CSCD27 – Network Security

Shih-Chin Liang 11/09/2014

Question 1: Course Feedback

Send it to you via email

Question 2: Key-Handling Vulnerabilities with Public-Key Systems

a) i) Yes, Eve, the eavesdropper, has to solve g^{ab} to obtain the messages given g. Consider the assumption that a and b is securely distributed, then solving g^{ab} given g is called Diffie-Hellman problem which is considered hard. This is because prime factorization is a NP problem. Therefore, before anyone prove P = NP assuming it is true which is very unlikely. Then, there doesn't exist an efficient algorithm for Eve to solve it. As a result, Diffie-Hellman (DH) Key-Exchange Protocol is secured against eavesdropping.

ii) No, Mallory can generate two keys one for Alice and another one for Bob. Then, a man in the middle attack is performed by exchanging the respective key with Alice and Bob. Now, Mallory can decrypt the message send from Alice and encrypt it to Bob and vice versa without them knowing.

b) i) Yes, it's secure against Eve if the RSA is configured properly. Again, it is because finding the prime factorization is a NP problem for large number. Therefore, it's computational infeasible to do it.

ii) No, it's not secure. Even though the encryption algorithm changes, but Mallory can still do the same trick described above(2a)ii)).

c) i)As argue above(2b)i)), it's secure against Eve.

ii) It's secure against Mallory now assuming RSA is properly configured. It's because Mallory can't create public keys for each of them(Alice and Bob) and secretly be their bridge of communication.

d) i), ii) , iii) As argued in 2c), the method is secured against Eve and Mallory. Thus, adding another security feature won't weaken the security overall because it's already secured. However, the added security feature can prevent the attacker from getting all their message if one message has been break.

Question 3: Don't be Evil

Partner: Carmen Flores 998906983

Question 4: Exploiting Weak RSA Keys to Decrypt HTTPS Packets

```
POST /cscd27f14/ViewSecret HTTP/1.1
Content-Type: application/x-www-form-urlencoded
charset: utf-8
Cache-Control: no-cache
Pragma: no-cache
```

```
User-Agent: Java/1.6.0_32
Host: mathlab.utsc.utoronto.ca:41414
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 42

username=cscd27f14&password=dcf35c470d090eHTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=C6A1FEDAD4A91D5F62FE504D50670D39; Path=/cscd27f14; Secure
Content-Type: text/html
Content-Length: 1034
Date: Thu, 06 Nov 2014 21:32:59 GMT

<html>
<head>
<title>Secrets of Happiness</title>
</head>
<body>
<h1>Secrets of Happiness</h1>
<ul>
<li>'It is not easy to find happiness in ourselves, and it is not possible to find it
elsewhere.'</li>
<li>'All happiness depends on a leisurely breakfast.'</li>
<li>'If you want happiness for an hour, take a nap.<br/> If you want happiness for a day,
go fishing.<br/> If you want happiness for a year, inherit a fortune.<br/> If you want
happiness for a lifetime, help someone else.'</li>
<li>'When one door of happiness closes, another opens, but often we look so long at the
closed door that we do not see the one that has been opened for us.'</li>
<li>'Happiness is when what you think, what you say, and what you do are in harmony.'</li>
<li>'To be without some of the things you want is an indispensable part of happiness'</li>
<li>'Optimism is a happiness magnet. If you stay positive, good things and good people
will be drawn to you.'</li>
<li>'Ice cream is happiness condensed.'</li>
</ul>
</body>
```

The value of p is 819412462441404687809382611 3

The value of q is 155433647198461027340359052650210078745279090728577075304079292906871010999 5023538012485471003433330828566020298075769650392568387374649187786550771989902725120710 2262278680571817169261263452242836721127096300509656928177929591710741117876178047883330343700515792044255540432173197

After reading various different methods mentioned in the assignment, we quickly come to an agreement that it is either balanced and unbalanced prime. Therefore, we run algorithm for both method and the Lenstra elliptic curve factorization is one of it. It's because there is an easy to use python implementation online and also it is the fastest algorithm to find small divisors.

