Lecture 20: PGP, IPSec, SSL/TLS, and Tor Protocols

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

March 28, 2017
10:08am

Goals:

- PGP: A case study in email security
- Key management issues in PGP
- Packet-level security with IPSec
- Transport Layer Security with SSL/TLS
- **Heartbeat Extension** to the SSL/TLS protocol
- The Tor protocol for anonymized routing

CONTENTS

20.1: INFORMATION SECURITY FOR NETWORK-CENTRIC APPLICATIONS

- As mentioned earlier in these lecture notes, ensuring *information security* in network-centric applications requires paying attention to:
  - authentication
  - confidentiality
  - key management

- As shown in Figure 1, information security may be provided at different layers in the internet suite of communication protocols:
  - We can provide security services in the Network Layer by using, say, the IPSec protocol, as shown in part (a) of Figure 1. While eliminating (or reducing) the need for higher level protocols to provide security, this approach, if solely relied upon, makes it difficult to customize the security policies to specific applications. It also takes away the management of security from the application developer.

Four Layer Representation of the TCP/IP Protocol Stack (See Lecture 16)

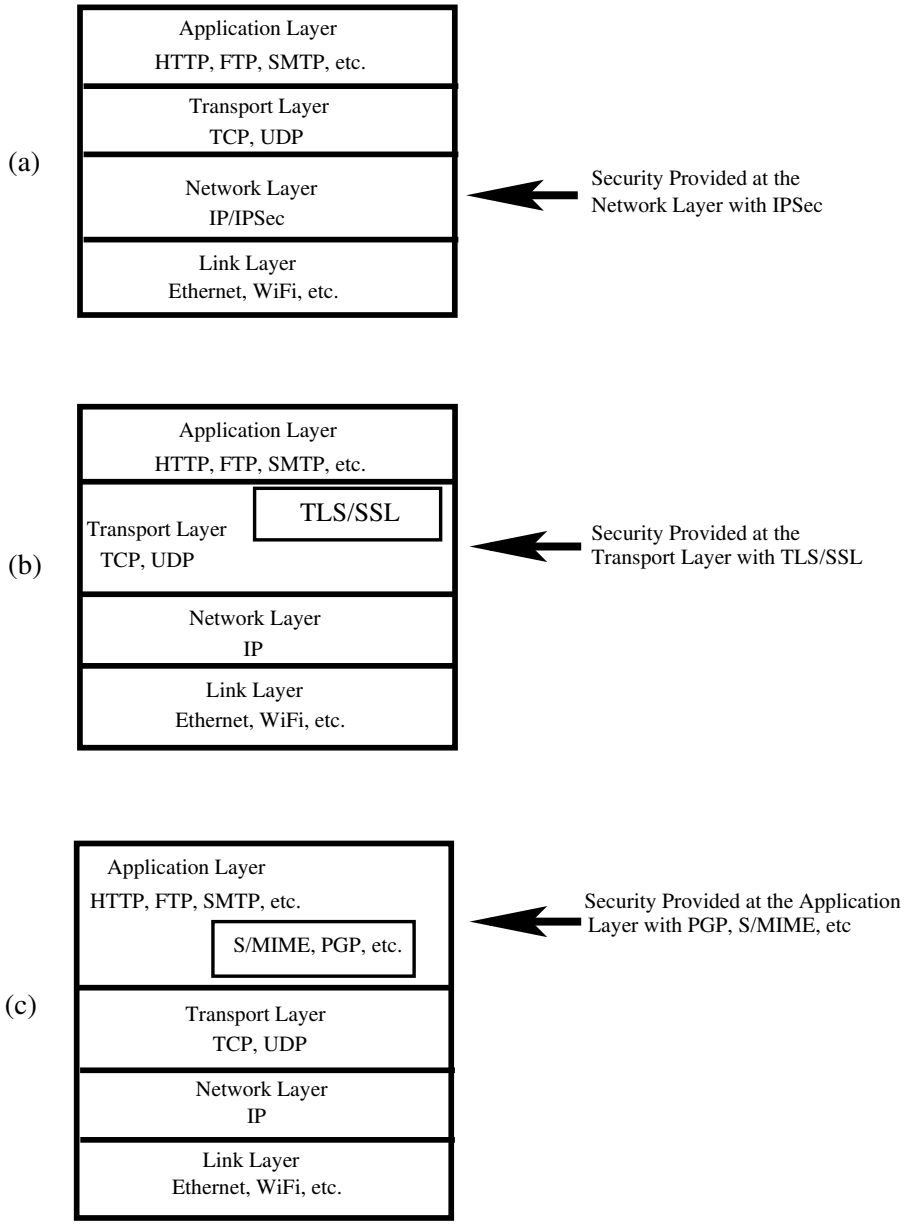

Figure 1: *Confidentiality and authentication for information security can be provided in three different layers in the TCP/IP protocol stack, as shown in this figure.* (*This figure is from Lecture 20 of "Computer and Network Security" by Avi Kak*)

– We can provide security in a higher layer, but still in a manner that is agnostic with regard to specific applications, by adding security-related features to TCP packets. This can be done with a Session Layer protocol like the Secure Sockets Layer (SSL/TLS). This is shown in part (b) of Figure 1. [*As stated in Section 16.2 of Lecture 16, in a 4-layer presentation of the TCP/IP protocol stack, the SSL/TLS protocol is usually placed in the Application Layer. However, again as stated in Lecture 16, more accurately speaking, the SSL/TLS protocol belongs to the Session Layer in the 7-layer OSI model of the TCP/IP stack.*] [Note that the firewall security provided by `iptables`, as presented in Lecture 18, also operates at the transport layer of the protocol stack. However, that is primarily defensive security. That is, `iptables` based firewall security is not meant for making information secure through authentication and confidentiality services.]

– We can embed security in the application itself, as shown in part (c) of Figure 1. The applications PGP, S/MIME, etc., in that figure are all security aware. [The proxy servers, as presented in Lecture 19, can also provide security at the application level. However, as with `iptables`, that is again primarily defensive security in the form of access control. It is generally not the job of the proxy servers to provide authentication and confidentiality services.]

- In each of the three different layers mentioned above, authentication can be provided by public-key cryptography (see Lecture 12) and by secure transmission of message digests or message authentication codes (see Lecture 15). [As mentioned previously in Lecture 15, authentication means **two** things: When information is received from a source, authentication means that the source is indeed as alleged in the information. Authentication also means that the information