Unit 2. Task 5: Attacks to SSL Protocol

Javier Aguilera Aguilera 2º CFGS DAW

SSL is esentially a very secure and reliable protocol because it has a hard and madure theorical body but its implementations may have several errors. New criptoanalisis tecniques and the increased capacity of computation are the main factors that increase the vulnerability of SSL. Most attacks that affects SSL are Man-in-the-middle and identity thief attacks in social networks.

A vulnerability noticed in 2008 was a programmation flaw of SSL: Incorrect implementations of random functions used in openSSL/Debian. Other type of vulnerability is known as *Downgrade*, which occurs when an attacker force the user to use an older version of SSL. Another programmation flaw it based on the inclusion of the carácter NULL (/0) in the certificate name. It causes that all characters written after the NULL to be skipped and due to that, the identity thief can be made easily. A solution given is to denied all certificates whose nome contains NULL character.

The easiest method to break the security provided by SSL is to make the user thinks that he is using SSL where he does not in fact. An easy example is when in a Man-in-the-middle attack the attacker sends a false digital certificate as if he were a bank (for example). Another way is using SSLStrip an ingenious tool that automatic Man-in-the-middle attacks by substituting http instead of https.

Some recommendations given are:

- Keep your browser up to date.
- Use directly the url with https.
- Denied the access to a web when the certificate is not valid.