Assignment 8

1. **Send a spoofed email to stamp@cs.sjsu.edu. Do not identify yourself in the spoofed email. In your submitted solution include the contents of the spoofed email and explain how you sent the email.**

I used an EC2 instance on amazon AWS with Linux, used sendmail command to send the email to [stamp@cs.sjsu.edu](mailto:stamp@cs.sjsu.edu)

**Message:**

Subject: Student Complaint

Dear Professor Mark Stamp,

I have been informed that recently a student from your CS166 class has filed a complaint against you, claiming that you are unfairly grading his homework.

I will need you to explain that during the meeting on April 1st, 3pm at my office.

Regards,

Sami Khuri

--

Sami Khuri, Professor and Chair

Department of Computer Science

San Jose State University

One Washington Square

San Jose, CA 95192-0249

USA

Tel: (408) 924-5081

Fax: (408) 924-5062

eMail: sami.khuri@sjsu.edu

URL: http://www.cs.sjsu.edu/faculty/khuri

1. **What are the inherent security strengths and weaknesses of stateless protocols, as compared to stateful protocols? What are the inherent security strengths and weaknesses of stateful protocols, as compared to stateless protocols?**

The advantage of stateless protocol is that it is easier to design because it does not have to store any information about ongoing communication. For example if we use stateless protocol to communicate, if the client crashes or suddenly loses connection, in a stateless protocol, we do not have to worry about the communication because the system doesn’t know that it was communicating with another computer. Disadvantage of a stateless protocol, is that it has to accept all replies and process the information on the spot. And since it is a stateless protocol, when sending a message or receiving a message, we need to include more information about the current communication in the message.

In a stateful protocol, we have the advantage of remembering things; we can remember ongoing communication which can reduce the amount of information sent with the message to the server. A disadvantage of stateful protocol is that attackers can simulate one of the client and communicate with the server without having to give credential/information again.

1. **Provide a brief description of the IP "overlapping fragment attack" as discussed, for example, in RFC 1858. How can such an attack be prevented?**

The IP overlapping fragment attack consist of using the fact that different fragments on the same IP diagram that have offset can overwrite each other either fully or partially and with this fact, an attacker can send multiple fragments that may seem harmless, but when reassembled it can become harmful.

A firewall can be configured to prevent these kinds of attacks, by setting it to require a minimum for the offset of the fragment, therefore preventing overlaps.

1. **Recall the ARP cache poisoning attack discussed in class. How can you prevent such an attack? Does your suggested prevention measure create any potential vulnerability? Why or why not?**

There are many ways to prevent an ARP cache poisoning attack, one of the ways is making ARP protocol as stateful, that way we do not need to accept all replies and only accept replies that we actually requested. Another way is to make ARP cache static, so that the information in the cache has to be updated manually. A third solution is the “Dynamic ARP inspection” used by cisco; it prevents poisoning by intercepting all ARP request and response and then verifies its authenticity.

I think using Dynamic ARP inspection create the vulnerability of a DOS attack, because it has to intercept all ARP request and responses.

1. **Read this report, which discusses a 2007 attack on the DNS root servers. Write a brief summary of the report. In your summary, be sure to mention how the attack packets were successfully filtered.**

During 2007, at least six root DNS servers were hit by a DDoS attack from Asia-Pacific region. Out of the six DNS servers only the G-root ran by the US DoD and the I-root ran by the ICANN were affected, the reason of this is because only these two DNS roots haven’t installed “Anycast”. Anycast was invented due to the DDoS attack in 2002 that took down 9 out of 13 root DNS and root server operators decided that they have to improve the server’s stability. Anycast works by allowing different servers in different places to act as one, therefore being able to spread the load of a DDoS into many servers to relief the stress, Anycast can also spread the data around geographically so that even if one server is down, the other ones are still working.

In 2006 engineers discovered a DDoS attack on the DNS roots and they were able to see that all the attack packets are larger than 512-byte and since a normal query is around 100-byte, they just filtered out all the packets that are larger than 512-bytes.

1. **Outline a DoS attack that exploits the TCP 3-way handshake. Discuss possible defenses against such an attack and discuss possible countermeasures that Trudy could use to circumvent your suggested defenses.**

To perform a DoS attack that exploits the TCP 3-way handshake, we just have to keep sending SYN request to a server, since the server needs to keep a connection open for each SYN request, the server would be overwhelmed by the amount of connections open by all the SYN request that are received.

To prevent a DoS attack, we can simply ignore SYN request that comes from that computer, we can do that by blocking the IP address whenever we feel that it is a DoS attack, either by frequency of the SYN requests, number of SYN request, etc.

For Trudy to counter this defensive approach, Trudy would need to have different IP addresses to keep stressing the server. Main solutions to having multiple IP addresses can be either by proxy, or by performing a DDoS attack which would require the access of a lot of compromised computers to send request to a specific server.

References:

Problem 4: <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html>

<http://en.wikipedia.org/wiki/ARP_spoofing>

Classmates: Jay Patel, Jeffrey Su