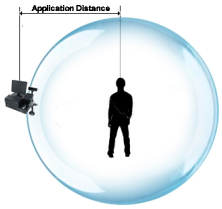

A relay attack is a type of attack related to man-in-the-middle and replay attacks, in which an attacker relays verbatim a message from the sender to a valid receiver of the message. The sender may or may not be aware of even sending the message to the attacker; if the sender is aware, it is likely under the impression that the attacker is the intended receiver of the message.

Encrypting the communication between the honest endpoints does not protect against such attacks.

For NFC technology, the main solution that has been off□ered to date is distance bounding, in which a tightly timed exchange of challenges and responses persuades the verfi□er that the prover cannot be further away than a certain distance. This solution, however, has some drawbacks:

- It still won't say whether the speci□fic endpoint the verifi□er is talking to is the intended one or not□. It will only tell the veri□fier whether the real prover is □nearby□.
- It involves hard real time processing to measure the transfer time and deduce the distance.

For BCC technology, the attacker may use his own body to connect two honest endpoints. By touching the eGo holder, the attacker may connect the holder's eGo with his own eGo compliant

device and so benefit from the credentials within the eGo without agreement. Time-based protocols to prevent fraud by evaluating the application distance between two honest devices are not possible when using the body as a communication medium.

How to prevent it?

If the application distance is short (less than 10 meters) then it can be evaluated by using the RTLS capability of the IEEE802.15.4a. The eGo and the eGo compliant devices can define the maximal application (**from 0.30 m to 50 m** **NLOS**) distance and reject the transaction if this application distance is exceeded.

The Intra-Body Communication signal can flow from the eGo holder to the attacker carrying an eGo compliant device. The eGo holder is not aware about the malicious eGo pairing, so to prevent it, the simplest way involves getting an Out-Of-Band agreement from the eGo holder.