Security Architecture for Open Systems Interconnection for CCITT Applications

1. **CCITT** has identified a need for a series of Recommendations to enhance security within the Open Systems Interconnection architecture. The term "security" is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. Vulnerability is any weakness that could be exploited to violate a system or the information it contains and threat is a potential violation of security.

2**. Recommendation X.200** describes the Reference Model for open systems interconnection (OSI). It establishes a framework for coordinating the development of existing and future Recommendations for the interconnection of systems.

3. **The objective of OSI** is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved. At various times, security controls protect the information exchanged between the application processes.

4. Recommendation X.800:

This Recommendation uses the following terms drawn from the respective International standards:

- Connectionless-mode transmission (ISO 7498/AD1)
- End system (Rec. X.200/ISO 7498)
- Relaying and routing function (ISO 8648)
- Management information base (MIB) (ISO 7498-4)
- In addition, the following abbreviations are used:
- OSI open systems interconnection;
- SDU for service data unit;
- SMIB for security management information base; and
- MIB for management information base.

4.1 The relationship of services, mechanisms and OSI layers

OSI Layers	Services	Mechanism
Physical	a) Connection Confidentiality b) Traffic Flow Confidentiality	Total encipherment of the data stream
Data Link	a)Connection Confidentiality b)Connectionless Confidentiality	The encipherment
Network	a) Peer Entity Authentication b) Data Origin Authentication Access Control service; d) Connection Confidentiality; e) Connectionless Confidentiality f) Traffic Flow Confidentiality g)Connection Integrity without recovery h) Connectionless Integrity	a) Protected password exchange and signature b) Encipherment c) Access control d) Routing control e) traffic padding f) data integrity
Transport	a) Peer Entity Authentication; b) Data Origin Authentication; c) Access Control service; d) Connection Confidentiality; e) Connectionless Confidentiality f) Connection Integrity with Recovery g) Connection Integrity without Recovery h) Connectionless Integrity.	a) Protected password exchange and signature b) Encipherment c) Access control d) Routing control e) Data integrity

Session	No Security Services are provided	Not Applicable
Presentation	a) Connection Confidentiality b) Connectionless Confidentiality c) Selective Field Confidentiality d)Traffic Flow Confidentiality e)Peer Entity Authentication f)Data Origin Authentication g)Connection Integrity with Recovery h)Connection Integrity without Recovery j)Selective Field Connection Integrity k) Connectionless Integrity p) Non-repudiation with Proof of Delivery.	a) Syntactic transformation b) Encipherment c) Signature mechanisms d) data integrity e) notarization
Application	a) Peer Entity Authentication b) Data Origin Authentication c) Access Control Service d) Connection Confidentiality e) Connectionless Confidentiality f) Selective Field Confidentiality g) Traffic Flow Confidentiality h) Connection Integrity with Recovery j) Connection Integrity without Recovery k) Selective Field Connection Integrity m) Connectionless Integrity n) Selective Field Connectionless Integrity p) Non-repudiation with Proof of Origin q) Non-repudiation with Proof of Delivery.	a) Authentication b) Signature c) Encipherment d) Traffic padding e) Lower layer data integrity f) signature

4.2 Security management

4.2.1. OSI **security management** is concerned with those aspects of security management relative to OSI and to security of OSI management. Management aspects of OSI security are concerned with those operations which are outside normal instances of communication but which are needed to support and control the security aspects of that communications.

4.2.2. Security management may require the exchange of security-relevant information between various system administrations, in order that the SMIB can be established or extended

There are **three categories of OSI security management** activities:
a) System security management;
b) Security service management; and
c) Security mechanism management.
This documents presents description of different types of threats e.g. Accidental threats, Intentional threats, Passive threats, Active threats and different types of attacks like Masquerade, Replay, Modification of messages, Denial of service, Insider attacks, Outsider attacks, Trapdoor, Trojan horse. Also it emphasis on the need of security policy, its role and its approaches in use of security architecture.