Experiment No:16

**Aim**: To analyze working and performance of keylogger as fraudulent access to passwords and other confidential information.

**Theory**:

keyloggers

The expectations from computerized processes, applications and delivery channels are constantly on the rise these days. This necessitates a situation where in the computerized environments need to be totally secure, always available and be reliable to the core so that the growing expectations are fully met. However, many new technologies do surface which constantly pose a threat of one sort or the other. One such emerging technology which has great ramifications on the information security front is the usage of 'Keystroke Loggers'.

Keystroke logging (often called keylogging) is a diagnostic tool / device to capture the user's keystrokes. On the positive side, it can be beneficial to determine the causes of errors in computer systems, measure employee productivity, support law enforcement and espionage [for instance to obtain passwords or encryption keys for law enforcement and other purposes.

However, the flip side is that the keyloggers widely available on the Internet can be used to spy on the computer usage of others. Key logging can be achieved by both hardware and software means. Hardware keyloggers could be devices attached to keyboard cable or devices installed inside the keyboards. The former has the advantage of easy installing and they may go undetected for quite some time. The keylogger inside the keyboard (the keyboard of the target system) is the toughest to install and also is virtually undetectable unless specifically looked for. Software keyloggers are software applications specifically designed for the purpose and like any other computer program are distributed as a trojan horse or as part of a virus. An attacker connecting to a host machine to download logged keystrokes risks being traced. The most difficult task, therefore, for a keystroke logger is to escape being tracked while downloading data that has been logged. A trojan that sends keylogged data to a fixed e-mail address or IP address also risks exposing the attacker.

Currently there is no easy way to prevent key logging. However, users should constantly observe the programs which are installed on their systems. Anti-spyware applications are able to detect many keyloggers and cleanse them. Enabling a firewall does not stop keyloggers per se, but can possibly prevent transmission of the logged material over the net. Network monitors (also known as reverse-firewalls) are useful to alert users whenever an application attempts to make a network connection.

keylogger detection software is also available. Some of this type of software use "signatures" from a list of all known keyloggers. One drawback of this approach is that it only protects from keyloggers on the signature-based list, while the system remains vulnerable to other keyloggers. Other type of detection software analyzes the working methods of many modules in the computer system blocking many different types of keyloggers. One drawback of this approach is that even legitimate, non-key logging software is also blocked in this respect. Using the virtual keyboard wherever available would help prevent keylogger compromises as in such cases the keyboard is not being used for the input.

**Conclusion**:

Thus, we successfully analyze working and performance of keylogger as fraudulent access to passwords and other confidential information.