Angel Hernandez

11/04/2014

Comp 595MC/L

NFC Data Transfer Through a Secure Channel

**Summary:**

Using NFC technology a user will be able to customize and submit data through a secure channel so that a receiver device can display this information.

Outline of actions:

1. User logs into application via pin authorization, in order to change sensitive data.
2. The user then taps their device to the receiving device, causing a peer generated token to be generated as well as encrypts the data.
3. The receiving device then receives and decrypts the information after verifying token.
4. In order to showcase a general use for NFC data transfer, the receiving device will also pull information from a MYSQL server to show the following:
   1. Mock crime history to show the use for policemen
   2. Workplace ID timestamps to show the use for corporation.
   3. Passport information identification.

(All MySQL data will be in the form of simple data tables)

**Demo:**

The demo will consist of two devices, one to send the other to receive. There will be four items to display for the demo.

Part one will show the receiver displaying information that the user has entered in the sending device. This will be demoed in the style of a personal passport with information such as name, eye color, height, etc.

Part two will also utilize the MySQL server and lookup information regarding the user, this is where the Mock Crime report will be shown.

Part three will consist of the receiving device using the MySQL server but it will not only receive data, but send data as well. This is to gather information for a corporation setting, items like timestamps for when a worker clocks in or out, as well as data surrounding his corporate identification (ID number, job description, security clearance, etc.).

Fourth and lastly I will be showing how secure the device is by viewing the pin lock mechanism as well as the inner working of token data transfer and encryption.

**Testing:**

Testing will done within three phases: connectivity dependence, simplicity, and security.

With connectivity dependence testing will continuously be done with importance to device network connection. The device will be set into NFC only and Wi-Fi only modes. This is done in order to secure a working connection as well make sure there are no problems when it comes to sending and receiving data from a server.

Simplicity is key when it comes to usage, in order to make sure that anyone can use this application I will be giving out test builds to a selected few without giving instructions other than what the application does. This should benefit the application by further developing the UI from the help of feedback from testers. My goal is to create a nice and intuitive display such as the one shown by the Martijn Oostdijk from EIT ICT Labs, their layout has a simple and elegant design for displaying data in the form of a digital passport. Unfortunately their project dwindled last year, but the idea is there and I hope to build upon what they had in mind.

Lastly is security, after reading “Touch and Run with Near Field Communication”, a research paper about the uses of NFC from Stanford university, the main issue with NFC is its prone to 3rd party attacks it would be difficult to find a way to test for items such as a Man-in-the-Middle attack. But it is possible to test if our security system actually works. For this I will create a separate receiver application that reads NFC data only and make sure my sender application both recognizes and rejects the application.

Security testing checkpoints:

* + The generated token system from the description should cause an error to the unauthorized receiving application.
  + The encryption of the data should be unreadable to the unauthorized application.
  + The application should be aware that the receiver is unauthorized.

Necessary software and hardware:

Java, Eclipse, MySQL.

Two android NFC capable devices, MySQL server.

* Two android devices are already owned, and the server can be hosted remotely from my home computer.

References:

Dodson, Ben, Hristo Bojinov, and Monica S. Lam. "Touch and Run with Near Field Communication (NFC)Ben." Stanford University, 2010. Touch and Run with Near Field Communication (NFC) (2010): 1-6. Print.

OOSTDIJK, MARTIJN. "Security, Something, Something..." Security, Something, Something... N.p., 16 June 2013. Web. 06 Nov. 2014. <http://martijno.blogspot.com/>.