CE0973a - Issues in Network Security
2: SSL and Names

James A Sutherland

Abertay University

Monday, 18th January 2016

OSI Layers

Open Systems Interconnection model, 1984: ISO 7498/X.200

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

SSL/TCP/IP

SSL on TCP on IP on Ethernet/other
IP just gets packets (usually 1500 bytes) from A to B
TCP adds connections on top of that
SSL then encrypts and authenticates

TCP

Transmission Control Protocol, 1974 IEEE paper, Vint Cerf & Robert Kahn[1]

20 byte header, plus data

SYN	"I'd like a connection to port 443 please"
SYN+ACK	"OK, here is connection data"
ACK	"Great, we have a connection!"

Ends similarly: FIN,ACK in each direction

[1] http://web.archive.org/web/20150723184900/http://ece.ut.ac.ir/Classpages/F84/PrincipleofNetworkDesign/Papers/CK74.pdf

SSL so far

- Starts with DNS
- TCP connection to 443
- SSL request ("hello")
- HTTP request

Note that names actually appear in (up to) 3 different places!

Names in SSL

The Many Names of SSL

One name	example.com
Wildcards	*.example.com
SAN	example.com, *.example.com, *.test.example.com
SNI	"Who do you want me to be?"

EV adds a validated company name, only allows a simple hostname.

Sniffing

- Easy to intercept - wireless, taps, BGP, DNS...
- Ethereal/Wireshark to listen on local network segment
- Threats to Privacy
- DNS, SNI, traffic analysis

Recap, Practical Tasks

Lab tasks for week 2:

1. Get the example packet capture from Blackboard
2. Install Wireshark (`http://www.wireshark.org/`)
3. What was the user up to, and how do we know?
4. How could she hide it better?