

# How does the man in the middle attack work in Diffie–Hellman?

Asked 12 years, 7 months ago   Modified 2 years, 5 months ago

Viewed 105k times



41



I'm having doubts about the mechanics of a man in the middle attack during a Diffie–Hellman key exchange. I have heard that it can happen during the key agreement communication. But in the presence of CA (Certificate Authority) the receiver can authenticate the sender as he received the sender's public key. Therefore, how is a man in the middle attack possible?

public-key-encryption

diffie-hellman

Share

Improve this question

Follow

edited May 25, 2012 at 12:34



Leigh

28.9k ● 10 ● 57 ● 108

asked May 6, 2012 at 13:48



Chanikag

1,439 ● 2 ● 19 ● 32

2 Answers

Sorted by:

Highest score (default)





100

I think you're confusing the basic Diffie-Hellman, which is a key exchange protocol, with the 'authenticated version' which uses a certificate authority (CA).



Nice explanation of how the basic Diffie-Hellman is vulnerable to man-in-the-middle [from RSA Labs](#).



"The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. In this attack, an opponent Carol intercepts Alice's public value and sends her own public value to Bob. When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice. Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key. After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants."

and it follows with the authenticated version, also known as the [Station-to-Station protocol](#):

"Roughly speaking, the basic idea is as follows. Prior to execution of the protocol, the two parties Alice and Bob each obtain a public/private key pair and a certificate for the public key. During the protocol, Alice computes a signature on certain messages, covering the public value  $g^a \bmod p$ . Bob proceeds in a similar way. Even though Carol is still able to intercept messages between Alice and Bob, she cannot forge signatures without Alice's private key and Bob's private key. Hence, the enhanced protocol defeats the man-in-the-middle attack."

So the basic version is susceptible to a man-in-the-middle attack, the authenticated version that uses public key certificates is not.

