Exercises - Week 11
Network security II

1. Are the following statements True or False:

a) **If two web clients both retrieve the same URL from a given HTTPS (HTTP-over-TLS) server, then the bytes they transmit over the network to the server will be identical.**
b) **Can TLS prevent TCP RST injection attacks?**
c) **In a network using DMZ, all traffic going to the LAN (intranet) has to be authenticated.**
d) **At least 3 RTT (round trip time) are needed before starting to transmit data when using HTTP-over-TLS.**
e) **When using TLS, if the adversary managed to get the *session* key, then all packets from previous sessions can be decrypted.**

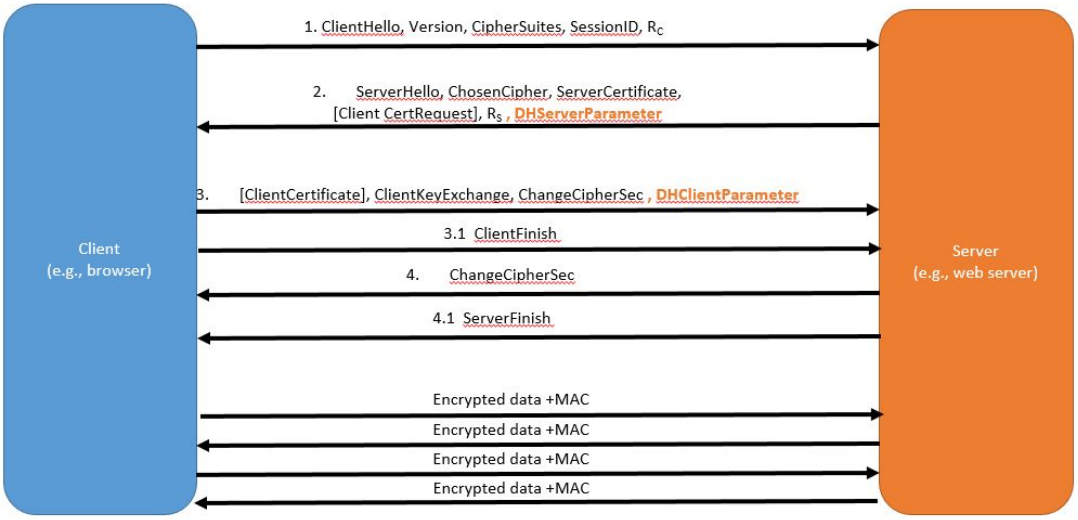
a) False - TLS encrypts the connection and different clients would have different shared keys which results in non-identical transmissions. Also the handshake would look different (e.g., keys, challenges R_X, etc)
b) False - TLS encrypts content but not headers. The RST bit is in the header, so you can still perform the attack. The OS would see the TCP packet with the RST and instead of checking higher levels(TLS) it would terminate the connection.
c) True - In a network using DMZ, a host bastion filters all traffic going to the LAN to protect the hosts against compromisation, the traffic has to be authenticated to belong to the “universe of good things”
d) True - The client needs to create a connection for each OSI layer before going to the higher level. Hence, it needs to create a TCP connection, then a TLS connection, and finally it can start the HTTP. 1 RTT is needed for the TCP handshake and 2 RTT are needed to establish the TLS session.
e) False - the session key used to encrypt traffic is different every time. Recovering one key does not give information about past sessions.

2. In the lecture we have discussed how to configure TLS so that the client creates a key and uses “key transport” mode (encrypting with the public key of the server) to make the symmetric key arrive to the server.

a) **What is the security concern with this approach?**

In the “key transport”, the client encrypts a random key with the server’s public key and sends it to the server. If an adversary steals/brute forces the private key of the server, then he can decrypt any of the past or future communication which were based on the stolen key. In other words,It does not provide forward security

b) In the cryptography lecture we saw that a way to avoid this problem is to use Diffie Hellman to agree on a session key that is thrown away at the end of the session. Look at the messages exchange in the TLS handshake. In which of the steps should the exchange of DH exponents be done? Justify.



After step 3 Client and server can compute their shared key using DH!!!

In the 1 step, the client sends a list of preferred key exchange materials. After receiving this list, the server knows the capability and preference of both parties, so it can determine the final key exchange method. In the 2 step, the server sends both the result of the algorithm negotiation (DH for key exchange) and its DH public key. In step 3, the client sends its DH public key to the server. At the end of the 3 step both parties can compute the DH shared key. After computing this shared key they can start the encrypted communication in the same way as if key transport was used.

3. After finishing his PhD, John became an IT manager in EPFL. EPFL's Fire lab, has developed a new stateless firewall. As his first task, John needs to set-up this firewall for EPFL network. Help John to accomplish the following tasks by describing the filtering rules that he should establish on the firewall. If a task is impossible to achieve, help John to convince the Fire lab head why the new firewall won't work for that purpose.