Question 5: SSL Stripping

Snippet:
2014-11-09 19:36:04,818 Sending header: host : www.facebook.com
2014-11-09 19:36:04,818 Sending header: referer : http://www.facebook.com/
2014-11-09 19:36:04,818 Sending header: cookie : datr=YwhgVOfj-sws4S6FcZdeFXJT; reg_fb_ref=
https%3A%2F%2Fwww.facebook.com%2F;reg_fb_gate=https%3A%2F%2Fwww.facebook.com%2F
2014-11-09 19:36:04,818 Sending header: content-type : application/x-www-form-urlencoded
2014-11-09 19:36:04,818 SECURE POST Data (www.facebook.com):
lsd=AVrw5w6M&email=adsonly%40live.com&pass=password&default_persistent=0&timezone=
&lgnrnd=163547_Cm40&lgnjs=n&locale=en_GB
I have an account called adsonly@live.com and for safety reason I entered my password as password. This works because I empty everything before I run the script. So, this is the first http request.
a) SSL stripping uses the fact that SSL connection is normally encountered by HTTP connection. Thus, it focuses the attack on the http connection. It's done by changing http:// links to https:// link or <a href=https://> to <a href=http://...> and store the maps. When the client send an http request for the SSL connection proxy it as HTTPS connection to the server. So, both side thinks the connection is secured, but the traffic is being monitored by the attacker because the client is sending the information in http instead of https.
b)The easiest way is to check the URL. If the user are entering log in information in SSL and the URL isn't https, then the user knows s/he is under attack.
c) HTTP Strict Transport Security is used to prevent SSL stripping attack. The policy now forces the client and the domain and the sub domain always maintain SSL connection whenever there is a connection between the server and the client for a period of time set by max-age.
d) This still doesn't solve the problem. There are multiple reasons. First, in order for HSTS to work, the client still have to establish an initial connection with the server first. The same attack can still applied to it. Second, the HSTS can be destroyed manually for example in a browser like Firefox. Thus, if the attacker gains access in victim's computer. It can still perform SSL stripping attack without the user knowing it. Thirdly, according to Leonardo Nve's BlackHat talk in Asia this summer, altering the DNS server can still bypass the security layer HSTS build. Finally, the development of HSTS is limited. There are still 33% of people's browser haven't implemented HSTS. http://caniuse.com/#feat=stricttransportsecurity

Question 6: ARP-Cache Poisoning

A)The man in the middle attack can be done by using the software Ettercap.
The complete tutorial including setup(Step 1-3) is here.

http://www.chmag.in/article/jun2012/mitm-ettercap

Assuming the setup is done.
With little technical expertise, the attacker can just simply input #ettercap –Tq –M arp:remote /«T»/ where T is the IP of the target with root privilege.
Since this is not a well configured OS, thus 100 percent attack success rate can be achieved.

B)Assuming there was no previous request, Mallory can begin the attack by sending a malicious ARP reply to Bob in which it associates m(Mallory's MAC address) to A(Alice's IP address). Bob's computer will now think Mallory's computer is Alice. Next, Mallory then send a malicious ARP reply to Alice's computer, associating m(Mallory's MAC Address with Bob's IP. Alice's computer will now think Mallory's computer is Bob. Then, Mallory can turn on IP forwarding. This will enable Mallory's computer to forward the traffic from Alice to Bob. At this stage, any traffic between Alice and Bob has been forwarded to Bob or Alice. Alice and Bob should remain unaware of their communication has been intercepted.

C)Assuming the LAN is small. By manually assigned static ARP entries to all computers can prevent the attacker from doing any ARP-Cache Poisoning related attack. However, just as the assumption stated, this only works for a small network.

D)The attacker can just simply sending ARP reply continuously in which the IP address is associated with different MAC addresses. When this happens, the tool will keep blocking the IP address of the computer even when the system admin is constantly investigating/clearing. Thus, the denial-of-service attack is launched successfully.

Question 7: TCP SYN-Cookies

a)No, ack flood works on pre-established connection, then flood the server with fake ack request. The server with SYN-Cookies can validate the ack. So, if some amount of fake acks has been send from the client, then the server can prevent the ack flood by dropping the connection between the client and server. However, in the extreme case, where every connection in the queue is performing ack flood, then the server might be congested for verifying all the acks from all the connections/clients in the queue.

b)Yes, if the attacker obtains enough SYN-Cookies value, then they could packed the SYN-Queue by tricking the server to believe they are legit connection, and the method SYN-Cookies relied on to solve the filled queue won't work anymore because the server won't be able to rebuild the queue in quick succession. However, since the SYN-Cookies value only last for a short period of time. This is not really practical.