iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40282

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

NFC Based Login for Mobile Apps and Websites

Amrit Prasad, Nandita Bangera[2], Utkarsh Shekhar[3]
India

Abstract: ***This paper is concerned to show how a mobile phone equipped with Near Field Communication (NFC) can be used to construct a Single Sign-On authentication system (Celikkan & Gelis, 2014, August). When logging in to numerous online sites, customers no longer have to juggle a plethora of usernames and passwords to keep track of. As omnipresent computing devices, smartphones are utilised for a wide range of functions, from authentication to tracking to medical care to entertainment and e-payment. Among NFC's many advantages is that it uses short-range communication, which enhances security while also making it simple to use. Our Chrome browser extension allows users to easily authenticate and manage their personal information from their mobile devices. Owing to browser security restrictions, JavaScript code (used in the Google Chrome extension) cannot access computer system resources when executing in a browser. As a result, the Java applet is used to run the software on the user's computer. With the help of the extension, NFC Reader may be accessed and used, and a connection between Java and JavaScript can be established. Using NFC, the user does not have to input any account information because it is automatically uploaded to the online login page.***

IndexTerms: NFC, Login, Mobile apps , website, RFID , Authentication, Sign-in

I. INTRODUCTION

As the internet grows, keeping track of diverse users authentication credentials becomes increasingly challenging. The most popular means of establishing a user's identity is to enter their login and password. In an attempt to prevent the problem, there are some hazards involved with utilising one login and password for practically all of your online accounts (Gaw & Felten, 2006, July). It's possible that you won't be able to use the same login on all of your accounts. To maintain passwords for many accounts in sync, one must update them all at the same time, which takes time and effort. Using different account usernames and passwords, on the other hand, solves the problem of remembering a large number of account usernames and passwords. Because of the added complexity, passwords with special letters, numerals, and other characters are more difficult to remember. To overcome this problem, several alternatives based on the concept of single sign-on have been proposed (SSO). Browsers now include a password vault to help users remember and auto-fill passwords. However, because the security of the passwords is dependent on the system, it was not a secure solution. To safeguard information from being read in plain text, password managers can save encrypted data in the cloud. The fact that you lose control of your data is a downside of this strategy. You give up the security of your data because it is vulnerable to being processed.

II. PEELING THE APPLET

This layer serves as a link between mobile devices and desktop computers. To check if a phone is nearby, it uses an NFC reader to send a request (Çavdar & Tomur, 2015, May). If a phone is found, data is then transferred to the browser using NFC technology. NDEF data is transmitted between both the mobile device as well as the applet via the Simplified NDEF Exchange Protocol (SNE) provided by this layer. JavaScript Object Notation-formatted account information is contained in the NDEF message payload. Machines and people can both readily scan and comprehend JSON, which is a compact data transfer format.

A. The Browser Layer

JavaScript and HTML are used to write the code that runs on the browser. For every page with a login form, the appropriate JavaScript code and HTML applet tag code are inserted into the website. When the applet sends its JSON-formatted data, the browser layer parses it to extract username and password and then submits the page after using the auto-filled account information.

B. Implementation

Illustrates the two primary components of NFC-SSO implementation. The host part is developed as just a Chrome browser plugin using JavaScript, HTML, and CSS and contains a Java applet for the Android operating system. Contactless communication between both the NFC-enabled phone and the host is provided by an NFC reader. The NFC Reader is the ACR122U NFC contactless Card Reader (ACR122U). Android 4.1.2 and the Chrome web browser on Windows 10 are used to test the implementation.

III. RELATED WORK

Mobile phone manufacturers, operating system suppliers, mobile phone operators, & financial institutions all work together to implement NFC mobile payments (Alliance, 2007). NFC-enabled devices use SEs to safely store private information used for mobile cashless payments. In the future, people could pay using their smartphones instead of credit cards, thanks to NFC-enabled credit cards. Contactless PoS readers get account information from mobile devices through an RF link when a user holds or taps his or her phone near a reader.

