# COM-301 Computer Security
# Exercise 8: Network Security

November 29, 2023

## Network Security

1. EPFL decides to retire the use of Gaspar accounts for authenticating to WiFi. They decide to register students MAC to give access to the WiFi and only 1Gb per month so that they study and not go on Facebook. What are the security implications of this decision?

   **Solution**:
   Since MAC addresses have no protections against impersonation you can:

   Impersonate: which leads to students stealing each other's allocated bytes.

   Abuse resources: one student can create fake MACs to get access to more resources than those assigned to him/her.

2. Are the following statements True or False:

   (a) The reason why TCP can be hijacked is the poor authentication mechanism

   (b) DNSSEC provides confidentiality of DNS queries

   (c) Routing security relates to the capability of an adversary to influence the routes that messages will follow.

   (d) You can use IPSEC in tunnel mode to build a VPN

   (e) 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.

   (f) At least 3 RTT (round trip time) are needed before starting to transmit data when using HTTP-over-TLS.

   (g) When using TLS, if the adversary manages to get the session key, then all packets from previous sessions can be decrypted.

   **Solution**:

(a) True - Authentication in TCP depends on a weak secret, the sequence numbers. These can become known to the adversary if the connection is in the clear and the adersary can eavesdrop on it; or if the TCP implementation uses a weak random number generator, and the adversary could guess the sequence numbers and hijack the session. An authentication mechanism using a weak random number generator is considered as poor.

(b) False - The answers are signed by the authoritative DNS resolvers, which provides authentication and integrity. However, they are not encrypted, so DNSSEC doesn't provide confidentiality.

(c) True - An adversary should not be able to influence the route and the delivery of messages over a network.

(d) True - A lot of VPN are built over IPSEC in tunnel mode because it guarantees confidentiality, integrity, authenticity, and protection against replay attacks. IPSEC protects the IP packet by encrypting the payload using symmetric cryptography, and it ensures authentication and integrity of the IP header.

(e) False - TLS encrypts the connection and different clients would have different shared keys with the server, which results in non-identical transmissions. Also the handshake would look different (e.g., keys, challenges RX, etc).

(f) True - The client needs to create a connection for each OSI layer before going to the higher level. It needs to create a TCP connection, then a TLS connection, and finally it can start the HTTP communication. One RTT is needed for the TCP handshake and two RTT are needed to establish the TLS session.

(g) False - the session key used to encrypt traffic is different every time. Recovering one key does not give information about past sessions.

3. 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) Which of the following is needed to maintain this property with respect to the Internet Service Provider (Justify):

      i. DNS have to be routed through the VPN

      ii. DNS have to be routed outside the VPN

      iii. Who cares about DNS, we are not hiding the IP of the DNS resolver

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

(c) John is a member of a MyPrivateDiary.com, a service that enables John to have private diary in 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)

i. VPNX company
ii. John's ISP (internet service provider)
iii. John's curious friend
iv. MyPrivateDiary.com
v. MyPrivateDiary's ISP

**Solution**:

(a) Option (i). 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) Nope, that leaves the IP in the clear!

(c) The 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.
The 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.

4. If we suspect that a DNS resolver has been poisoned. Is it a good idea to consult other DNS resolvers for the answer? Why?

**Solution**:
Yes. Following the separation of privilege principle, if we ask more than once we force the adversary to compromise more than one resolver effectively increasing the cost of the attack.

5. Jane is a PhD student who wastes her time on Facebook. Jane's sympathetic professor decides to monitor Jane's internet connection and redirect Facebook visits to Google Scholar. Which of the following approaches enables Jane's professor, who has full control over the local network, to help Jane? (Justify)

(a) Filtering outgoing IP connections

(b) Dropping DNS responses to filtered sites

(c) ARP poisoning

(d) DNS hijacking

(e) BGP hijacking

**Solution**:

(a) IP filtering only prevents connections to Facebook without guiding Jane to Google Scholar.

(b) Jane needs to know Facebook's IP address to visit the site. Dropping DNS responses only prevents connections to Facebook without redirecting to Google Scholar.

(c) ARP poisoning is only for local networks. It doesn't work here as both Facebook and Google Scholar are out of the network. At most the professor can do a denial of service.

(d) DNS hijacking would work, and it is the best approach to guide Jane to Google scholar in this scenario.

(e) BGP hijacking is only possible for ASs and internet middle nodes, the professor cannot deploy it (unless it corrupts a node).

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

6. Unfortunately, Jane is very stubborn and she still wants to spend time on Facebook. Which of the following approaches can help Jane 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

**Solution**:

(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 Jane bypass the IP filtering but the DNS hijacking 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 her to check her Facebook.

(e) DoH provides both integrity and confidentiality to the DNS and it prevents both DNS hijacking and dropping. Although, using DoH alone is not enough to bypass the IP filtering.

Jane needs to use both IPSec in tunnel mode and DoH to completely circumvent the professor's attacks and happily waste her time on Facebook.

7. You want to do man in the middle between a PhD at EPFL and the Amazon Cloud Services. Can you do it if (justify your answer)

   (a) You are in the EPFL local network?

   (b) You are on vacation in Australia?

   (c) You are an Internet Service provider?

   **Solution**:

   (a) Yes, you can use ARP poisoning to make the gateway believe that you are the PhD machine, and the PhD machine that you are the gateway.

   (b) Yes, you can use DNS poisoning on the resolver used by the PhD student to try to reroute the traffic between the student and Amazon through your server.

   (c) Yes, besides DNS poisoning, in this case you can also change the routing tables inside your / other ASs to re-route packets through your server (BGP hijacking).

8. Can Intrusion Detection Systems help to prevent: (Justify)

   (a) BGP hijacking?

   (b) DNS Poisoning?

   **Solution**:
   No and no. Intrusion Detection Systems (IDS) analyze the patterns (signatures or anomalies) in your network. These attacks affect routing tables / IP-domain assignments. No analysis on your network will help avoiding them.

If you think about IDS in the neworks of the routers / resolvers. This also does not help much. There is no signature or pattern. The real problem is the content, which is hard to decide whether it is right or wrong (Though, as said in the class, some filtering can actually be done for corner cases. But it will not eliminate, or mitigate much the problem).

9. You are the network administrator for a large company.

   (a) Your company will be held liable for any spoofing attacks that originate from within your network and are sent out to the global Internet. What can you do to prevent spoofing attacks by your own employees?

   (b) What can be done to prevent parties outside your network from sending your employees spoofed traffic that impersonates your own employees?

   **Solution**:

   (a) Do not let packets with origin IP out of your network leave to the outside world.

   (b) Do not let packets that come from the outside world with an origin IP inside your network enter.

10. After finishing her PhD, Jane became an IT manager in EPFL. EPFL's FIRE lab has developed a new stateless firewall. As her first task, Jane needs to set-up this firewall for EPFL network. Help Jane accomplish the following tasks by describing the filtering rules that she should establish on the firewall. If a task is impossible to achieve, help Jane 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 Jane to keep the Facebook blocked.

(c) Connecting via a plain (non-encrypted) proxy

(d) Connecting via a proxy service based on IPSec Tunnel

**Solution**:

(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$\longrightarrow$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$\longrightarrow$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 request

11. 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).

(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.

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

**Solution**:

(a) 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)
- 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.
- It is not secure. There is no integrity! How do you know the shopping cart is correct?