X.800 Model of Network Security

X.800 Security Architecture offers helpful network security model.   
X.800 focuses on security *attacks*, *mechanisms* and *services*.

|  |  |
| --- | --- |
| *security attack* | evasion of security services to violate the |
|  | security policy |
| *security mechanism* | mechanism designed to detect, prevent or |
|  | recover from a security attack |
| *security service* | service enhancing security of data processing |
|  | systems and information transfers of organisation |
|  | that uses security mechanisms to counter attacks |

Passive attacks on network security include

|  |  |
| --- | --- |
| *eavesdropping* | monitoring transmissions and reading messages |
| *traffic analysis* | analysing patterns in communication |

Passive attacks on network security

* are *harder* to detect because they don't alter data
* can be made more difficult by *padding* and *encrypting* data

Traffic analysis of encrypted data can

* determine *location* and *identity* of communicating hosts
* observe *frequency* and *length* of messages being exchanged

It can be used to *guess* at nature of communication taking place.

X800 Model: Security Attacks

2. Kind of attacks

Active attacks on network security involve measures such as

* some *modification* of data stream
* creation of a *false* data stream

Active attacks on network security are divided into

|  |  |
| --- | --- |
| *denial of service* | stops or inhibits normal use or management of service |
| *Masquerade* | pretence that entity is some other entity |
| *Modification* | modifying message to get unauthorised effect |
| *Replay* | capture & resending of data to get unauthorised effect |

Denial of service can

* have specific target - starving audit service of messages
* be targeted at whole network - disabling or overloading it

Masquerades usually involve other forms of attacks as well.   
Message modification

* involves altering, delaying or reordering message
* changes legitimate request to get illegitimate effect

Replay may involve

* capturing security credentials and using them illicitly
* reusing message to delude recipient who they are talking to

**X.800 Model: Security Services**

3.The services

X.800 Security Architecture for OSI identifies 5 types of service

|  |  |
| --- | --- |
| *Authentication* | authenticate communicating peer & data sources |
| *Access control* | protect against unauthorized use of resources |
| *Data confidentiality* | protect data from unauthorized disclosure |
| *Data integrity* | counter active threats to data's integrity |
| *Non-repudiation* | protect against false denials of handling data |

Authentication covers two security services

|  |  |
| --- | --- |
| *Peer entity authentication* | corroborate its claimed entity |
| *Data origin authentication* | corroborate its claimed data source |

Access control is X.800 service in its own right that controls

* who can access a resource
* conditions under which access occurs
* operations that may be performed on resource

Data confidentiality covers four security services

|  |  |
| --- | --- |
| *Connection confidentiality* | ensure secrecy on a connection |
| *Connectionless confidentiality* | ensure secrecy of a message |
| *Selective field confidentiality* | ensure secrecy of some data fields in |
|  | data on a connection or in a message |
| *Traffic flow confidentiality* | protection of information that might be |
|  | derived from observation of traffic flows |

**X.800 Model: Security Mechanisms**

4. The system

Network security mechanisms are either

* specific to network protocol layers
* pervasive

Specific security mechanisms cover

|  |  |
| --- | --- |
| *Encipherment* | encoding making data unreadable without key |
| *Digital signature* | signing process uses data confidential to signer |
|  | verification shows if signature made with data |
| *Access control* | using authenticated identity or data about user |
|  | to determine and enforce his access rights |
| *Data integrity* | using supplementary data that is function of |
|  | data to determine if data has been modified |
| *Authentication exchange* | data exchanged to ensure identity of user |
| *Traffic padding* | adding data to messages to stop traffic analysis |
| *Routing control* | rerouting data on secure paths to stop attacks |
| *Notarization* | using trusted 3rd party to assure security |  |  |  |  |  |  |

Pervasive security mechanisms cover

|  |  |
| --- | --- |
| *Trusted functionality* | using functions trusted by security policy |
| *Security labels* | marking of data by its security attributes |
| *Event detection* | detection of security related events like violations |
| *Security audit trail* | recording security data so audit is possible |
| *Security recovery* | recovery in response to event handling and |
|  | management functions |