Paying with a mobile payment app is no different from paying with a credit card or checking a bank account. TLS (Transport Layer Security) protects all payment apps against network attackers, according to the authors of (TLS). According to the authors, an Elliptic Curve-based signature might be used to sign and authenticate NFC transferred messages while also protecting them from other assaults, such as manipulation (Díaz García et al., 2020). In order to execute a mobile payment app safely, the authors propose an integrated TLS stack in the SE.

Certificate-based authentication can be used to send signed communications to clients, as described in this article. Short-lived X.509 certificates just on the client side are introduced to reduce the costs associated with certificate validation, transmission, and computation.

As previously indicated, the SE and PoS are both authenticated via certificate-based authentication. Certificates, on the other hand, place unwelcome restrictions on SE installed in mobile devices, which frequently have limited memory and battery life. NFC's deployment and performance will be impacted by a number of factors, including the time it takes to complete public-key cryptographic procedures. Certificates in wireless networks: further discussion can be found in.

IV. VULNERABILITIES AND ATTACKS ON NFC DEVICES

Even while NFC technology can be used for a wide range of applications, the lack of communication security primitives in the lower layers of NFC renders this technology vulnerable to a wide range of attacks and weaknesses. In this work, we assume that both the consumer as well as the devices are trustworthy, and we only discuss the security issues that may arise while conducting transactions via the NFC radio link.

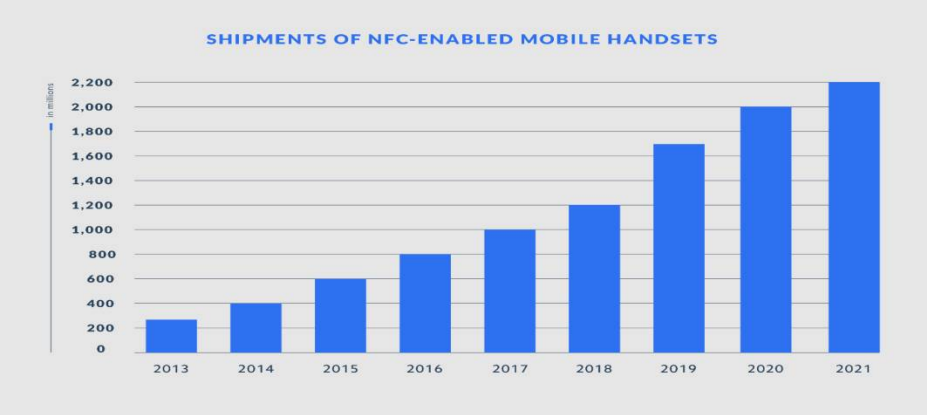
The NFC can be attacked from a variety of different angles (Pasquet et al., 2008, May). It primarily involves the use of malicious apps that have been installed on NFC-enabled gadgets instead of legitimate ones, including malware applications that use shared hardware components, such as smart cards, as side channels to extract or overwrite sensitive information stored on the cards. The authors also talk about malicious operating systems that allow an attacker to gain root access to a device and afterwards exploit vulnerabilities.

