COM-301 Computer Security
Exercise 8: Network Security

November 27, 2025

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?

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.

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

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?

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

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

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?
8. Can Intrusion Detection Systems help to prevent: (Justify)
   (a) BGP hijacking?
   (b) DNS Poisoning?
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?
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

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.)