Homework 5

Scott Ouellette

Scott_Ouellette@hms.harvard.edu

1.) CAN-SPAM section 5.a.5 requires all bulk email senders to require an opt-out link on all emails, as well as certain other requirements. How might clicking on these opt-out links be counter-productive for the email recipient?

These opt-out links provided within spam emails could potentially server another purpose. A given link could indeed opt the receiving user out of getting anymore spam from a given spammer, but the action of clicking on the "opt-out" link could end up signing the receiver up to receive even more spam than before!

2.) All routers today implement policies for packet filtering and forwarding and most of them use what are called Access Control Lists (ACLs) to configure these policies. Do some research on a commercially available router that uses ACLs (pick the router vendor of your choice) and describe in detail how ACLs are used and how the packet filtering is done. Include specific examples of the ACLs in your answer, but note that you do not need to describe how the hardware implements the packet filtering and forwarding. Make sure to identify the router you are describing. Note that most of the routers meant for home networks do not allow users to configure or view the actual ACLs, rather, they use a simple GUI interface to set router policy; such a device would not be a good example for this question. Also, many of the commercial routers also provide a GUI interface to setting ACLs. For this question, it is important that you describe the use of the ACL, not the GUI interface.

For this question, I have chosen to research the Cisco ASR 1009-X router. From what I can derive, most modern Cisco products have an operating system installed called Cisco IOS which allows one to configure different functionalities of the device. The Cisco ASR 1009-X router also has a REST API that allows for the management of ACLs. ACLs are used to filter traffic on a given network. To configure an ASR 1009-X router's ACLs, one can login and perform some commands directly through the Cisco IOS shell. For example, a very basic ACL configuration to explicitly permit all traffic coming from the network: `192.168.34.0` would be: `access-list acl_permit permit ip 192.168.34.0 0.0.0.255`

There are many types of ACLs supported by this router including: Standard ACLs, Extended ACLs, IP Named ACLs, Reflexive ACLs, Time-Based ACLs, and many more. Standard ACLs allow for the comparison of the source address of IP packets against addresses that are either permitted or denied in the ACL listing. Extended ACLs provide a bit more functionality and allow for comparison of the source and destination addresses of IP packets against source/destination addresses that are either permitted or denied in the ACL list. Extended ACLs on this router also allow one to specify specific layer 3/4 protocols to filter as well such as IP, TCP, UDP, and ICMP. IP Named ACLs are available for configuration as well, allowing for both Standard and Extended ACLs to be given human readable names. For example, one could configure a named Extended ACL that only allows for telnet traffic between two specific hosts with the Cisco IOS command: `ip access-list extended in_to_out permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet` . As the list goes on, the granularity around what type of traffic one can configure to permit/deny gets finer. A Reflexive ACL can be used to filter based on upper layer session information. Time-based ACLs allow for allowing access during specific time frames.

3.) What is a X.509 certificate? What is a Certificate Authority? Given that anyone can create a public/private key pair on their own, describe why certificates and certificate authorities are necessary and how they are used?

An X.509 certificate at its simplest is a combination of asymmetric cryptography, hashing, and digital signatures. What this certificate is actually providing is: a way to verify that a website is trusted and is who they claim to be, a way for data to be transmitted confidentially,

and a way for ensuring the integrity of the data being sent between the parties (end-users and the website). Underneath it all the X.509 certificate is a digitally signed document reflecting a website's identity and public key.

Certificate Authorities are corporations that issue these digital certificates. It is integral that Certificate Authorities must be trusted by all actors in a given interaction on the web.

CAs are necessary because they allow for the prevention of the following attack scenario from being able to happen. Imagine a scene where there are two folks, User A & User B, that want to be able to transmit data amongst themselves securely. They have a notion of asymmetric cryptography and have shared their public keys with each other in a secure manner. Due to the fact that public key information is public, a bad actor could get their hands on these keys. They could then jump in between the users and probe their conversation by decrypting, reading/utilizing the payload, and re-encrypting then sending the message off to its intended destination. In this scenario, the original message would get to User B just fine and both users would have no clue that their information was being spied on. This is typically called a Man in The Middle attack.