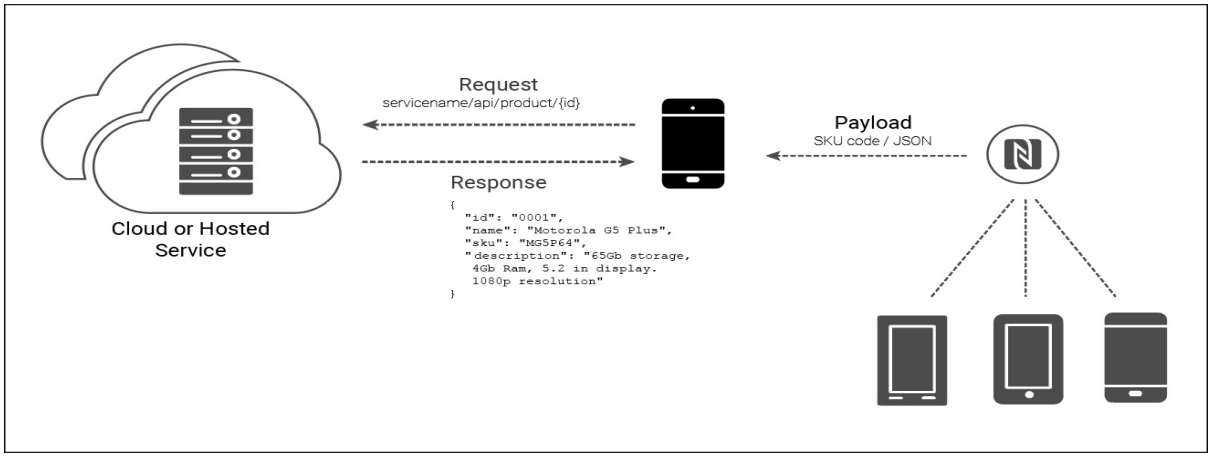
The aforementioned difficulties can be alleviated by using existing solutions. In the same manner that rogue URLs and Internet browsers can provide a problem, NFC tags could also be a threat. It's possible to hijack NFC tags and replace them with harmful content, such as redirecting users to an attacker's website or making phone calls or sending SMS messages, without requiring user authorization.

V. PROPOSAL FOR SECURITY

In order to protect critical payment apps and user account data, cryptography should be the primary mechanism. NFC-enabled mobile devices replicate credit cards and store the user's data in a Secure Element in the mobile payment ecosystem, which is a replacement for the physical credit card (Ondrus, 2015, August). The secure element may store and run several contactless applications, as well as third-party data management.

It is possible to create a connection between a mobile device and an OTA server using a TLS extension, in which the mobile device acts as an intermediary. In the subsequent subsections, we discuss our proposed approach for preventing attacks on the NFC interface. In our system, we leverage certificate-based authentication between the PoS and a trusted third party (TTP) and shared secret authentication between the TTP and the NFC-enabled device. Since the TTP and mobile share a secret key, we'll assume that the cryptographic computations are done in SE. Assumedly, SE offers strong tamper resistance because of the implementation of various physical equipment/software protections, which make it impossible to extract and modify private or secret data in SE. To begin with, we'll assume that the PoS and/or the mobile device are both online. To make a mobile payment, users must connect to a PoS that has an Internet connection. A PoS with Internet access and one without an Internet connection are both examples of how our proposed approach could work.





