Communication Protocols and Internet Architectures
Harvard University
CSCI S-40, Summer 2018

Homework Assignment #5 Solutions

Question 1) 2 points total

CAN-SPAM section 5.a.5 requires all bulk email senders…. please see the homework for the complete question.

ANSWER

CAN-SPAM requires opt-outs, but by submitting an opt-out request, you are verifying that the email address that the spammer used was valid, that your ISP let the email through and delivered it to your mailbox, and that you read your email. This is the information a Spammer wants to know and an unscrupulous Spammer would take advantage of it to sell your email address and send you more Spam.

Question 2) 3 points total

All routers today implement packet filters….. (Please see homework for the complete question.)

ANSWER

In general, routers implement packet filters using what are called access control lists or ACLs. These ACLs specify and control which specific network traffic is forwarded by the router to a given network, versus being dropped by the router. At a minimum, access lists contain the following information: source and destination address information, protocol information (TCP, UDP, ICMP), application specific UDP/TCP port numbers, and associated filtering rules. When a packet reaches a router which has implemented an access list, filtering decisions are made based on these criteria. (These criteria are also known as rules.) The specific physical network interface on the router that the ACL applies to is also specified, as is whether the rule is for inbound or outbound packets.

Each packet is evaluated against the access criteria or rule, and the packet is either forwarded along to the destination network if the access list says to allow the forwarding, or it is discarded. If forwarding is allowed, the ACL rule that specifies this is typically called a "Permit." Access lists include an implicit "Deny" at the end of their access list which means that a packet which has not met the criteria in an explicit "Permit" rule will be dropped. (Note that address mask parameters can also be used in ACLs although you did not need to describe their use in your answer.)

The following is a simple generic example of an ACL that permits outbound web access for a machine with an IP address known as "Client-IP-Address."

Permit TCP Client-IP-Address Any (meaning to any external host) port 80
Permit TCP Client-IP-Address Any (meaning to any external host) port 443

Note that this ACL would be applied to the WAN link since we are filtering outbound traffic and that two rules are used: one for port 80 and one for SSL traffic on port 443.

As a more specific example, consider a Cisco series 7000 router. These routers support multiple I/O cards, each with multiple LAN and WAN interfaces. As with all of the Cisco routers, packet filtering is implemented as an integral part of the IOS software package.

The control commands used in the router include what Cisco calls Access Groups and Access Lists. For example, the following configuration (which comes from one of the Cisco configuration manuals) permits outbound TCP traffic from ethernet interface #0 on router R1 with destination port values matching WWW (port 80), Telnet (port 23), SMTP (port 25), POP3 (port 110), FTP (port 21), or

