HW #4 - CNS Sapienza

Daniele Oriana 1457625

3 Dec 2015

20150910-Q3

TLS vs. IPSec
Q3.1 [2/30] Describe at a high level the main security goals of TLS.
Q3.2 [2/30] Describe at a high level the main security goals of IPSec.
Q3.3 [1/30] Describe an application/infrastructure scenario where TLS looks more useful than IPSec.
Q3.4 [1/30] Describe an application/infrastructure scenario where IPSec looks more useful than TLS.

Answer

Q3.1

Transport Layer Security (TLS) is a cryptographic protocol that provide security for communications over networks encrypting the segments of network connections at the transport layer end-to-end. It is able to prevent eavesdropping, tampering and message forgery and, in addiction, provides endpoint authentication and communications confidentiality over the internet using cryptography. One of the goals of TLS is to provide an authentication in typical end-user/browser usage, for this case it supports a unilateral type of authentication in wich only server is authenticated, is possible to obtain also a mutual authentication(but required the use of some certificates).

Q3.2

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications. It guarantees a type of security that we can imagine as a cut across protocol layers (therefore different from the several

application specific security mechanisms), we can say that the IP security represents the security between IP and TCP. So, one of the main security goals of IPSec is to guarantees a security that can be used by all applications, we can consider it as a sort of transversal security among applications. The most important targets of IPSec is to provide authentication, confidentiality and key management; in addiction we have to note that IPSec allows to encrypt and/or authenticate all traffic at the IP level. There are other benefits of this protocol, for example:

- a firewall/router provides strong security to all traffic crossing the perimeter
- is resistant to bypass
- is below transport layer, therefore transparent to applications
- can be trasparent to end users and allows to realize Virtual Private Networks
- can provide security for individual users if desired

Among the services offered by IPSec we can also mention: the prevention of unauthorized use of resource, the detection of an individual IP datagram, data origin authentication and rejection of replayed packet.

Q3.3

A possible protocol in which TLS is more suitable than IPSec is HTTPS, in fact in the HTTP transactions over the internet tipically only the server is authenticated, so TLS is perfect for this situation since it can provide some protection even if only one side of the communication is authenticated.

Q3.4

We find the predominant use of IPsec in the VPN creation. VPN (virtual private network) is a private telecommunications network, established between subjects using a public transmission system as transport infrastructure, such as the Internet network. So the definition of the VPN shows how the level of security provided by IPSec is perfect for the scenario involved.