Cheatsheet:
SMTP (email): IP, TCP:25
HTTP : IP, TCP:80
HTTPS : IP, TCP:443
DNS: IP, UDP

A sample rule for the task "Only people located at the EPFL should be able to check their mail" is:
Allow: { IP. src: {inside EPFL} , IP. dest : {mail.epfl.ch}, TCP.dest.port : 25 }
Deny: { IP. dest : {mail.epfl.ch}, TCP.dest.port : 25 }

a) **EPFL's site (epfl.ch) should not allow connection from scammers.com**
b) **People inside EPFL should not have access to Facebook.**

After censoring Facebook, students created a FreeFacebook organization which provided the following options to students. Help John to keep the Facebook blocked.

c) **Connecting via a plain (non-encrypted) proxy**
d) **Connecting via a proxy service based on IPSec Tunnel**

a) Deny: { IP. dest: epfl.ch, TCP.dest: {80,443}, IP.src: scammers.com}
The firewall should prevent web requests, HTTP (port 80) and HTTPS (port 443), to the epfl.ch site from senders in scammers.com.
b) Deny: { IP. src: {inside EPFL} IP. dest: facebook.com, TCP.port: {80,443} }
The firewall should prevent web access to the facebook site from users inside the epfl network.
c) Deny:{IP. src: {inside EPFL}, TCP->Proxy.dest: {facebook.com}}
Since users are using a proxy, the server will not see the facebook address in the IP destination. In here we are assuming that John doesn't know the address of the proxy otherwise he could simply block the proxy address. Without knowing the proxy address beforehand, John cannot simply block all connection which may look like a proxy because this may block the whole web. However, the plain proxy is not encrypted, so the firewall can read the payload of the communication, and students need to tell the proxy to redirect to the facebook. John sets a rule to check for a proxy in the TCP connection and if it tries to connect to the facebook block it.
d) Deny:{IP. src: {inside EPFL}, DNS->address.url: {facebook.com}}
In the IPSec tunnel, all the payload is encrypted and the firewall can no longer check for "re-route to facebook". However, students are not using a secure channel for their DNS. Hence, John can check DNS packets and drop the address requests for facebook. Without knowing the IP address for facebook students cannot visit the site.

4. After deploying the EPFL Firewall, Moodle managers decide to trust users inside EPFL, and they deployed an internal Moodle HTTP server which is only accessible from inside the EPFL. Trudy is a student in Com 301, and because of her expertise, she gets a student job in the EPFL IT section. Because of her student work, she couldn't study for one of the midterms, and she decided to put a fake post on Moodle to announce that the midterm is canceled. Moodle still has the user/password

protection and she needs to post this as a TA, so everyone would believe her. Trudy is sure that TAs won't miss questions before the midterm, so she waits for them to respond to a question to hijack a TA connection.
Note: Moodle user/password authentication doesn't send the password in the clear and doesn't allow replay attacks.

a) **How can Trudy hijack the flow?**
b) **After her successful attack, Trudy got caught by IT staff and loses her student job and losses her EPFL network access. Is Trudy able to hijacking another Moodle connection and exacts her revenge from evil TAs even if she has no access to the exchanged packets? If yes, how? If no, why?**

Trudy decides to use TCP hijacking to achieve her goal.

a) As she works for EPFL, she can observe every packet which goes through the EPFL network, so she can see the exchanged packets to get the sequence numbers, she will be able to hijack the flow by sending TCP packets with the correct sequence numbers that will be accepted by the Moodle server. If she has access to a router, she can directly modify the packet sent by a TA.
b) Yes, Trudy could take a revenge from the TAs. Trudy no longer has access to EPFL network to observe packets in the network and see the sequence numbers, but she still can send packets from the internet to the EPFL network, and she can spoof her IP address to fake the IP address of the TA. As TCP uses weak random number generators, it would be possible for Trudy to guess the correct sequence numbers in order to hijack the flow.

We wrote this question thinking about TCP hijacking, but during the exercise session many of you came up with other attack vectors (Well done!). Options provided by different students:

- Use DNS spoofing to conduct a Man-In-The-Middle (valid both for a) and b))
- Use BGP Hijacking to conduct a Man-In-the-middle (valid both for a) and b))
- Use ARP Hijacking to conduct a Man-In-the-middle (only valid for a))

If you have another attack not in this list let us know and we will let you know.

5. Consider an ecommerce website that includes the notion of a "shopping cart." Customers visiting the site put items of interest in their shopping cart. After finishing their browsing and shopping, they click on Checkout to pay for the items. At that point, the customer logs into the site to enable the site to retrieve their payment information.

(a) Suppose that the site implements the shopping cart by storing the associated items and prices in files on the server, with one file for each customer. The site identifies customers by their IP addresses.

This design is vulnerable to a DoS attack. Sketch it in a single sentence (remember to hone your skills: 1 sentence is not 2 sentences).

Two possible attacks:

1. The adversary can add millions of items from one IP to a shopping cart to exhaust the memory of the server.

2. The adversary can spoof/compromise many IPs and for each buy an item creating too many shopping carts to exhaust the memory of the server.

