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

\[ h = \text{hash}(\text{plaintext, salt}) \quad e = \text{encrypt}(\text{plaintext, key}) \quad d = \text{decrypt}(\text{ciphertext, key}) \]

**MAN IN THE MIDDLE ATTACK ON STANDARD AUTHENTICATION METHOD**

```
Alice
password = 54321
key = zzz
e(password, key) = passhash
e(54321, zzz) = "deadbeef"
SEND: "deadbeef"
```

```
Mallory
alice key = zzz (DH MITMA)
```

```
Bob
password = 54321
key = yyy
e(password, key) = passhash
e(54321, yyy) = "badcoded"
```

```
d(deadbeef, zzz) = 54321
e(54321, yyy) = "badcoded"
SEND->Bob: "badcoded"
```

**RECV: "badcoded" matches**

**NEW AUTHENTICATION METHOD**

```
Alice
password = 54321
key = zzz
h(54321, key) = "blahwoot"
SEND: "blahwoot"
```

```
RECV: "blahwoot" matches
pubkey now saved for future use in known_hosts
```

```
h(ok, password) = GOOD!
h("ok", 54321) = "awesome"
```

```
RECV: "awesome" matches
```

**MAN IN THE MIDDLE ATTACK ON NEW METHOD**

```
Alice
password = 54321
key = zzz
h(password, key) = passhash
h(54321, zzz) = "blahwoot"
SEND: "blahwoot"
```

```
Mallory
can't reverse hash to get pass!
can't send h(ok, password)
doesn't know password
```

```
Bob
password = 54321
key = yyy
h(password, key) = passhash
h(54321, yyy) = "wtfmate"
```

```
RECV: "blahwoot" != "wtfmate"
SEND: BAD!
```

**RECV: BAD!**

pubkey NOT saved in known_hosts

**both sides fail authentication**

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