FTP data (port 20). Notice an implicit deny all clause at the end of an ACL denies all other traffic, which does not match the permit clauses.

```
hostname R1
!
interface ethernet0
ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

Question 3) 3 points total

3.) What is a X.509 certificate? What is a Certificate Authority? Given that anyone …… (Please see the homework for the complete question.)

ANSWER

X.509 is an ITU standard for describing and authenticating certificates. (This continues to be an active area of work in both the ITU and the IETF and you should visit the IETF working group website for a current status.) An X.509 certificate is used to distribute a public key in such a way that the receiver of the certificate can be reasonably certain that the key belongs to the party claiming to own the key. Certificates are typically used for secure communication with a web server; in these cases, you want to be certain that the web server that is sending out the key (within the certificate) is in reality, the web site or service that it is telling you it is.

A certificate contains the public key, information about the owner of the key, and a digital signature of all this information from the Certificate Authority (CA) signed with the CA's private key.

CAs must of course also make their public keys available, and they do this in certificates as well. These certificates are digitally signed by "higher" level CAs and this means that CAs are organized hierarchically with root CAs at the "highest" level. The public keys of root CAs' are "well known" and are typically bundled into browsers or operating systems. Given this hierarchical approach, a user should be able to verify all of the certificates in the chain; in other words, the original certificate, plus the certificates of the CAs that signed the previous certificate, until the root CA is reached.

Given that anyone can generate a private/public key pair on their own, Certificates and CAs are needed so that users can verify that the public key of the web service they want to use, actually belongs to that service. Without certificates there is no way to verify that the public key you get is the correct key.

Question 4) 3 points total

4.) Assume that you are submitting your homework as a file attached to an email…..

ANSWER

A Digital Signature is in concept an electronic version of a "handwritten signature". With a paper document, the presence of a handwritten signature provides a form of authentication for the document. A Digital Signature can be used to provide the same type of authentication for messages that are transmitted electronically. That is, a Digital Signature provides to the receiver a certain level of assurance that an electronic document came from a specific sender and was not altered after the sender "signed" it.

Digital signatures can be implemented using a combination of Hashing Algorithms and Public Key Algorithms. A Hashing Algorithm involves using a one-way mathematical function (called a Hash Function) to transform the random number of characters making up the electronic message into a fixed length bit string, called a Hash Code. A Hash Code can be thought of as a numerical representation of a given message.

Electronic messages can of course also be encrypted. This involves using a mathematical function to transform a plaintext message into an unreadable, encrypted message. The encryption key is the parameter used by the mathematical function during the transformation process. In the case of a Public Key Algorithm, keys come in pairs. That is, there is a public key and a private key. A public key is a key that is made public (i.e., anyone has access to it) and a private key, in contrast, is kept secret. A message that is encrypted using the public key can be decrypted into its original form using only the corresponding private key. The inverse is also true: a message that is encrypted using a private key can be decrypted into its original form using its corresponding public key.

Therefore, with these building blocks, a Digital Signature could be used to submit homework in the following way:

A student researches and completes the assigned homework, then uses a Hash Function to calculate a Hash Code for the homework document. The student then encrypts the Hash Code using their private key. The encrypted Hash Code and homework document are then sent electronically to Harvard. A member of the teaching staff then computes a Hash Code of the homework using the same Hash Function used by the student. Then, the Harvard staff member decrypts the encrypted Hash Code sent by the student using the student's public key. If the two Hash Codes (the one sent and the one calculated from the received homework assignment) are equal, then Harvard can be reasonably assured that the homework assignment has not been altered, and did in fact come from the student.

While this question did not ask that the homework be encrypted, it is of course possible to do that as well. If your answer stated that the homework had to be encrypted to be signed, that is not correct.

Question 5) 3 points total

5.) Describe the functionality and operation of a SIP proxy server and also…. (Please see the homework for the complete question.)

ANSWER

In general terms, a proxy acts on behalf of a client, or as an intermediary between a client and another server. For example, a web proxy server receives the request from the client, interprets it (based on some policy) and then acts on it by forwarding the request on the client's behalf, or by providing locally cached information back to the client.

In the same way, a SIP proxy server acts on behalf of a SIP based user agent (i.e., a SIP phone) by providing features such as call signaling and call routing services, user authentication and call management services. Not all of this functionality needs to be provided by a single SIP proxy and in SIP, different types of proxies and servers such as Registrar, Location and Redirect servers have also been defined.

In order to understand the operation of a proxy, it is very helpful to follow a call placed between two SIP phones. Therefore, consider a SIP call placed by Alice to Bob when both Alice and Bob have registered with their respective proxy servers. The call placed by Alice (using a SIP INVITE) is sent to Alice's proxy server since this proxy server is responsible for handling and routing this call on Alice's behalf. In this case, Alice's proxy server is acting as an outbound proxy server and it processes the call by locating the proxy server that supports Bob and then sending Bob's proxy an updated INVITE. Bob's proxy server accepts the INVITE on Bob's behalf, locates Bob at that moment in time, and sends the INVITE to Bob (who then decides whether or not to answer the call.) The proxy servers stay in the path while the call is being set up but then typically drop out of the call flow once the call is established.

The above scenario includes the step where the proxy server that supports Bob is able to locate Bob even though Bob does not have a fixed IP address, or might be using one of many different clients. (The proper SIP phone for Bob might be his laptop, his cell phone or his PDA.) Figuring out where Bob is at a specific point in time is accomplished by the use of a Registrar service and Location Service. (The registrar and location services can run on a separate physical servers or they can use the same hardware as Bob's proxy server.)

The client (in this case Bob's current SIP user agent) would register their current location and IP address with the Registrar and the Registrar would then report this information to the Location Service. When a SIP Invite for Bob (or any other specific user) was received by the Proxy server that supports that client, the Proxy server would request the location information from the Location Server and then use it to send the Invite message to Bob.

Question 6) 3 points total

6.) You recently implemented a layer 2 switching environment that uses OpenFlow …..

ANSWER

A flow is basically a series of packets sharing the same set of characteristics, and in an OpenFlow switch, these flows are managed by a construct called a flow table. Each packet entering an Openflow switch will pass through one or more flow tables, and each of these tables contains specific instructions on how the switch should handle the packet.

More specifically, each table contains match fields which are used to match against specific frame and packet header parameters, plus additional fields such as counters. The 5-tuple we have studied include some of the parameters that are used to determine a match. Other parameters include layer 2 header fields such as MAC addresses and VLAN tags.

If a packet matches a flow entry, then the set of actions defined by the entry are executed. The typical results are that the packet is sent to another flow table for processing, the packet is dropped, or the packet is sent out to the network via one of the ports.

If none of the entries in a flow table are a match, then a table-miss event occurs, and when this occurs, the actions defined for the table-miss flow entry will be executed on the packet. These actions commonly include: dropping the packet, sending the packet to another flow table for processing, or forwarding the packet to the OpenFlow controller. The OpenFlow controller evaluates the packet and determines how it should be handled. This can include creating a new entry in a flow table on the switch, and then sending the packet back to the switch for subsequent processing (which takes into account the new table entry.)

(The source for this information is section 5.4 of the OpenFlow spec version 1.4.)

Question 7) 3 points total EXTRA CREDIT

7.) We demonstrated in lecture a SIP softphone calling another SIP phone…. (Please see the homework for the complete question.)

ANSWER

You will receive three points for setting up your account and leaving a voicemail, or explaining why you were not able to place the call. (We have heard from students that the cs40 SIP voicemail did not answer some of the time.)