Network Security v1

Note Title

[Note on source: these lecture notes are largely derived from Kurose & Ross, "Computer Networking", Chapter 8.]

Information transmission between electronic devices is often modelled as occurring at different layers. For us, the important layers are:

Layer	examples of communication at this layer	examples of security at this layer
Application layer	email dropbox web browser	PGP
Transport layer	TCP } use port numbers UDP } to deliver to correct program	SSL / TLS
Network layer	IP }- use IP address to deliver to correct computer	IPSec
Link layer	ethernet WiFi	WPA

Recall that secure communication has at least 3 separate goals:

- confidentiality: keep the message secret, typically by encrypting it
- authentication: verify who sent the message, typically by verifying a digital signature
- integrity: ensure the message is not altered, typically by including an encrypted hash of the message

As we know, the internet was not originally designed with security in mind. Therefore, even today, much of the traffic on the internet does not have the above security features. In particular, most email and web browser traffic is not secure.

[Demo: - Yahoo mail goes in plain text from a web client.
- Dickinson web content at users.dickinson.edu permits insecure ftp

(Show both via Wireshark).]

In this lecture we examine four examples of how security has been incorporated into the internet – one example from each of the above layers.

(1) Example of Application Layer security: Email with PGP

PGP ("Pretty Good Privacy") is a system for using RSA public key cryptography to encrypt, decrypt, and sign things such as files and email messages.

PGP can be set up to work automatically with your email program, or you can manually encrypt and decrypt your messages.

Because it uses public key crypto, you need to know Alice's public key before you can send an encrypted message to Alice. She needs to know *your* public key before she can send an encrypted message to you. You can distribute your key by:

a) emailing it to someone
b) make it available on your website
c) register it with a Certificate Authority (CA)

Demo: – find some PGP keys on the web
(search for "my PGP public key")
– send an encrypted message to Adele <adele-
and receive, decrypt too.

Interesting note: Few people bother to encrypt email. Why?

(2) Transport layer encryption with SSL/TLS

Recall that Transmission Control Protocol (TCP) is a major way of delivering streams of data between two computers, with given numeric ports on the source and destination computers.

Security is added to a TCP connection by using

SSL (secure sockets layer)
or TLS (transport layer security) ⟵ a variant of SSL

SSL/TLS is very widely used
e.g. - secure web browser connection with address https://...
- many email clients
- remote login and remote desktop programs

SSL is popular because it's very easy to adapt any program to use it — just use an SSL connection rather than plain TCP, and everything else is done for you.

Compared to TCP, SSL requires at least 2 extra messages to set up, and quite a bit of additional computation for encryption.

[Demo: Wireshark when establishing https session,
e.g. with google.com
useful Wireshark filter: tcp.dstport==443 or tcp.srcport==443]

Note: SSL uses public key to establish shared secret, followed by symmetric key crypto

③ Network layer security with IPSec

IPSec provides security (i.e. confidentiality, authentication, integrity) to IP (Internet Protocol).
That is, it can be used to protect all traffic between two computers.
Therefore, a company can protect essentially all traffic on its network by enabling IPSec on all its computers.

This could be considered wasteful, since a lot of additional encryption and decryption is performed. But it is a good example of

Defense in Depth

— an important security principle stating that it is wise to have multiple independent layers of security.

Note: IPSec also uses public key to establish shared secret, followed by symmetric key crypto.

(4) Example of Link layer security: Wifi Security: WEP + WPA

We don't study details, but this example is a great demonstration of how even expertly-designed protocols can possess security flaws.

- WEP (wired equivalent privacy), standardized in 1999:
  - very widely used
  - later discovered to be easily cracked
    See wikipedia: "freely available software ... [can] crack any WEP key in minutes"

- WPA (wifi protected access), ratified 2004
  - replaced WEP
  - current version, WPA2, is widely used, although there are some known problems (see wikipedia)