IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 4, April 2017

Novel Approach to access Notices/Assignments using NFC Technology

Prof Neha S Pharande[1], Vaishnavi Bulbule[2], Madhura Deshmukh[3], Saloni Jain[4]

Assistant Professor, Department of Computer Engineering, Sinhgad College of Engineering, Pune, India [1]

Student, Department of Computer Engineering, Sinhgad College of Engineering, Pune, India [2,3,4]

Abstract: Smart posters are a promising new use case for NFC-enabled mobile devices. A secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. This project enforces and integrity of smart poster data as well as authentication/authorization of administrators and end-users, thus ensuring that only authorized users can access the content. This project is useful for secure sharing of college assignments. First the NFC Smart Poster is designed by admin. NFC tag contains information; the tag can be embedded into the object. For example, the poster is created for first year student and it contains information about assignment. The object can be placed to notice board. When the first year student touch his android mobile phone to tag, it will connect to server. After that authentication server will check the details of student and also check whether the student is first year student. If yes, then it will share that assignment information with student. We present S-SPAN - a secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. S-SPAN enforces confidentiality and integrity of smart poster data as well as authentication/authorization of administrators and end-users, thus ensuring that only authorized users can access the content.

Keywords: Near field communication, secured smart poster authentication using NFC.

I. INTRODUCTION

To accomplish above AIM, we will be using NFC (Near Field Communication) technology. The user will be using his/her mobile phone to see the information available in a poster. In NFC, the communication occurs when two NFC compatible devices are brought together less than four centimetres, or simply by touching themselves. It operates at 13.56 MHz and can transfer data up to 424 Kbits per second. In an NFC model two devices are involved in the communication, which are called initiator and target. Initiator is an active NFC device which is responsible for starting the communication. Also it has an embedded energy component whereas target can be either a tag, RFID card or an NFC device which responses the initiator’s requests. These are intermediate level. “Network and communications” deals with new protocols, data and communication aspects. Tags, Antennae, Readers and NFC Chip” deals with the hardware aspects. “Security and Privacy” deals with CIA principles, Non Repudiation and other possible vulnerabilities. We present S-SPAN - a secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. This document will be helpful to the developer to implement and testers to do testing of this project. Also it will helpful to other who wanted to do any changes in this system.

II. RELATED WORK

Smart posters, which allow businesses or other organizations to disseminate information to end-users in a more interactive fashion than standard posters, are an increasingly popular application of NFC tags. Such tags store small amounts of read-only (or less commonly, rewriteable) data. A typical use case for NFC smart posters is to provide users of NFC-enabled smartphones with quick access to a URL related to the poster content. Smart posters are a promising new use case for NFC-enabled mobile devices, but to date there has been a general lack of security mechanisms for NFC smart posters.

2.1 Enhancement and security in the system

The confidentiality and integrity of smart poster data as well as authentication/authorization of administrators and end-users is not checked. NFC tags are vulnerable to spoofing as well as cloning, and the RF channel, like any wireless channel, is susceptible to data modification or man-in the-middle attacks. Furthermore, the NFC protocol as currently defined has some weaknesses, e.g. the standardized NFC Data Exchange Format (NDEF) does not guarantee integrity

DOI10.17148/IJARCCE.2017.6479

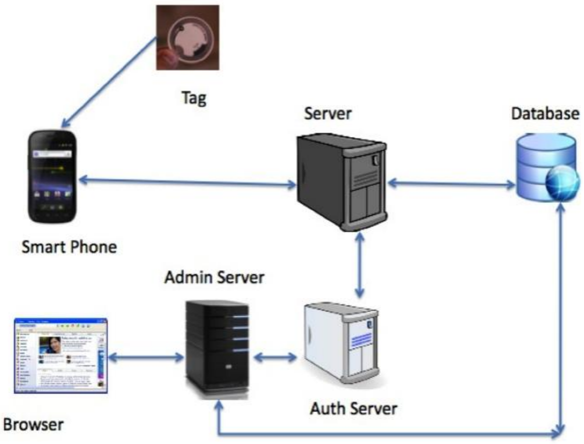
and authenticity, even in the presence of a digital signature. There are also situations that call for smart posters to contain sensitive information only privy to specific users. For example, a museum may wish to use NFC smart posters in tandem with a custom smartphone application, to provide additional information about exhibits on the condition that the content should only be available to users who have paid for admission on a given day.

2.2 Motivation

The main goal of S-SPAN is to secure smart posters against attacks on tags, end-user devices, the RF communication channel, as well as the NFC protocol, thus ensuring confidentiality and integrity of poster data as well as authentication of poster administrators and end-users. We present S-SPAN - a secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. S-SPAN enforces confidentiality and integrity of smart poster data as well as authentication/authorization of administrators and end-users, thus ensuring that only authorized users can access the content.

