Assignment 2

William Mak

November 07 2014

1 Course Feedback

See Email

2 Key-Handling Vulnerabilities with Public-Key Systems

A i Eve will not know enough information to decipher any future messages between Alice and Bob

ii No this scheme is insecure against Mallory she would be able to modify $g^a modp$ or $g^b modp$ with her own values. Alice and Bob will still be able to send messages between each other but Mallory would also be able to read them.

B i Yes this will be secure against Eve, even though she can see the public keys this is not enough for her to decipher any of the messages.

ii No Mallory could insert her own public key instead of either or both Alice and Bob's keys. In this case her own private key would be able to decipher any future messages.

C i Yes, there's absolutely nothing Eve can do to read the messages between Alice and Bob.

ii Yes, Even if Mallory knew their public keys she wouldn't be able to read the messages or create her own.

D i Yes, there's absolutely nothing Eve can do to read the messages between Alice and Bob.

ii Yes, Mallory would not be able to do anything to the messages betwwen Alice and Bob.

iii Yes, In the very unlikely case that Mallory can brute force either of their private keys in the previous case she would be able to modify messages between Alice and Bob. But in this case she would have less than a day to brute force the key and she would only be able to modify messages for one day.

3 Don't be Evil

See Mathlab submission

4 Exploiting Weak RSA Keys to Decrypt HTTPS Packets

Primes:
$p = 155433647198461027340359052650210078745279090728577075304079292906871010999502353801248547100343333082856602029807576965039256838737464918778655077198990272512071022622786805718171692612634522428367211270963005096569281779295917107411178761780478833303437005157920442555404321731 97$
$q = 819412462441404687809382611 3$

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=A97E8AD20E35C5261C973B16A001F1EE; Path=/cscd27f14; Secure
Content-Type: text/html
Content-Length: 1034
Date: Fri, 07 Nov 2014 18:29:48 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>'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 fish
<li>'When one door of happiness closes, another opens, but often we look so long at the closed do
<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 dr
<li>'Ice cream is happiness condensed.'</li>
</ul>
</body>
</html>
```

4.1 Method used to determine primes

To determine the prime factors of the modulus we used a piece of software called yafu(http://yafu.sourceforge.net/). Examining the source it uses a wide variety of algorithms in a very complicated manner. These include "Shanks Square forms factorizations", "Fermat's Factorization method", and "Pollard Rho Factorization method". Using these methods Yafu was able to compute both factors in a very reasonable amount of time.

5 SSL Stripping

A SSLstrip relies on severla use cases. First it assumes that a user will not type out the full "https://" in their browser since it needs to pretend to be a HTTPS session while being HTTP. Secondly it requires there to be traffic from non-ssl pages to secure ssl pages.

B The best way to thrwart someone using SSLStrip is to ensure their site has SSL enabled on every page.

C A site like facebook's best way to protect against this is to make it extremely clear when switching to and from SSL so the user has no confusion as to which is which. As well as informing the user of the risks if this happens.

D Yes since HSTS forces web browsers to use HTTPS and never with HTTP

E Snippet:

```
2014-11-09 00:34:44,612 Sending header: content-type : application/x-www-form-urlencoded
2014-11-09 00:34:44,612 POST Data (www.facebook.com): lsd=AVq2omPV&email=email%
40hotmail.ca&pass=supersecurepassword&default_persistent=0&timezone=&lgnrnd=21332
_-VDl&lgnjs=n&locale=en_US
```

6 ARP-Cache Poisoning

A A simplistic ARP attack would be to send an ARP reply to a victim telling them the false location to something system critical, for example the router. This would cause the victims system to be unable to access that resource. This would only work if the victim's system is accepting unsolicited replies.

B If Mallory wanted to perform a Man in the Middle attack on Alice and Bob she would start by sending a "reply" to Bob stating that her computer's MAC address was Alice's a, now Bob will think that Mallory's IP address M is Alices A. Next Mallory sends a "reply" to Alice stating that her MAC address was Bob's b, now Bob will think Mallory's IP address M is Bob's B. Now finally whenever Alice sends a packet to Bob her packet will be received by Mallory instead who can do whatever she likes. And the forwards it along to Bob. and vice versa for any traffic coming from Bob.

C The easiest solution would be to use static IP tables this means that there is no confusion as to which IP address is who on the network. This would address any issues with preexisting computers on the network. But this would still be problematic if when a new computer joins the network there is already a Man in the Middle.

D This tool would only slow an attacker down, in both scenarios described in previous questions they only have at most 3 different IP addresses and MAC addresses. Which means they would be only able to launch this attack against one or two devices in the network, every 30 seconds. Which with a patient attacker isn't that big a deal.

7 TCP SYN-Cookies

A Yes, if the attacker responds with an invalid **ACK** code. As well the attacker can spoof their IP address in the SYN which means that the server will send their requests to a falsified IP address and then waste resources on these invalid cookies.

B No, probably not since most of the IP addresses in the SYN will be valid the server will have no trouble getting a response from them. But in the case that the attacker has enough bandwidth to overpower the server it would still go down from the overwhelming number of requests.