Principles of Data and System Security

Broad Topics

- Privacy, Secret, Public
- Security: confidentiality, Integrity
- Access Control
  - DAC: ACL, Authorization, Capabilities
  - RBAC, ORCON, Clinical Information systems
  - MAC: BLP, Biba,
  - Take Grant Systems

Topics

- Information Flow Control
  - Lattice Flow Model
  - Certification Semantics
  - Executional Monitoring
  - DLM Model
  - RWFM Model

ABAC

- ABAC
- Application –based Control
- Sandobxes, Virtual Machines

Language Security

- Certification Semantics
- Executional Monitoring
- Issues: Complex data Structures, Exceptions, failures, Concurrency, nondeterminism, Critical Embedded Systems

Database Security

OS Security

- Linux
- SELinux
- RunTime Monitors
  - Issue with ACL and Capabilities

Vulnerabilities

- Vunerabilities
- Attacks

Malware Detection

- Classes
- Detection: syntactic, semantic, behavioural
- SCADA Malware: Stuxnet
- Tainting, Clustering
- Fuzzing

Security Protocols

Information Management