III.PROPOSED SYSTEM

The main goal of S-SPAN is to secure smart posters against attacks on tags, end-user devices the communication channel, as well as the NFC protocol,



Thus, ensuring confidentiality and integrity of poster data as well as authentication of poster administrators and end-users.

We present S-SPAN - a secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. S-SPAN enforces confidentiality and integrity of smart poster as well as authentication/authorization of administrators and end-users, thus ensuring that only authorized users can access the content.

3.1 Backend Server

The backend for the smart poster application consists of two major components, namely a web interface for administrators as well as an API for the mobile application. Only specific authorized users are allowed to access the administrative web interface.

3.2 Mobile Application

Our API provides the mobile app with read-only access to the database of tag IDs. For security reasons, all API requests must be made via HTTPS

3.3 Authentication Server

All pages and scripts on our backend server are protected, so the Smart Poster app must check the user’s authentication status on each request to the server

Users and Characteristics

The user of this system will be any android mobile phone user who wants to access or get the information from the poster.

DOI10.17148/IJARCCE.2017.6479

3.4 Operating Environment

Software has two major component one the server and the second one is the mobile application. The server will required Windows XP/Vista/7 machine with minimum 1GB RAM and 100 GB hard disk. Android 2.3 enable handset is required for mobile application with NFC.

IV. ALGORITHM

Secured Smart Poster Authentication Algorithm

This algorithm emphasizes on security of the smart posters used in universities or institutes.

1) The NFC tag is stuck in the universities or institutes where it is easily accessible by students or staff members.
2) Users will tap their NFC enabled mobile devices which have the app to get the notices and assignments on the NFC tag.
3) Magnetic induction is generated in the NFC tag because of mobile devices' battery power and the NFC tag gets generated.
4) There is a private key in each NFC tag which is detected by the mobile devices' NFC reader and the data which is available in the database server is acquired on the mobile app directly.
5) The private key is encrypted and there is a secured HTTP communication that takes place between the tag and the server through Advanced Encryption Security Algorithm.
6) If the user is authentic only then will he be able to get the contents of the database. For this, the users need to already register themselves to the administrator of the server.
7) The data of database in the server side uses hashing techniques to secure the user's id and password. Also the user's data is secured by using SHA technique.
8) Whenever a user is registered, he will get a message on his mobile device with the id and password which will be only known to the user not even to the administrator as it will be in the hashed format.

V. CONCLUSION

From the consideration of all the above points we conclude that, S-SPAN is very beneficial for fast access of data. It can be used in universities by the students to access assignments and notices. Thus, approach to eliminating tag spoofing and cloning is to store no information other than a string of random bytes in the tag. This is different from the conventional approach of storing the complete resource in the tag itself. Thus, if an attacker attempts to clone our tag, all he gets is a bunch of random numbers, from which no information can be gleaned about the resource. These random numbers function as the tag ID, and an authenticated user queries the database using an HTTPS connection, thereby thwarting any possibility of eavesdropping. The administrator, a trusted member whose responsibility is to register the tags, has access to audit logs of the posters and can revoke any poster, if malicious activity is suspected.

ACKNOWLEDGMENT

We are profoundly grateful to **Prof. N. S. Pharande** for her expert guidance and continuous encouragement throughout to see that this project rights its tar-get since its commencement to its completion. We would like to express deepest appreciation towards **Dr. S. D. Lokhande**, Principal, Sinhgad College of Engineering, **Prof. M. P. Wankhede**, Head of Department, Computer Engineering whose invaluable guidance sup-ported us in completing this project. At last we must express our sincere heartfelt gratitude to all the staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

REFERENCES

[1] Briand, L. C., Daly, J., and Wüst, J., "A unified fram S-SPAN: Secure Smart Posters in Android using NFC, IEEE 2013 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6263736
[2] [2] [1] Briand, L. C., Daly, J., and Wüst, J., "A unified fram S-SPAN: Secure Smart Posters in Android using NFC, IEEE 2013 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6263736
[3] M. M. A. Allah, "Strengths and weaknesses of near field communication nfc technology," Global Journal of Computer Science and Technology, vol. 11, no. 3, Mar. 2011.
[4] M. Roland, J. Langer, and J. Scharinger, "Security vulnerabilities of the ndef signature record type," 2011 Third International Workshop on Near Field Communication (NFC), pp. 65–70, Feb. 2011
[5] http://www.ijser.org/researchpaper5CLiterature-Survey-On-NFC-applications-and-controller.pdf
[6] http://www.im.ethz.ch/publications/Switching the role of NFC tag and reader for the implementation of Smart Posters.pdf
[7] https://software.intel.com/en-us/android/articles/nfc-application-development-on-android
[8] Sufian Hameed, Bilal Hameed, Syed Atyab Hussain, Waqas Khalid" Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters"2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications

DOI10.17148/IJARCCE.2017.6479