0.1 Security Model

Public Key Encryption (PKE) and Public Key Message Authentication (PKMA) schemes are two of the most significant and well studied cryptographic primitives. Traditionally, both notions are defined as non-interactive (i.e., used for single messages). Both the sender and receiver need not keep any state, such non-interactive "one−and−done" philosophy is also crucial in many applications. Joined with the fact that we now have many efficient candidates for both signature and encryption schemes, it might appear that there is limited benefit in prolonging the syntax of signature/encryption schemes to allow for possibly interactive realizations.
The biggest disadvantage of non-interactive signatures is the fact that there is no interaction between the sender and the receiver. Hence, this works for a single message only which is very limited. To avoid this, a new scheme was proposed by [**?**] that assumes the presence of interaction between the sender and the receiver which is logical especially in the case where there is a conversation. This new scheme is "Interactive Encryption and Message Authentication" [**?**]

This interactive scheme offers some advanced security properties which are impossible to be achieved with the non-interactive schemes, Deniability and Forward Security.

- ***Deniability:*** A Public Key Message Authentication protocol is deniable if the sender S can authenticate a message m to the receiver R in such a way that R cannot use the transcript of their conversation as evidence to later convince third parties about the fact that S took part in the protocol and authenticated m.
- ***Forward Security:*** Forward security guarantees that any leak of secret information at some time t should not affect the security of protocol runs that occurred in the past, i.e., at any time $t' < t$. Forward security is a desirable property that is not known to be achieved by standard non-interactive public key encryption.

We consider a problem that consists of an attacker "Alice" who already has breached a network and gained access to a machine controlled by a victim "Bob". Alice intends to exfiltrate data from Bob's machine to her machine via multiple n channels. We assume that there is a watcher "Eve " who can read all the n channels and modify b out of n channels, where $b \leq (n-1)$.

To define our interactive security Model, we start by describing a ***Measured Matrix*** consisting of two matrices.

- ***Round Complexity:*** Which is the number of iterations that we should do to send p packets over n channels.
- ***Communication Complexity:*** Which is how many bits we transmit with respect to the size of the file that is intended to be transferred.

0.1.1 Security Properties

We define the security properties, ***completeness***, and ***unforgeability***.

- ***Completeness:*** Is the property which guarantees that Alice will receive the complete file that she is trying to exfiltrate from Bob's machine.
- ***Unforgeability:*** Is the property that ensures that it's not possible for the adversary to forge a packet and send it to Alice as if it were coming from Bob. In other words, ***Unforgeability*** guarantees that Bob will not be fooled by the adversary.
- ***Authenticity:*** Is the property which guarantees that Alice will receive messages from Bob only.

The watcher Eve changes the content of the communication channels with various objectives that include:

1. Deleting a packet so that Bob never receives it. Thus, preventing communication between Alice and Bob, censorship;
2. Inserting a new packet invented by Eve and send it to Alice wishing she will consider it authentic, forgeability;
3. Changing the order of packets sent through the channels.

0.1.2 Protocol Proposal

The proposed protocol is an innovative exfiltration technique that uses n covert channels to exfiltrate files from a controlled machine to a controlled server. The aim of this protocol is to guarantee that the attacker will receive complete and unforgeable data that he is trying to exfiltrate even in the presence of a Man In The Middle who's trying to modify or corrupt the data.