NFC Security: Proposal

Andrey Tydnyuk

February 5, 2013

Abstract

The goal of my research is to establish a secure way to confirm location with NFC tags. If there was a way to do that, restaurants can have NFC tags that customers can scan to confirm that they have eaten at the restaurant. This can then be used to confirm that they have in fact been to the establishment when they review it on a service like Yelp. NFC tags can also be used in multiplayer games with a real-life component. For instance, if players get clues and have to travel to a certain location to scan a tag, the administrators want to have a way to confirm that the players actually physically visited the game site before they give a certain reward. Currently, this is impossible due to the fact that NFC tags have no security layer on top of them. If there is no security, and all the tags do is point you at a URL, one person can go grab the URL and then post it online for everyone to access. The purpose of this research is to develop a way to make sure that the only way for a person to acccess some data is to make physical contact with an NFC tag that points them to it.

1 Minimum Viable Product

My goal is to come up with several ideas for secure location check-in via NFC tags and implement one of them. At the very least I hope to get one of these ideas fully implemented and working. This will most likely require writing an application, a small webapp and code for the tag to transmit to the phone.

I am not sure which idea I will implement yet, but if I try to make sure that the tag does not have to do any computation, I will have to redirect the phone to a web application that will do the crypto stuff and write a confirmation to the application that registers and confirms the fact that the phone was in fact at the specified location.

Along with an implementation I also plan to include an analysis section detailing the different attacks that this application prevents and the attacks that it is vulnerable to. I will state the assumptions that I am making in regard to the security and the guarantees that I make with the cryptography portion of the transaction.

2 Schedule

I plan to structure this project around three main checkpoints. These checkpoints will be the first of every month, up to and including May.

For the first checkpoint I am hoping to come up with several implemetation ideas. These ideas will be fairly detailed and will pretty much be similar to design documents. I will have a plan on how to implement each one and the different guarantees that each idea will provide. Each of these ideas will also have a list of features that I will have to implement in order to make a working demo out of it.

For the second checkpoint, the target is to have one of the ideas that I came up with in the last checkpoint finished and working. I think that this is a good target goal. If the idea I pick turns out to be easy, I will start working on a harder one, and if it turns out to be difficult I hope to have at least 70% of it done by the second checkpoint.

For the last checkpoint, I will have hopefully fleshed out one or two ideas into full working applications and will have written up analysis documents for each detalining their workings and the security behind them. By this time I hope to have finished a working demo for the project and a paper that goes over all of the finer details. This might include a comparison between my implementation and other ideas that I did not choose and will contain suggestions for further improvements.