Attacking the Interlock Protocol

Abstract

The Interlock Protocol is used as a mechanism to foil the Man in the Middle Attack, however by the attack proposed below, it is shown that the Interlock Protocol is insecure. It involves faking the first packet of the communication and the ‘man in the middle’ sending forth half of the (n) th packet when he receives half of the (n+1) th packet and completes the attack.

Keywords: Man in the Middle Attack, Interlock Protocol.

Introduction

Let Alice and Bob be two legitimate users attempting secure communication with out a shared secret and Mallory be the Man in the Middle.

The following are the sequences of the Man in the Middle Attack.

1. Alice sends Bob her public key. Mallory intercepts it and sends Bob his own public key.
2. Bob sends Alice his public key. Mallory intercepts it and sends Alice his own public key.
3. Then Alice sends a message encrypted by "Bob’s" public key. Since the message is really encrypted with Mallory's public key, he decrypts it with his private key, re-encrypts it with Bob's public key and sends it to Bob.
4. Then Bob sends a message to Alice, encrypted using "Alice’s " public key, which is again Mallory's public key, he decrypts it with his private key, re-encrypt with Alice's public key and send it to Alice.

The following are the sequences that define the Interlock Protocol.

1. Alice sends Bob her public key
2. Bob sends Alice his public key
3. Alice encrypts her message with Bob's public key. She sends half of the encrypted message to Bob.
4. Bob encrypts his message using Alice's public key. He sends half of the encrypted message to Alice.
5. Alice sends the other half of encrypted message to Bob.
6. Bob puts the two halves of Alice's message together and decrypts it with his private key. Bob sends the other half of the message to Alice.
7. Alice puts the two halves of Bob's message together and decrypts it with her private key.

Here Mallory can still substitute his own public key for Alice and Bob. Now when he intercepts half of Alice's message, he cannot decrypt it with his private key and re-encrypt it with Bob's public key .He must invent a completely new message and send half of it to Bob. When he intercepts half of Bob's message to Alice, he has the same problem. He cannot decrypt with his private key and re encrypt with Alice's public key. By the time the second half of the message of Alice and Bob arrive, it's already too late to change the new message he invented. The conversation between Alice and Bob need to be completely different. However if Mallory can mimic Alice and Bob, they might not realize that they are being duped and may get away with his scheme.

The Attack

The attack involves faking the first full-transmitted packets of Alice and Bob. Then Mallory transmits the half of the (n) th packet when he receives the (n+1) th packet.

It is explained as below.

Let
A=Alice
B=Bob
M=Mallory

1:1 indicate first packet, first half
1:2 indicate first packet, second half

2:1 indicate second packet, first half
2:2 indicate second packet, second half
and so on.

An empty column in the table denotes the actual sender.

No:	Alice	Mallory	Bob
1		A->1:1	M->1:1
2	M->1:1	B->1:1	
3		A->1:2	M->1:2
4	M->1:2	B->1:2	
5		A->2:1	A->1:1
6	B->1:1	B->2:1	
7		A->2: 2	A->1:2

Since the first full packet is faked, Mallory has one full packet of Alice with which he can decrypt with his private key and re-encrypt it with Bob's public key and vice versa and successfully launch the Man in the Man in the Middle Attack .It is assumed that a delay in the first block does not rise suspicion and for the attack to be successful more than one block is to be transmitted. This attack on the Interlock protocol works even if an initialization vector or hash be used, since it can be faked by Mallory.

E.g.: Consider that every message except the very first one has a hash of the previously received message as follows

A -> (M ->) B: half 1 of message A1

B -> (M ->) A: half 1 of message B1 | hash (half 1 of message A1)

A -> (M ->) B: half 2 of message A1 | hash (half 1 of message B1)

B -> (M ->) A: half 2 of message B1 | hash (half 2 of message A1)

A -> (M ->) B: half 1 of message A2 | hash (half 2 of message B1)

and so on. Since M captures A1 and B1, he can compute the hashes for both the initial message and the one that follows. Hence the attack still works.

E.g.: Consider they send the hash of the other half as follows

A -> (M ->) B: half 1 of message A1 | hash (half 2 of message A1)

B -> (M ->) A: half 1 of message B1 | hash (half 2 of message B1)

A -> (M ->) B: half 2 of message A1 | hash (half 1 of message A1)

B -> (M ->) A: half 2 of message B1 | hash (half 1 of message B1)

and so on.M fakes the first message in both direction, and then computes the hashes. The attack still works.

Conclusion

The Interlock protocol says the conversation of Alice and Bob must be completely different. How ever by the above shown attack it is obvious that if the first packet in both directions is faked, the Inter Lock Protocol fails.

Appendix

Man In the Middle Attack - Modification of transmitted data in a communication channel by an intruder in the channel when the communicating parties have no shared secret.

Interlock Protocol - A protocol used to foil the Man in the Middle Attack for real time communication.

Bibliography

1. Bruce Schneier*, Applied Cryptography*, Wiley Publications, Second edition, 2001.

PS: The Man in the Middle Attack and the Interlock Protocol is extracted for reference as in (1)

Reviews

Sincere thanks to Marcel Popescu, Dr. Mike Rosing and Bruce Schneier for their valuable time in reviewing the same.

By Sarad A.V
S.I.T, Tumkur.
Karnataka, India.