**NATIONAL INSTITUTE OF TECHNOLOGY DELHI**

**Department of Computer Science & Engineering**

**CSB451 – Network Security & Cryptography**

***Assignment – 9***

**Submitted By:**

**Himanshu Verma 201210023**

**Submitted To: Dr Karan Verma**

1.a A password is easier to remember than a MAC secret key.

A human can run a password-based authentication protocol without a computer (e.g., over the phone).

1.b A MAC allows authenticating a request (not just a principal).

An attacker who sees many MACd messages cannot produce new ones. (In contrast, an attacker who observes a password login learns your password.)

1.c MACs are faster to compute.

MACs are shorter (128 bits versus 384 bits or more)

1.d Signatures do not require a shared secret.

Many parties can verify a single signature.

2. **Attack:** The attacker observes Alice’s authentication attempt. Then the attacker sends the same tag t to the server later on. Essentially, the MAC tag ‘t’ here acts as a password.

**Fix:** At authentication time, the server chooses a random 256-bit nonce and sends it to Alice. Alice must apply the MAC to the nonce and her username.

**3.** The attacker can find a collision in H in roughly 2 64 time. Therefore the attacker can find two messages that have the same MAC tag in roughly this much time.

**4.**

|  |  |
| --- | --- |
| Direct Digital Signature | Arbitrated Digital Signature |
| It only requires the communicating parties. | It requires an arbiter along with communicating parties to send or receive messages. |
| In this the digital signature encrypts the whole plain text with the sending party’s private key. | The encrypted message is send by X to arbiter Z with Y’s id, timestamp and some random number PQ. |
| The message is directly transmitted between both parties without any help from an intermediate. | An arbiter is needed to transmit the message. |
| The timestamp is not maintained by both sides. | The timestamp is maintained by all three members by default. |
| It clocks a processing speed of 16 MHz. | While Raspberry Pi clocks a processing speed of 1.4 GHz. |
| It is implemented using public key. | It is implemented using private key. |
| Vulnerable to any kind of replay attack. | The timestamp is used to protect the message from any kind of replay attack. |
| Trust is needed between sender and receiver because of the absence of an independent verification process. | When using an arbitrator, the sender and the receiver must have trust that the arbitrator will not only time-stamp and send the document as directed, but also take care that there should not be any kind of modification in the data. |
| Requirement of private key to be held by sender and public key by both sender and receiver and incase the sender lost the key then he asserts that signature is forged. Having the private key stolen and then falsifying signatures is a potential security risk when utilizing a direct digital signature. | There is possibility of biasing that an arbiter will be biased in favor of one party or the other if any discretion is used. |