(Note that the second attack may have a much larger cost than the first, since the adversary may need to compromise the IPs or buy them -- e.g., from a botnet).

(b) Suppose that instead the site keeps a list of shopping cart items on the client side. Every time a user clicks on add-to-cart, the server sends all of the associated details (item name, price, quantity) in its reply, incorporating them into a hidden HTML form field. Through some Javascript magic, now when the user finally clicks on Checkout, all of the previously bought items embedded in the hidden form field are sent to the server. The server then joins them together into a list and presents the user with the corresponding total amount for payment.

b1. Is this design vulnerable to the DoS attack you sketched above? Explain why or why not.

The server no longer keeps any information (or even get notified) about user's cart, so trying to add items won't consume resources at the server side.

b2. Is this design secure from other attacks? If so, explain the basis for your claim. If not, describe an attack on it. (You can assume that the site is safe from web attacks such as CSRF, XSS and SQL injection, and uses HTTPS for the Checkout procedure.)

It is not secure. There isg no integrity! How do you know the shopping cart is correct?

EXERCISES FROM LAST WEEK

Week 10 - Ex. 2. One of the uses of VPNs is to hide the destination of a communication. This is because, when a user connects to the internet through a VPN, this user service provider (or anybody observing his communication in the path to the VPN) can only see the VPN IP and not the final destination thanks to the IPSec Tunnel encryption.

a) **To maintain this property with respect to the ISP:**
    a) **DNS have to be routed through the VPN**
    b) **DNS have to be routed outside the VPN**
    c) **Who cares about DNS, we are not hiding the IP of the DNS resolver**

Justify

Option a). DNS queries are not encrypted, if the DNS go outside the VPN, then the ISP can see in the request which domains are being visited.

b) Would the fact that no-one can see the final IP hold if the VPN was built using IPSec in transport mode?

Nope, that leaves the IP in the clear!

c) John is a member of a MyPrivateDiary.com site which provides private diary over the cloud. After learning about VPNs in Com-301, John bought an application called VPNX which uses IPSec Tunnel mode to create a tunnel and redirect every connection through the tunnel. John wrote a story about his new VPN application on his diary. Which one of the following entities can read John's diary? (Justify)

a. **VPNX company**
b. **John's ISP (internet service provider)**
c. **John's curious friend**
d. **MyPrivateDiary.com**
e. **MyPrivateDiary's ISP**

Connection to the VPN server is encrypted, so John's friend and his ISP cannot read his packet or know that he is visiting the MyPrivateDiary.com.
IPSec tunnel is between John and VPNX server, and they both share the same symmetric key. Hence, the VPNX knows that John is connecting to the diary site. Furthermore, VPNX can read the content of John packets, so they can read John's diary.
IPSec only provides confidentiality, integrity, and authentication inside the tunnel. MyPrivateDiary.com and its ISP are located after the end of the tunnel. They cannot detect the original IP address of John (it is replaced with the VPNX address), but they can read the diary.

Week 10 - Ex. 6. John is a PhD student who wastes his time on Facebook. John's sympathetic professor decides to monitor John's internet connection and guide Facebook visit to Google Scholar. Which of the following approaches allows John's professor, who has full control over the local network, to help John? (Justify)

a. **Filtering outgoing IP connections**
b. **Dropping DNS responses to filtered sites**
c. **ARP poisoning**
d. **DNS hijacking**
e. **BGP hijacking**

a. This only prevents connections to the Facebook without guiding to the Scholar.
b. John needs to know Facebook's IP address to visit the site. This only prevents connections to the Facebook without guiding to the Scholar.
c. ARP poisoning is only for local networks. It doesn't work here.
d. DNS hijacking is the best approach to guide John.
e. BGP hijacking is only possible for ASs and internet middle nodes.

The best way to ensure that John doesn't stray from the research path is enforcing all a, b, and d option together.

Unfortunately, John is very stubborn and he still wants to visit Facebook. Which of the following approaches can help John to visit Facebook without getting caught? (Justify)

a. IPSec in transport mode
b. IPSec in traffic mode
c. IPSec in tunnel mode
d. DNSSEC
e. DNS over HTTPS

a. Transport mode reveals the real destination IP address to the network. It can be blocked with IP filtering.
b. There is no traffic mode in IPSec!
c. IPSec tunnel mode lets John bypass the IP filtering but the DNS poisoning and dropping prevents him from getting the IP of Facebook, so he cannot visit Facebook.
d. DNSSEC ensures the authenticity of the DNS response. This only prevents redirection to the Scholar, but it won't enable him to check his Facebook.
e. DoH provides both integrity and confidentiality to the DNS and it prevents both DNS poisoning and dropping. Although, using DoH alone is not enough to bypass the IP filtering.

John needs to use both IPSec in tunneling mode and DoH to circumvent his professor's guidance and waste his time.