1) Introduction

Laptops, smartphones, tablets and many other types of consumer devices support wireless network connections. Wireless has understandably become the preferred form of computer for many people due to its portability and convenience. NFO devices always work wirelessly. Wireless network has made a big difference to the world as without it, the world would have been converted into a jungle of wires. NFC (Near Found Communication) is a sub area of Wire Less Network and includes technologies like Bluetooth and Infrared.

The increase of cheaper, smaller and more powerful mobile devices have made wireless Ad Hoc networks to become one of the fastest growing areas of research. This new type of self-deploying network may combine wireless communication with high degree node mobility. Unlike conventional wired networks they have no fixed infrastructure. This flexibility makes them attractive for many applications for a situation where either supporting structure is unavailable or deployment is unfeasible such as military networks and disaster recovery operations. The adhoc self-organization also makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time consuming high-cost task. Security is an indispensable need for both wired and wireless network communications. Unlike wired networks, wireless networks pose a number of challenges to security solutions due to their unpredictable topology; wireless shared medium, heterogeneous resources and stringent resource constraints etc. There are a wide variety of attacks that target the weakness of this kind of network. In this type of network, security is not a single layer issue but a multilayered one. I have focused on pairing where the possible attacks are most vulnerable.

Pairing takes place for Bluetooth and NFO (near found objects eg RFID tag). First Bluetooth V2.1 proposed Secure Simple pairing & it is continued till now. It is used with most interesting Technology, RFID today. Recently MCI (Medical council of India) has decided to implement RFID card for professors working in the medical colleges.
Red Cross in Ahmadabad uses RFID for its patients to know their medical history. RFID also uses pairing.

The different combinations of connectability and discoverability capabilities can be divided into three categories, or security levels:

1) Silent: The device will never accept any connections. It simply monitors NFO Traffic.

2) Private: The device cannot be discovered, i.e. it is a so-called non-discoverable device. Connections will be accepted only if the BD ADDR (Bluetooth Device Address) of the device is known to the prospective master. A 48-bit BD ADDR is unique and refers globally to only one individual Bluetooth device.

3) Public: The device can be both discovered and connected to. It is therefore called a discoverable device.

### TABLE I
DEVICE CAPABILITIES AND SIMPLE PAIRING ASSOCIATION MODELS

<table>
<thead>
<tr>
<th>Device 1</th>
<th>Device 2</th>
<th>Association Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayYesNo</td>
<td>Display Yes No</td>
<td>Numeric comparison</td>
</tr>
<tr>
<td>Display Only</td>
<td>Display Only</td>
<td>Numeric comparison</td>
</tr>
<tr>
<td>Keyboard Only</td>
<td>Keyboard Only</td>
<td>Passkey Entry</td>
</tr>
<tr>
<td>NoInput NoOutput</td>
<td>NoInput NoOutput</td>
<td>just works</td>
</tr>
<tr>
<td>Display Only</td>
<td>Display Only</td>
<td>Numeric comparison</td>
</tr>
<tr>
<td>Keyboard Only</td>
<td>Keyboard Only</td>
<td>Passkey Entry</td>
</tr>
<tr>
<td>NoInput NoOutput</td>
<td>NoInput NoOutput</td>
<td>just works</td>
</tr>
<tr>
<td>Keyboard Only</td>
<td>Keyboard Only</td>
<td>Passkey Entry</td>
</tr>
<tr>
<td>NoInput NoOutput</td>
<td>NoInput NoOutput</td>
<td>just works</td>
</tr>
</tbody>
</table>

1.1) What is simple secure pairing?

Secure Simple Pairing SSP uses a much more elaborate mechanism, known as elliptic curve cryptography, that avoids the use of a PIN code as part of the Link Key
calculation process (PIN codes or other user numbers can still be used as part of the authentication process though), but rather use extremely large random number for seeding Link Key calculation. The number of possible Link Keys is thus no longer limited to less than $2^{128}$ possibilities, which is far beyond any realistic attacker capabilities. In order to realize this, the SSP process starts by establishing a different kind of shared secret in between the two devices. This shared secret is known as the Diffie-Hellman key (DHKey) and is a 192-bit random number.

As a prerequisite, both devices have each a private key and a public key. The public key is transmitted over-the-air and can be known by anyone, but the private key will never be disclosed. We will call these two keys the SSP Public / Private key pair, but these are also known as Diffie-Hellman Public / Private key pair (Diffie and Hellman being the two persons who developed the algorithm). The carefully chosen mathematical space and algorithms used for creating the SSP key pairs are such that:

- It is very hard (i.e. impossible using current state-of-the-art computers) to calculate the Private Key using the Public Key (but it is easy to calculate the Public Key based on the Private one)
- Given two SSP key pairs A and B, there exists a well-known function $F$ such that $F(\text{PublicA}, \text{PrivateB}) = F(\text{PublicB}, \text{PrivateA})$. The result of this function is the DHKey.

Figure 1.1: Public Key Exchange Details

When both device’s Controllers and Hosts support Secure Connections, the P-256 elliptic curve is used. When at least one device’s Controller or Host doesn’t Support Secure Connections, the P-192 elliptic curve is used.
Pka=public key of A
SKa=private key of A
Pkb=public key of A
SKb=private key of A
DHkey (A) = PKbSKa \text{ mod } 192

Only the very two devices owning A and B are able to calculate the same DHKey. This is the magic behind SSP: the two devices will be capable of pairing without the need to transmit any critical information over-the-air, and without the need to share this information by an out-of-band mechanism (such as typing it on a keyboard). The DHKey will be used as a seed for calculating the Link Key. The rest of the pairing process is similar to LMP pairing.

**SSP is considered simple for the following reasons:**

- In most cases, it does not require a user to generate a passkey.
- For use-cases not requiring MITM protection, user interaction can be eliminated.
- For numeric comparison, MITM protection can be achieved with a simple equality comparison by the user.
- Using OOB with NFC enables pairing when devices simply get close, rather than requiring a lengthy discovery process.