HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 5

Mehmet Taha USTA – 21527472

Subject: Man-in-the-middle attack on Diffie Hellman. Explain

Man In The Middle Attack

In this attack type, various listening operations are carried out by infiltrating between 2 connections and the capture of the desired data is started. There is more than one way to start the listening process to join the network and solve the unencrypted connection between the 2 networks. In some of these methods, the client actually logs on to the server site, but the data transferred while sending the request can be transmitted to the middle attacker. In some attack types, the client accesses a copy of the same page prepared by the attacker before reaching the real site and transfers the information of the site he wants to login to the attacker, if it is not careful, the copy prepared by the attacker can give the site to the site. Attack methods such as MITM can be done without the need for very serious network knowledge, and also we come up with software that integrates into different operating systems. With these softwares, the system to be attacked is determined by just a few clicks, and the listening process is initiated, and then MITM can be implemented, and even the ssl systems can be modified thanks to the built-in certificate system for the vehicle used.

For attackers to succeed in MITM attacks, the victim must direct the victim to the proxy server rather than the actual server.

The following scenarios are implemented in this;

1.LOCAL AREA NETWORK (Local Area Network):

    1.1.ARP poisoning

    1.2.DNS spoofing

    1.3.STP mangling

2.FROM LOCAL TO REMOTE (Remote Local Area Network):

    2.1.ARP poisoning

    2.2.DNS spoofing

    2.3.dhcpspoofing

    2.4.ICMP redirection

    2.5.IRDP spoofing - route mangling

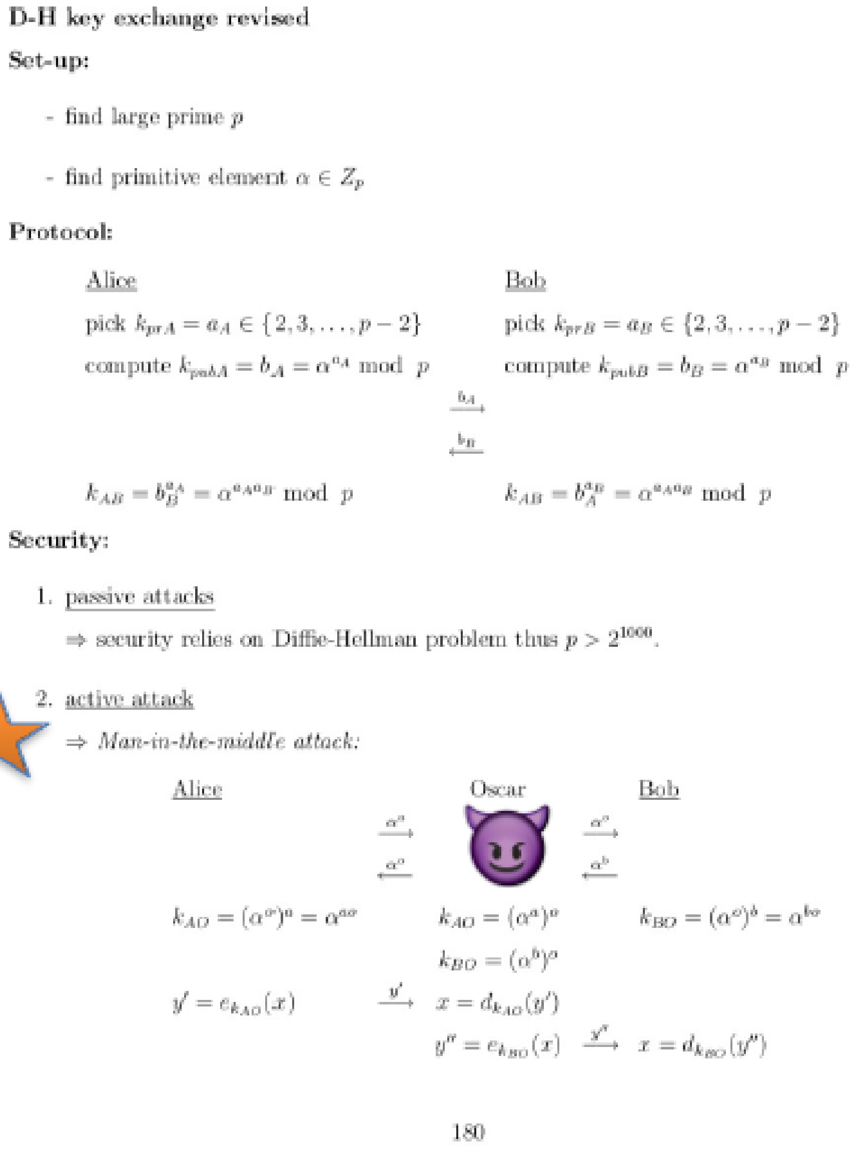
3.REMOTE (Remote Network):

    3.1.DNS poisoning

    3.2.Traffic tunneling

    3.3.Route mangling

FOR INSTANCE MAN IN THE MIDDLE ATTACK ON DIFFIE HELLMAN



D-H key exchange revised

Set-up:

- find large prime p
- find primitive element $\alpha \in Z_p$

Protocol:

Alice		Bob
pick $k_{prA} = a_A \in \{2, 3, \ldots, p-2\}$		pick $k_{prB} = a_B \in \{2, 3, \ldots, p-2\}$
compute $k_{pubA} = b_A = \alpha^{a_A} \bmod p$		compute $k_{pubB} = b_B = \alpha^{a_B} \bmod p$
	$\xrightarrow{b_A}$	
	$\xleftarrow{b_B}$	
$k_{AB} = b_B^{a_A} = \alpha^{a_A a_B} \bmod p$		$k_{AB} = b_A^{a_B} = \alpha^{a_A a_B} \bmod p$

Security:

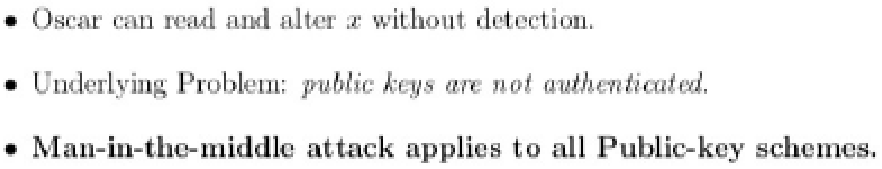
1. passive attacks

   ⇒ security relies on Diffie-Hellman problem thus $p > 2^{1000}$.

2. active attack

   ⇒ *Man-in-the-middle attack:*

Alice		Oscar		Bob
	$\xrightarrow{\alpha^a}$		$\xrightarrow{\alpha^o}$	
	$\xleftarrow{\alpha^o}$		$\xleftarrow{\alpha^b}$	
$k_{AO} = (\alpha^o)^a = \alpha^{ao}$		$k_{AO} = (\alpha^a)^o$		$k_{BO} = (\alpha^o)^b = \alpha^{bo}$
		$k_{BO} = (\alpha^b)^o$		
$y' = e_{k_{AO}}(x)$	$\xrightarrow{y'}$	$x = d_{k_{AO}}(y')$		
		$y'' = e_{k_{BO}}(x)$	$\xrightarrow{y''}$	$x = d_{k_{BO}}(y'')$



- Oscar can read and alter x without detection.
- Underlying Problem: *public keys are not authenticated.*
- **Man-in-the-middle attack applies to all Public-key schemes.**