NETWORK SECURITY AND CRYPTOGRAPHY

Basic concepts: Information Systems reviewed; Batch Systems ; On-line Systems ;Wide Area Networks(WAN), Metropolitan Area Networks(MAN),Local Area Networks (LANs: applications types)

Security defined ; Roles.

Models: Characteristics of security models , Reference monitor concept, Formal Security Models - Harrison- Piazzo model, Ulman Model, Bell La-Fadila Model, Object-oriented Model, Clares Willson, Chines Wall Model,etc.

Information Flow , Role based access control. Covert channels, Security mechanisms in Operating Systems.

Policy Paradigm: Meta policies.

Implementing a security model , formal specifications and verification methodologies. Targets; Facility , Hardware , Software ,Applications, Data Communications, Procedures (Administrative), Personnel.

Threats to Security: Areas of vulnerability, Physical Security, Data Security, Systems Security, Computer System Security, Communication Security, Personnel Security Threat Perpetration: Sources. Manmade, accidental. Threat prevention measures. Identity verification , Cryptography. Disaster recovery and Contingency Plan , Security Management , The future of Computer Security.

Books :

1. Security & Protection in Information Systems by Grissonnanche, North Holland
2. Cryptography and Data Security by Denning, Addison Wesley.
3. Computer Security Management by Frocht, Boyal & Frasev.
4. Security architecture for open Distributed systems by Muflic, JohnWiley.
5. Network Security by Kacifman & Perlman, PHI.
6. Http//www.Theory.les.MIT.edu/Rivest