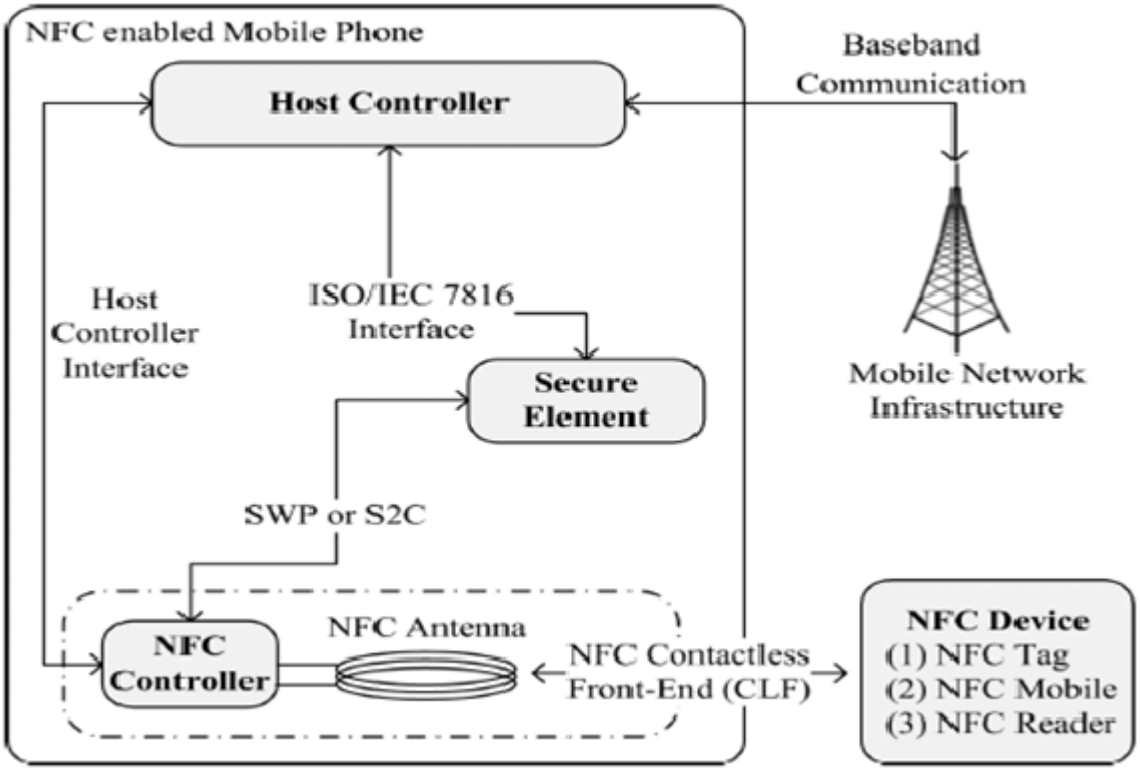


Table
Configurations for NFC communications.

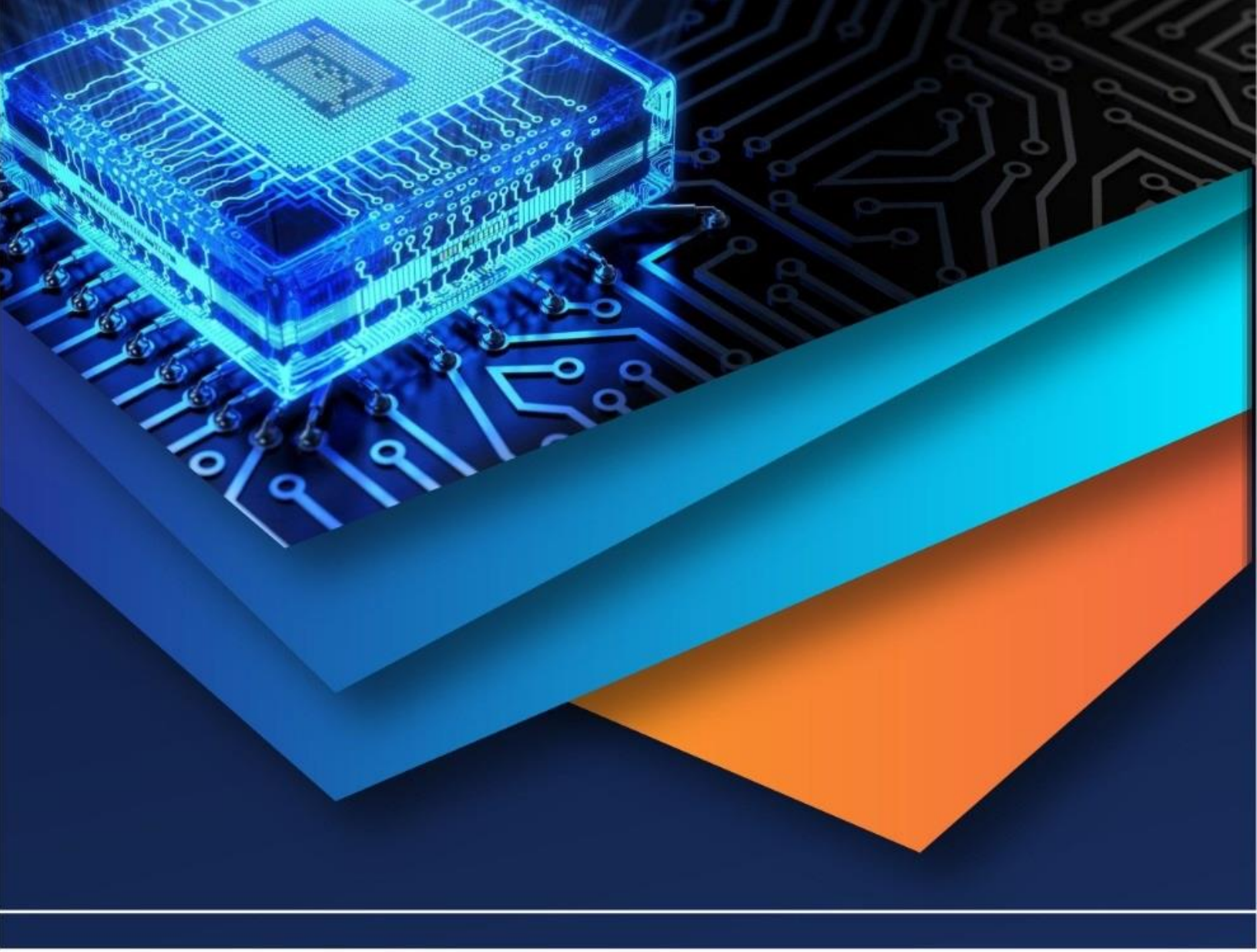
Device A	Device B	Description
Active	Active	Assuming that the NFC peer-to-peer solution is described as the data transmitting module producing an RF field and the data receiving device operates as a passive device. When one device delivers data, the other device is passive, and vice versa.
passive	Active	Device A generates an RF field and therefore is active, while Device B is passive.
Active	Passive	The device Is a working device, whilst Device B is a stand-by one.

