Preventing Man-in-the-Middle Attacks with Diffie-Hellman Key Exchange and Authentication

h = hash(plaintext, salt) e = encrypt(plaintext, key) d = decrypt(ciphertext, key)

MAN IN THE MIDDLE ATTACK ON STANDARD AUTHENTICATION METHOD

Alice	Mallory	Bob
password = 54321		password = 54321
key = zzz	alice key = zzz (DH MITMA)	key = yyy
	bob key = yyy (DH MITMA)	
e(password,key) = passhash		e(password,key) = passhash
e(54321,zzz) = "deadbeef"		e(54321,yyy) = "badcoded"
SEND: "deadbeef"	d(deadbeef,zzz) = 54321	
	e(54321,yyy) = "badcoded"	
	SEND->Bob: "badcoded"	
		RECV: "badcoded" matches
	MITMA successful :(	

NEW AUTHENTICATION METHOD

Alice	Bob
password = 54321	password = 54321
key = zzz	key = zzz
h(54321,key) = "blahwoot"	h(54321,key) = "blahwoot"
SEND: "blahwoot"	
	RECV: "blahwoot" matches
h(ok,password) = GOOD!	h(ok,password) = GOOD!
h("ok",54321) = "awesome"	h("ok",54321) = "awesome"
	SEND: "awesome"
RECV: "awesome" matches	
pubkey now saved for future use in known_hosts	
DH + authentication verified	

MAN IN THE MIDDLE ATTACK ON NEW METHOD

Alice	Mallory	Bob
password = 54321		password = 54321
key = zzz	alice key = zzz (DH MITMA)	key = yyy
	bob key = yyy (DH MITMA)	
h(password,key) = passhash		h(password,key) = passhash
h(54321,zzz) = "blahwoot"		h(54321,yyy) = "wtfmate"
SEND: "blahwoot"	can't reverse hash to get pass!	
	can't send h(ok,password)	RECV: "blahwoot" != "wtfmate"
	doesn't know password	**SEND: BAD!**
RECV: BAD!		
pubkey NOT saved in known_hosts		
both sides fail authentication		

Samy Kamkar - samy@samy.pl - August 4, 2009