Môn học: Mã Hóa Thông Tin

Tên đề tài: Tìm Hiểu NFC và Vấn Đề Bảo Mật

Giáo viên:

Học viên: Bùi Huỳnh Thúy Mai

Lớp:

Tìm Hiểu NFC và Vấn Đề Bảo Mật Dữ Liệu

1. Giới Thiệu

Trong những năm gần đây thị trường thanh toán di động đang được triển khai ở Việt nam ngày càng nhiều do một số nguyên nhân đặc thù là dân số Việt nam khá trẻ, sử dụng điện thoại thông minh và sẳn sàng sử dụng công nghệ mới. Vì thế, ngày 29/09/2017, dịch vụ Samsung Pay đã được triển khai ở Việt nam, cụ thể là tại nhiều cửa hàng như Highlands coffee, Gongcha, nhà hàng Golden gate chấp nhận thanh toán bằng Samsung Pay cũng như nhiều ngân hàng như Viettin, BIDV chấp nhận thanh toán qua Samsung Pay. Hay gần đây ngân hàng Tiền phong giới thiệu chương trình thẻ Visa contactless.

Bên cạnh thanh toán di động trong ngân hàng, người ta còn dùng “contactless ticket” trong khi sử dụng phương tiện công cộng. Cụ thể là Singapore đã thử nghiệm hệ thống dùng contactless Master card để thanh toán tiền mua vé và sử dụng như contactless ticket trong hệ thống tàu điện MRT. Với công nghệ này, Singapore đang muốn áp dụng rộng rãi trong giải pháp thành phố thông minh. Việt nam có thể xem xét giải pháp này trong khi triển khai hệ thống tàu điện do lợi thế về dân số trẻ sử dụng nhiều smartphone.

Những ví dụ trên đặt vấn đề cho việc tìm hiểu về công nghệ giao tiếp tầm ngắn (near field communication – NFC) và an toàn dữ liệu cho giao.

1. Tìm hiểu Công Nghệ NFC (Near Field Communication)
2. Công nghệ NFC là gì?

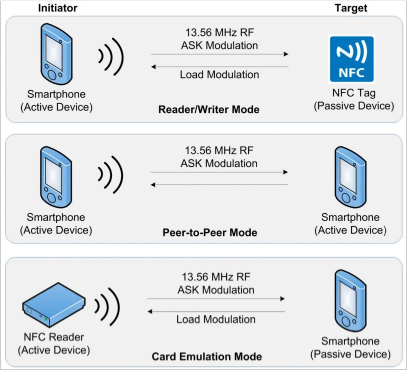
NFC là chuẩn giao tiếp (kết nối) không dây tầm tầm ngắn, không cần có kết nối internet (Wifi, 3G, LTE). NFC sử dụng sóng vô tuyến hoạt động ở băng tần 13.56Mhz, tốc độ truyền dữ liệu từ 106 Kb/s – 424 Kb/s trong phạm vi tối đa 4 cm cho phép 2 thiết bị hỗ trợ giao thức NFC có thể truyền và nhận dữ liệu cho nhau.