Share Improve this answer

Follow

edited Jul 22, 2022 at 13:57



Bruno Rohée


3,524 ● 28 ● 32

answered May 8, 2012 at 10:16



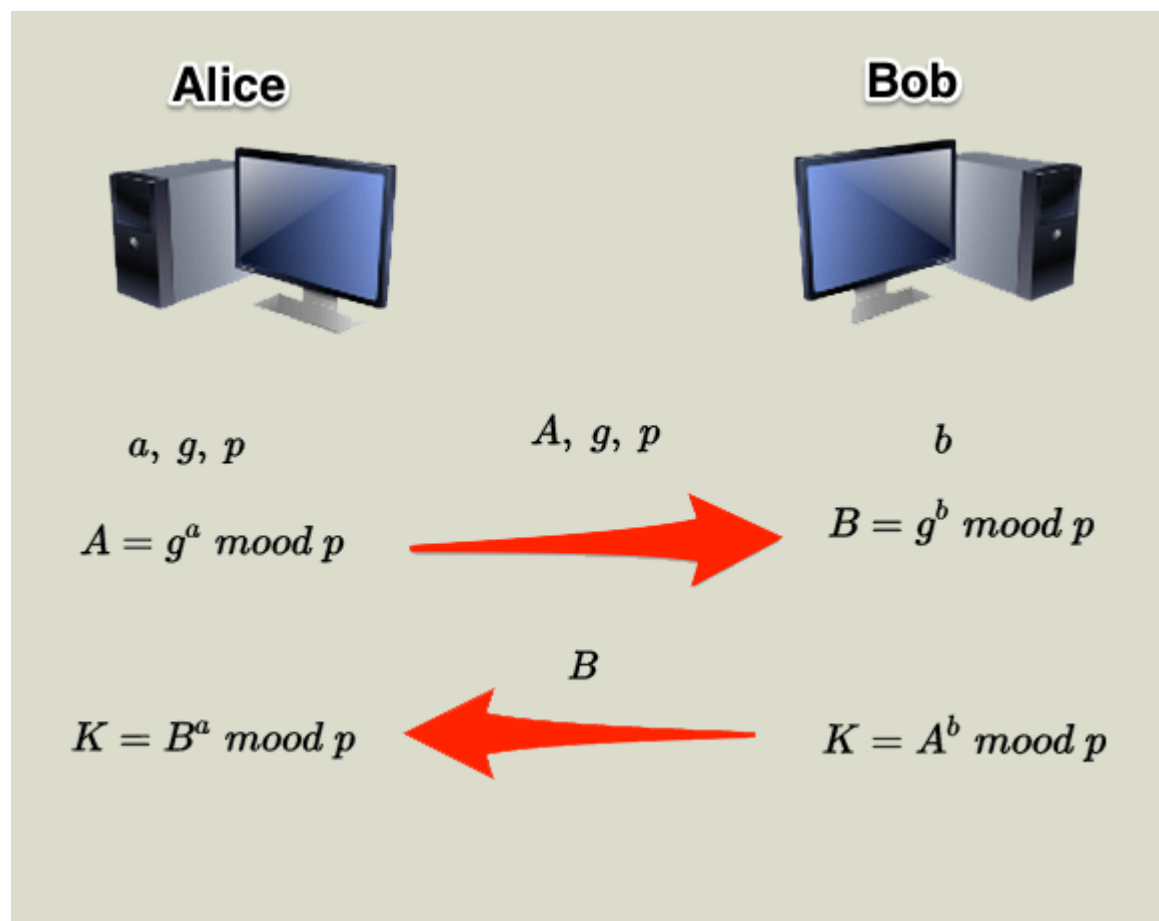
Peanut

2,251 ● 2 ● 26 ● 38

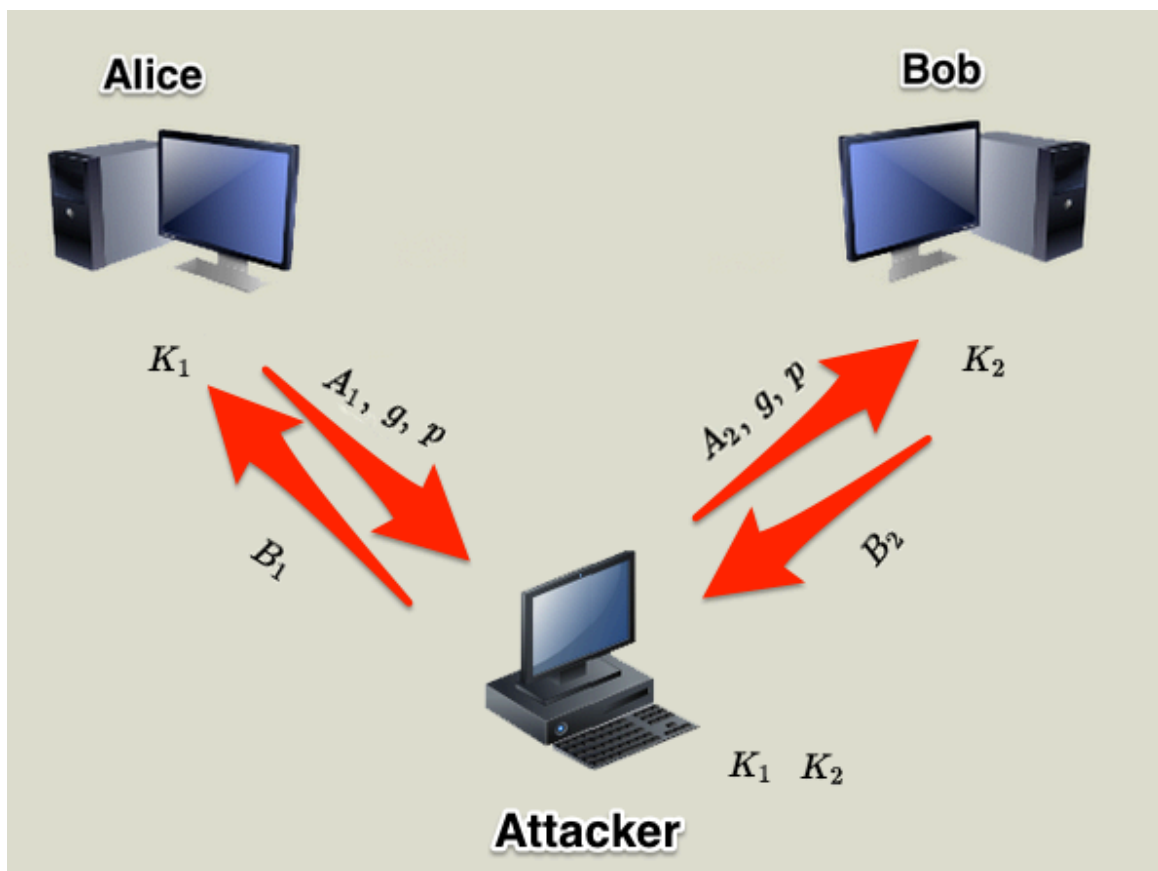
- 
- 3 Yes, someone listening to the medium won't be able to intercept, but someone bridging the medium would. However the authenticated version does not make sense at all. If you already hold a certificate and therefore public key of the other party, what's the point in using DH ? – Rafael Jul 16, 2013 at 13:22 
-

I don't think I understand your point... Why are you differentiating between listening and bridging? They're both just forms of interception, and as the answer says in the authenticated version it's fine for messages to be intercepted as the interceptor can't fake the messages. In the authenticated version at the start of the protocol the parties don't have the other party's public key certificate. – [Peanut](#)  
Jul 16, 2013 at 14:24 ✎

This is how Diffie-Hellman works:



And this is how the man-in-the-middle attack works in Diffie-Hellman:



There are two D-H key exchange, Alice and Attacker share the same key with  $K_1$ , while Bob and Attacker share the other same key with  $K_2$ .

Because Alice and Bob had no prior knowledge of each other.

But the Attacker must keep listening and forwarding.

Share Improve this answer

Follow

edited Aug 12, 2018 at 22:54



Achala Dissanayake

860 ● 3 ● 16 ● 35

answered Oct 17, 2013 at 2:38



JZAU

3,567 ● 33 ● 38

Can you edit your answer and post the images again please? Maybe using [imgur.com](https://imgur.com) so they won't break again.

– [orange](#) Dec 12, 2014 at 17:18

---

10 Why mood? Is is it not called mod? – [matfax](#) Jul 30, 2017 at 13:31

---

@MatthiasFax Yes, you are right. Sorry about the typo.

– [JZAU](#) Jul 30, 2017 at 23:38

---