Topic: ..... Date: ..... Page No: .....

DTU/2K16/MC/13 - Anish Sachdeva

Q2) Describe security services defined by the ITU-T(X.800) related to the security goals and attacks.

Ans2) The International Telecommunication Union- Telecommunication Standardization Sector (ITU-T) provides some security services and some mechanisms to implement those services.

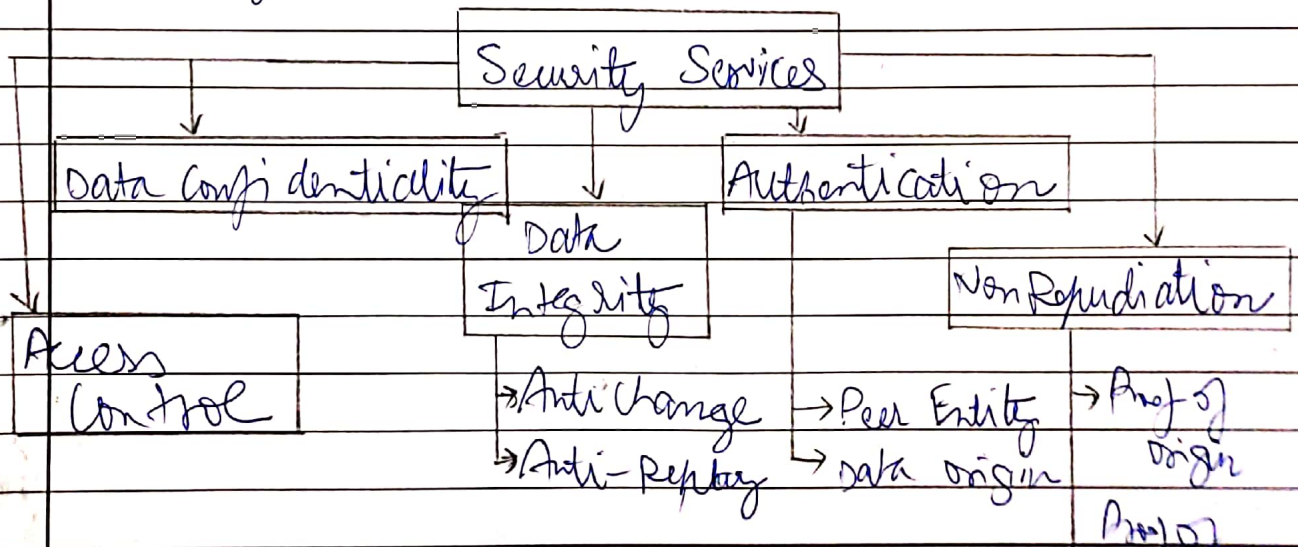
Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

Also a mechanism can be used in one or more services. We discuss them now:-

Security Services

ITU-T(X.800) has defined 5 services related to the security goals and attacks. The taxonomy of the services is given below.

Security Services



GOOD WRITE A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

It is easy to route one or more of these services to one or more of the security goals. It is also easy to see that these services have been designed to prevent the security attacks mentioned.

Data Confidentiality

Data confidentiality is defined to defend Disclosure attack. The service as defined by X.800 is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis attack.

- Data Integrity

Data Integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary. It may protect the whole message or a part of it.

- Authentication

This service provides the authentication of a party at the other end of the line. In connection-oriented communication, it provides authentication of the sender or reciever during the connection establishment (peer entity authentication). In connectionless communication it authenticates the source of the data (data origin authentication).

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

- **Non Repudiation**

Non Repudiation service protects against repudiation by either the sender or the reciever of the data. In non-repudiation with proof of the origin, the reciever of the data can later prove the identity of the sender if denied.

In non-repudiation with proof of delivery the sender of data can later prove the data were delivered to the intended recipient.

- **Access control**

Access control provides protection against unauthorized access to data. The term access in this definition is very broad and can involve reading, writing, modifying, executing programs and so on.

Q3) DTU/2K16/MC/13

* **Security Mechanisms**

ITU-T (x.800) also recommends some security mechanisms to provide the security services defined above. Following is the taxonomy of these services.

→ Encipherment
→ Data Integrity
→ Digital Signature
→ Authentication Exchange
→ Traffic Padding
→ Routing Control
→ Notarization
→ Access Control

GOOD WRITE
A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

- **Encipherment**

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today - 2 techniques Cryptography and Steganography - are used for enciphering.

- **Data Integrity**

The data integrity mech mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The reciever receives the data and the checkvalue. He creates a new checkvalue from the data and compares the newly created checkvalue with the one he has received. If the 2 checkvalues are the same, the integrity of the data has been preserved.

- **Digital Signature**

A digital signature is a means by which sender can electronically sign the data and the reciever can electronically verify the signature. The sender uses a process that involves proving that she owns a private key related to the public key and she has announced publically. The reciever uses the sender's public key to prove that the message is in deed signed by the sender who claims to have sent the message.

Scanned with CamScanner

Topic: ..... Date: ..... Page No: .....

- **Authentication Exchange**
  In authentication exchange two entities exchange some messages to prove their identities to each other. For example one entity can prove that she knows something that only she is supposed to know.

- **Traffic Padding**
  Traffic Padding means inserting some bogus data into the data traffic to thwart the adversary's attempts to use traffic analysis.

- **Routing Control**
  Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

- **Notarization**
  Notarization means selecting a third party (trusted) to control the communication between 2 entities. This can be done for example to prevent repudiation. The reciever can involve a trusted party to store the sender request in order to prevent the sender from later denying that she had made such a request.

- **Access Control**
  Access control uses methods to prove that a user has access rights to the data or resources owned by a system. Examples of proofs are passwords or PIN's.

GOOD WRITE
A Mark of Quality

Teacher Sign. .....

Scanned with CamScanner

· Relation Between Services & Mechanisms

The above table shows the relation between security services and mechanisms. The table shows that 3 mechanisms, Encipherment, digital signatures and authentication exchange can be used to provide authentication. The table also shows encipherment mechanism may be involved in three services (Data Confidentiality, Data Integrity, and Authentication)

Security Service	Security Mechanism
Data Confidentiality	Encipherment and Routing control
Data Integrity	Encipherment, Digital Signature, Authentication Exchanges
Authentication	Encipherment, Digital Signature, Authentication Exchange
Non-Repudiation	Digital Signature, Data Integrity and Notarization
Access Control	Access Control Mechanism

Scanned with CamScanner