - Authentication/encapsulation
- Perfect forward security

Highlights : Network Security Architecture

- VPN
- Firewalls and packet filters
- Traffic reconstruction
- Access Control List
- Network address translation
- Intrusion detection
- Honeypots