Computer Security Fall 2023
Network Security Homework

Srdjan Matic, Juan Caballero
IMDEA Software Institute

Guidelines

This homework is due by **Monday, 27th, 2023 23:59:59 GMT+1**.

Please send your solutions in PDF format to `srdjan.matic@imdea.org`.

No collaboration is permitted on this assignment. Any cheating (e.g., submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade.

Problem 1: Initial Sequence Number Guessing *(14 points)*

Which of the following ISN selection methods used by a server are secure? If you believe that a method is not secure, explain the reason.

a. The server generates its ISNs by using the 32 least significant bits of MD5, calculated over a random value chosen for each connection. *(2 points)*

b. The server generates its ISNs by using the 32 least significant bits of MD5, calculated over bitwise AND among a constant value selected at random at boot time and the server IP. *(2 points)*

c. The server generates its ISNs by using the 32 least significant bits of a known secure hashing (i.e., SHA256) over a bitwise AND among a constant value selected at random at boot time and the server IP.

d. The server generates its ISNs by using the 32 least significant bits of a known secure hashing (i.e., SHA256) calculated over the value obtained using the generator for ISNs of MacOS 9. *(2 points)*

e. The server generates its ISNs by using the 32 least significant bits of a known secure hashing (i.e., SHA256) calculated over the content of the "data" portion of a TCP segment received from the client. *(2 points)*

f. The server generates its ISNs by performing a XOR among the following five variables: source IP, source port, destination IP, destination port, current time. *(2 points)*

g. The server generates its ISNs by performing a XOR among client ISN and a random value selected at boot. *(2 points)*

Problem 2: Scanning *(12 points)*

A security researcher has identified the IP address of a command-and-control (C&C) server and wants to gather information about the botnet controlled through this server. By reverse-engineering a malware sample that connects to the C&C server, the researcher finds out that the communication happens through the following ports: 110, 143, 587.

1. Which protocols typically runs on these ports? *(3 points)*

2. For each probe sent on one of these ports, the researcher observes a different behavior:

   (a) from port 110 the server replied with a "ACK" packet;

   (b) from port 143 there was no response from the server;

   (c) from port 587 the server replied with an "ICMP port unreachable"

   Could you infer which protocol (i.e., TCP or UDP) did the researcher use in each probe? *(6 points)*

3. Could the server be behind a firewall? Motivate your answer. *(3 points)*

Problem 3: Denial-of-Service *(20 points)*

One way to achieve Denial of service is to flood the target machine(s) or resource(s) with requests in an attempt to overload the system and prevent legitimate requests from being fulfilled. This kind of attack can be carried out at any layer of the network stack.

1. Describe <u>two</u> DoS attacks that can be carried out at the application layer. *(8 points)*

2. Describe one possible defense against DoS attacks at application layer. *(4 points)*

3. Describe one DoS attack that relies on ICMP "ping" packets. *(4 points)*

4. Describe one solution for attributing the source of (spoofed) packets. *(4 points)*

Problem 4: Denial-of-Service Amplification *(14 points)*

1. Describe two reflector attacks with amplification, that (*i*) do not rely on DNS and where (*ii*) the attacker needs to *crawl* the Internet to discover amplifiers. Include information on:

   (a) the number of amplifiers identified in the paper

   (b) all the involved parties

   (c) the type of requests and responses sent by each party

   (d) the average packet amplification and maximum bandwidth amplification factors that the attacker can achieve. *(14 points)*

   (*Hint*: There are several attacks in the NDSS'14 paper by Rossow, but I want you to provide the details of the requests involved.)

Problem 5: HTTPS *(12 points)*

A security researcher executes a mobile application in an Android phone to study its network communication. The mobile app uses HTTPS to communicate with a remote server.

1. Since the communication between the mobile app and the server uses HTTPS, how can the can the researcher obtain the list of domains to which the mobile app connects? To which network does the mobile device need to be connected to? From which protocol message can the researcher obtain the domain information? *(4 points)*

2. Explain how the researcher could intercept (i.e., decrypt) the communication between the mobile app running in the mobile phone and the remote server. *(4 points)*

3. Under what circumstances does the interception succeed? What actions by the mobile app developer could protect against such interception? *(4 points)*

Problem 6: Certificates *(28 points)*

Check the HTTPS certificate for `https://www.upm.es` and answer the following questions. For each question, you need to provide a textual answer and a screenshot where the answer is visible.

1. How many certificates are there in the certificate chain? *(3 points)*

2. Are any of the certificates in the chain self-signed? If so, which one and why? If not, why not? *(3 points)*

3. What is the name of the Certification Authority that produced the leaf certificate? *(3 points)*

4. What is the organization name of the Certification Authority that produced the root certificate in the trusted store? *(3 points)*

5. What is the validity period of the leaf certificate? *(3 points)*

6. How many domains (*i.e., fully qualified domain names*) is the leaf certificate valid for? List the domains alphabetically *(4 points)*

7. For the leaf certificate, what are the URLs of the OCSP server and the certificate revocation list (CRL)? *(3 points)*

8. Download the certificate revocation list from the above URL. How many revoked certificates are there in the file? Note that how to view the contents of the CRL file varies depending on your OS and could require you to install a tool. Please provide the command used and the first 30 lines of human-readable content of the CRL file in the answer. *(6 points)*