Código Network Threat model and Security Assumptions

To be able to tackle the complex problems that arise in the design of decentralized applications, the categories of possible adversaries must be identified. This project has many commonalities with the OpenBazaar e-commerce platform [1]. Código network has a more narrow focus on peer-to-peer (P2P) distribution of firmware for embedded devices. The combination of the Código's narrow focus and the lack of monetary transactions makes it a much less vulnerable system. This comes from the fact that agents using the system, to receive firmware updates have no immediate financial incentives should they deviate from a proper execution of the protocol (This does not apply to OpenBazaar). Contrary, in the design of the network, the users need to protect themselves from malicious developers that want to infect embedded devices with malicious software.

A malicious developer is an agent in the network that will upload a "firmware" to the network knowing that the firmware is either not working or is exploitable in some way. The benefit of polluting the network with unusable software is to grief the users of the system and cause denial of service. Contrary polluting the network with exploitable firmware comes with many financial advantages as described in the introduction. A subtle observation is that in both cases the reward the malicious agent is either non-monetary or if it is monetary it comes from a source outside of the network. As a result, it is not possible to model the users of the system as rational and rely on a game-theoretic approach to protect the system against malicious developers. Another subtle observation, is that the adversary is a favorable position in decentralized environments. In the decentralized setting the attacker can generate multiple identities and use them collectively to attack the system. Additionally, the pseudo-anonymity that comes in every decentralized applications makes it harder for users to trust other agents of the network.

To protect Código Network for the aforementioned adversaries it assumed that the following hold true:

1. Cryptographic primitives such as Digital Signatures, RSA encryption, AES, SHA-256, SHA-3 are secure

2. The frameworks used (IPFS, Ethereum) are theoretically secured and implemented correctly

3. The libraries used to develop the network are secure (Namely: ...)

4. The embedded device used is secure.

[1] OpenBazaar is decentralized marketplace that uses cryptocurrencies.