The above scenario is avoided with the use of Certificate Authorities and X.509 certificates. As I mentioned before, everyone in the conversation must trust the CA. These folks trusting the CA will have a copy of said CA's public key information on their systems by a number of means. User A will still have their key pair as before, but they will send their public key off to the CA in a secure manner rather than directly to User B. The CA verifies that this key is coming from User A and will then digitally sign a certificate that includes User A's public key and an encrypted hash code and send it back to User A. User A can now share their certificate with User B and proceed to encrypt and send information as before. Now, any bad actor in the middle of these fine folks would not be able to intercept and re-encrypt the message with the same hash that the CA provided telling the receiving user that said message has been tampered with.

4.) Assume that you are submitting your homework via email. Describe in detail the methodology for using a digital signature using public-key cryptography to sign and submit your homework. (Note that an email that is digitally signed is not the same as encrypting it.)

To submit my homework over email and have the receiver be able to verify that it came from me and that its contents have not been altered I would have to encrypt as well as digitally sign said homework. Let’s assume that in this scenario that my homework was an extremely large file, and that it would take too many time units to encrypt with asymmetric cryptography. Let’s also assume that myself and the receiving party have securely transferred public keys.

First, I would run a one-way hash function over the contents of the homework and append said hash to the homework file. I would then create a session key and encrypt the contents of my homework, including this message digest, with it since it is much faster to do asymmetrically. I would then encrypt the session key with my private key and then again with the recipient's public key. I can, at this point, send the encrypted session key and encrypted homework over email. Once the homework is received, the recipient can then decrypt the session key with their private key and then again with my public key to get the session key. With the session key in hand, they can then go ahead and decrypt the contents of my homework. As a last check of integrity, they should run the same hash function over the contents of my homework to ensure that they see the same message digest.

5.) Describe the functionality and operation of a SIP proxy server and also the other types of SIP servers that would be used in a network to support VoIP. Try to be clear and specific in your answer about the functionality of each server since current real-world product implementations combine a lot of the functionality into a single box.

The other two types of servers that work in unison with the SIP proxy to support VoIP are: the Registrar server and the Location Server. As stated in the homework question it is quite often found that nowadays these services are all combined in one machine with marketing names like: Call Managers or Unified Communication Servers. While SIP clients are indeed able to communicate in a point-to-point manner, this requires the knowledge of the IP that you are to directly communicate with. To get around this limitation a combination of these three SIP Servers can be used. The SIP registrar is responsible for receiving and handling SIP REGISTER requests that contains a user’s identifying information, also known as an Address of Record. This identifying information would contain the IPs or locations of a given user's devices where they can currently be reached over SIP and could then be used to populate a database located on the SIP Location Server. When sip:usera@example.com wants to initiate conversation with sip:userb@example.com they will talk to a SIP Proxy which can then do a location query to the Location Server to get the last IP that sip:userb@example.com was known to be registered

with. The proxy can then pass along said information back to sip:usera@example.com where a media exchange will be initiated directly between the two users.

6.) Assume that you have recently implemented a Layer 2 switching environment in your network that uses OpenFlow. Assume that a packet enters the switch and a lookup is done in the flow tables in the switch, but no match is found. Describe the most common options for handling this packet. (Note: review the OpenFlow Switch Specification and the textbook for information on packet processing in OpenFlow switches.)

In this scenario, if no packet match is found, according to the OpenFlow specification the first step taken is to take a look and see if there is a matching table-miss flow entry. The table-miss flow entry states how a packet that hasn't been matched during a cycle of packet flow should be handled. From here, the packet could be sent off to the flow controller, dropped, or directed to another flow table where this match/table-miss cycle would happen again.

EXTRA CREDIT:

7.) In lecture, we will demonstrate a SIP softphone calling other SIP clients. Create an account for yourself on a SIP service provider (such as www.iptel.org) and using a SIP phone of your choice, call us at sip:cs40@iptel.org and leave us a voicemail message.

I was unable to make a successful call to cs40@iptel.org, but was able to connect to music@iptel.org and listen to The Turtles again