Các loại thiết bị được sử dụng

- Thiết bị mang tính chủ động

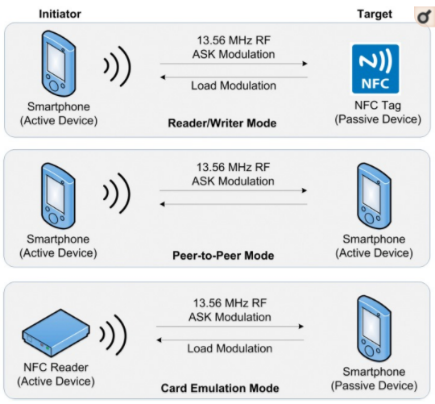
- Thiết bị mang tính bị động

1. Các phương thức giao tiếp trong NFC



1. Bảo Mật Thông Tin Trong NFC

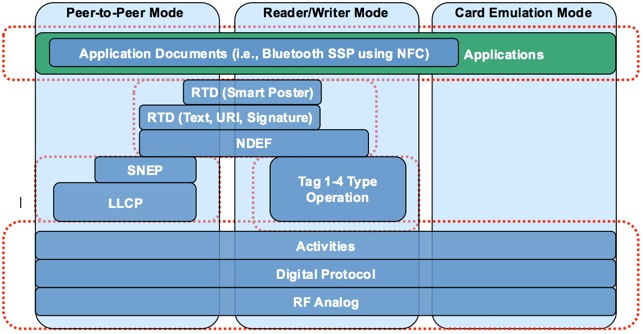
Near Field Communication (NFC) được gọi là giao thức giao tiếp không dây tầm ngắn. NFC là giao thức cho phép hai thiết bị giao tiếp với nhau, hoạt động ở băng tần 13.56 Mhz, tốc độ truyền dữ liệu từ 106 kb/s đến 424 kb/s trong khoảng cách từ 2 – 4cm. NFC hỗ trợ ba phương thức giao tiếp và mỗi phương thức giao tiếp có những yêu cầu về thiết kế, hoạt động khác nhau. Phương thức giao tiếp là thiết bị đọc hoặc thiết bị ghi (Reader/Writer) theo ISO/IEC 14443 & JIS X 6319-4/Felica, thiết bị có hỗ trợ NFC có khả năng đọc dữ liệu lưu trong thẻ NFC hoặc thiết bị hỗ trợ NFC theo đúng định dạng hoặc có thể ghi dữ liệu đến thẻ tệp. Loại thứ hai là giao tiếp ngang hàng theo ISO/IEC 18092 NFCIP-1 & ISO/IEC 21481 NFCIP-2, hai thiết bị được kết nối 2 chiều, có thể trao đổi dữ liệu với nhau . Loại cuối cùng giao tiếp mô phỏng thẻ theo EMVCo ISO/IEC 14443 & JIS X 6319-4/Felica, thiết bị hỗ trợ NFC là passive mode cho phép đầu đọc đọc dữ liệu được dùng trong kiểm soát vé, mở cửa.

 Những loại thiết bị được dùng trong NFC là điện thoại thông minh có hỗ trợ NFC, thẻ NFC và đầu đọc NFC. Thiết bị nào giao tiếp đầu tiên gọi là Initiator trong khi thiết bị nhận giao tiếp gọi là Target. Active device là thiết bị có sẵn nguồn năng lượng để giao tiếp và truyền dữ liệu. Passive device là thiết bị sử dụng nguồn năng lượng bên ngoài cho phép đầu đọc đọc dữ liệu.

[1] Các giao thức trao đổi dữ liệu

1. An toàn dữ liệu cho thẻ tệp NFC

Thẻ tệp NFC là passive mode được dùng để lưu trữ dữ lượng dữ liệu nhỏ trong ứng dụng và truyền dữ liệu đến điện thoại thông minh có hỗ trợ NFC hay đầu đọc thẻ đọc dữ liệu. Theo như mô hình định nghĩa giao thức NFC [2], trên mỗi tầng không có kỹ thuật mã hóa thông tin để bảo vệ dữ liệu nên thẻ tệp NFC dễ dàng bị tấn công từ bên ngoài.



[2] Định dạng giao thức theo tổ chức NFC Forum

[*diễn giải mô hình để thấy rằng không có bất kỳ biện pháp an toàn thông tin*]

Một số kỹ thuật có thể làm thẻ NFC bị tấn công như nghe lén, thay đổi dữ liệu bên trong tệp bởi một mã độc khác, phá hoại dữ liệu gây tình trạng từ chối dịch vụ hay đặt tác nhân trung gian can thiệp vào trong quá trình trao đổi dữ liệu làm thay đổi

1. An toàn dữ liệu cho đầu đọc NFC
2. An toàn dữ liệu trong quá trình giao tiếp NFC
3. Kết Luận
4. Tài Liệu Tham Khảo

[1] <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4507650/>

[2] <https://nfc-forum.org/>

[3]