FIT2093 Tutorial 9

Topics

- TLS, HTTP, HTTPS
- Certificates for HTTPS
- Issues with HTTPS websites

Review

1. What is the place of TLS in the TCP/IP network stack?

   TLS sits between the application layer and the transport layer.

2. What are the tasks of the TLS handshake and the TLS record protocol?

   TLS Handshake establishes the security association and the shared secret key to be used for encrypting the actual traffic. TLS record is the actual transport part, where the new shared key is used to encrypt packages.

3. Explain why a VPN does not provide end-to-end encryption.

   Encryption is only between VPN client (usually software) and VPN gateway. Traffic will be in clear in the internal network behind the gateway and also on the client side, an attacker can get access to the information before it is encrypted.

4. Why is it necessary that firewall filtering rules consider the destination port?

   The destination port identifies the actual service/process the packet is addressing. Firewall rules should express which services are allowed and what is forbidden. Without looking at the port number, the firewall could only block or allow traffic to particular devices based on their IP addresses, but not for particular services.

5. What is contradiction between filtering traffic by a firewall and encryption?

   Firewalls cannot look into encrypted packets and cannot identify the service tunneled through an encrypted channel. Therefore, malicious traffic can remain undetected. Thus, both security mechanisms cannot be properly applied at the same time. Re-encryption proxies enable filtering, but break end-to-end security assertions.

Task 1: TLS, HTTP, HTTPS

For this task you need to use *Wireshark* in order to look at three different examples of recorded network traffic. All three examples show parts of the communication between a client and a webserver.

Before you start, get files Example1.pcap, Example2.pcap and Example3.pcap from Moodle.

1.a Start Wireshark and open Example1.pcap.

- Can you identify the domain name of the server?
- Which protocols are used on application layer?
- Can you get information on the location of destination and source?

- Now open Chrome and type in the address that you have identified, using the protocol shown. Can you find any information on the security of the connection?

- The wireshark file just shows an extract with HTTP messages. Students should look at the different layers and see what kind of information they can get.
- The address is `http://www.bendigobank.com.au`. This page just uses HTTP. No authenticity, no encryption. Location for Bendigo bank and Monash University can be found. In Google Chrome, there should be the information that the connection is not secure.

1.b Open Example2.pcap in Wireshark.

- Can you identify the domain name of the server? It might be somewhere within the packet.
- Which protocoals are used on application layer?
- Identify which version of the security protocol is used. Is this considered to be a secure version?
- Now open Chrome and type in the address that you have identified, using the protocol shown. Can you find any information on the security of the connection?

- The server is the same, but this time with HTTPS:`https:///www.bendigobank.com.au/`.
- It uses TLSv1.0. If you look into the packets, you only find encrypted content. However, students should try to get some information on TLS 1.0 on the Internet and they will find that it is outdated and should no longer be used.
- If you click on the lock in Chrome (left from the address bar) you find information on the security of the site. It shows that the connection is secure, based on the certificate. Google Chrome currently does not check the version of the protocol used.

1.c Open Example3.pcap in Wireshark.

- Can you identify the domain name of the server?
- What is different to the other two examples?
- Which protocols are used? Are these considered t0 be secure?
- Now open Chrome and type in the address that you have identified, using the protocol shown. Can you find any information on the security of the connection?

This time it is another server, but also using HTTP: `http://combank.com.au`. However, you will first see an error and then see that the get request was diverted to HTTPS. Thus, the traffic automatically switches from HTTP to TLSv1.2. It uses TLS version 1.2, which is state of the art and considered to be secure.

Task 2: Certificates for HTTPS/TLS

2.a Use Chrome to open a webpage that supports TLS. For example https://combank.com.au/ Click on the lock shown on the left from the address bar.

- Who is the issuer of the certificate and how long is it valid?
- What is used for key exchange and which cipher suite is used during transport?

Symantec has issued the certificate. Expires on 27.02.2017.
TLS 1.2
Key Exchange: ECDHE_RSA
This is Elliptic Curve Diffie-HEllman, signed with RSA.
Cipher Suite: AES_256_GCM
This is 256 bit AES used in Galois/Counter Mode.

2.b Can you find the list of all certification authorities that are installed in Chrome? Can you find some revoked certificates? (Hint: Look in settings under advanced settings)

Just look in the menu -> settings -> advanced settings and scroll down to HTTPS/SSL and Manage certificates. Under *servers*, you find a few revoked certificates. If someone is interested in the story behind this, google for `UTN-USERFirst-Hardware`.

2.c This article shows a few of the main issues with certificates: https://arstechnica.com/security/2017/03/google-takes-symantec-to-the-woodshed-for-mis-issuing-30000-https-certs/

(a) Read the article.

(b) What are the different entities (companies, software, etc.) that need to be trusted to actually trust a certificate?

(c) Draw a diagram showing the process of certificate issueing and checking in the browser. It should contain entities (companies, devices, software) used for producing the different certificates and checking it. Assume that the server's certificate is directly signed with the issuer's root certificate.

Entities are the issuer of the certificate (the owner of the root certificate), software/hardware needed to produce the root certificate and the server's certificate, the company deciding which root certificates to bundle with the browser, the browser for checking, the server storing the secret key, the owner of the server, the client's PC.

Task 3: HTTPS with correct certificate and no lock

Now, using Google Chrome, try two other sites that should be secure:

3.a First, the website of the Australian Government: https://www.australia.gov.au/
What happens? Does it work? Lets try http://www.australia.gov.au/

3.b Second, the website of the German Parliament (Bundestag): https://www.bundestag.de/en/
Does this work? can you see the lock showing a secure connection?
Id not, try to find out what happens. Is the certificate not valid? Is the certification authority untrusted? What else?

1. Just look at the page and wonder why the Australian Government is not able to just get a certificate . . .

2. There is no lock. The problem is, that there are insecure elements loaded as part of the website. CLick on `View site information` (the small icon where the lock should be). Then, you find that the certificate and encryption is okay, but there is mixed content. Click on `View requests in network panel` and then reload the page.