

29th August '2020Cryptography & Network Security
MC - 407

Assignment - 1

DTU/2K16/MC/13 - Anish Sachdeva

(Q1) Describe different types of attacks threatening the confidentiality of information.

Ans 1)

Attacks Threatening Confidentiality

In general 2 types of attacks threaten the confidentiality of information: snooping and traffic analysis.

Snooping

Snooping refers to unauthorized access to or ~~intercept~~ interception of data. For example, a file transferred through the internet may contain confidential information.

An unauthorized entity may intercept the ~~transmission~~ transmission and use the contents for her own benefit.

To prevent snooping, the data can be made non-intelligible to the interpreter by using encryption techniques discussed in this book.

Traffic Analysis

Although encipherment of data may make it unintelligible for the interpreter, she can obtain some other type of information by monitoring online traffic.

For example, she can find the address (such as e-mail) address of the sender to the receiver. She can collect mass of requests and responses to help her guess the nature of the transaction.

Traffic analysis can also be performed by just visually seeing ~~the~~ the direction of the dish antenna that the country has pointed to. Just by observing the direction of a satellite dish and adversary such as Eve can figure out which country is the government in communication with. This is the reason why the satellite dishes and communication towers are covered.