MULTIMEDIA UNIVERSITY OF KENYA

FACULTY OF BUSINESS AND ECONOMICS

NAME: OWITI CHARLES

ADM. NO: BUS-242-063/2014

COURSE: BACHELOR OF BUSINESS INFORMATION TECHNOLOGY

UNIT: COMPUTER SECURITY AND CRYPTOGRAPY

LECTURER: MR. WAKHU J.G.

ASSIGNMENT: ATTACKS ON CRYPTOSYSTEMS

Attacking a cryptosystem

Correlation attack

It applies to a running key generator composed of several linear feedback shift register. The correlation attack is a divide and conquer technique. It aims at recovering the constituents of linear feedback shift register separately from the knowledge of some known plain text. Correlation attack exploits a statistical weakness that arises from choice of poor Boolean function. The attacker has access to both plaintext and ciphertext versions of the message. The main aim is to find the key that was used to encrypt the message. Once the key is found the attacker will be able to decrypt all the messages that had been encrypted using the key.

Dictionary attack

Attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext. It exploits the habit of users who choose passwords based on natural words. It is possible to use dictionaries containing thousands of words and to use this well known function until there is a match with the encoded password. This technique has proved immensely successful in attacking and compromising UNIX systems. Unfortunately, Windows systems are not immune from this type of attack. This is accomplished by obtaining a copy of the SMA file that contains the encrypted passwords, and as in the case of UNIX, comparing combinations of dictionary words until a match is found. Again, this is a popular technique for attacking this kind of system.

Man-in the middle attack

The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place. Host *A* wants to communicate to host *B*, hence requests public key of *B* and attacker intercepts this request and sends his public key instead. Thus, whatever host *A* sends to host *B*, the attacker is able to read. In order to maintain communication, the attacker re-encrypts the data after reading with his public key and sends to *B*. The attacker sends his public key as *A*'s public key so that *B* takes it as if it is taking it from *A*. By interjecting oneself into the path of secure communications or key exchange, it possible to initiate a number of attacks. An example is the case of an online transaction. A customer connects to what is thought to be an online bookstore but the attacker has hijacked the connection to monitor and interact with the data stream.

The customer connects normally because the attacker simply forwards the data onto the bookstore, thereby intercepting all the desired data. Also, changes to the data stream can be made to suit the attacker's needs.

In the context of key exchange, this situation is potentially even more serious. If an attacker is able to intercept the key exchange, he may be able to use the key at will (if it is unprotected) or substitute his own key.

It is managed by access controls of authorization and authentication, security policies and security management. Network security such as firewals.

Time attack

A timing attack allows the attacker to discover vulnerabilities in the security of a computer or network system by studying how long it takes the system to respond to different inputs. Timing vary depending upon on the encryption key because different systems takes slightly different amount of time to process different inputs. Timing attack looks at how long it takes a system to do something and uses statistical analysis to find the right decryption key to gain access.

This attack is protected by ensuring that all operations with a given algorithm takes the same time by quantizing the operations into a fixed time period.