VI. CONCLUSION

Many people are concerned about the security of NFC-enabled mobile payment systems' users' data (Akinyokun & Teague, 2017, August). NFC specifications don't specify any communication security primitives, which makes the technology vulnerable to a broad range of vulnerabilities & threats. NFC transactions are more secure and private thanks to a new security solution introduced in this context. We show that our technique saves time and money by minimising the amount of communication and processing required. We believe that our proposed design is appropriate for resource-constrained devices, such as the Security Elements integrated into NFC-enabled smartphones. Pre-shared secrets are being used to integrate our approach into the TLS protocol. In addition to providing entertainment, mobile phones can also be used to make payments. Because of the difficulty of keeping track of so many different login credentials, we've developed an SSO solution for mobile phones that works with Chrome as just a browser extension. Trying to log in to various websites with different usernames and passwords is inconvenient, and it might even pose a security risk. This study's solution comprises an Android app and a Chrome extension for the web browser. In the paper, a solution is provided that is successful versus key loggers because authentication data is auto-filled without the user having to type any information in. To combat phishing attacks, the URL of the mimicked or take a glance website will not equal the one that is kept on a user's mobile device. Man-in-the-browser attacks are not covered by this approach. Several mitigation elements, the first of which is knowledge, must be used to address man-in-the-browser attacks in a broader context.

REFERENCES

[1] Celikkan, U., & Gelis, C. (2014, August). NFC based mobile single sign-on solution as a chrome extension. In 2014 11th International Conference on Security and Cryptography (SECRYPT) (pp. 1-7). IEEE.
[2] Gaw, S., & Felten, E. W. (2006, July). Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and security (pp. 44-55).
[3] Çavdar, D., & Tomur, E. (2015, May). A practical NFC relay attack on mobile devices using card emulation mode. In 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1308-1312). IEEE.
[4] Alliance, S. C. (2007). Proximity mobile payments: Leveraging NFC and the contactless financial payments infrastructure. Smart Card Alliance.
[5] Díaz García, A. F., Blokhin, I., Anguita López, M., Ortega Lopera, J., & Escobar Pérez, J. J. (2020). Multiprotocol Authentication Device for HPC and Cloud Environments Based on Elliptic Curve Cryptography.
[6] Pasquet, M., Reynaud, J., & Rosenberger, C. (2008, May). Secure payment with NFC mobile phone in the SmartTouch project. In 2008 International Symposium on Collaborative Technologies and Systems (pp. 121-126). IEEE.
[7] Ondrus, J. (2015, August). Clashing over the NFC secure element for platform leadership in the mobile payment ecosystem. In Proceedings of the 17th International Conference on Electronic Commerce 2015 (pp. 1-6).
[8] Akinyokun, N., & Teague, V. (2017, August). Security and privacy implications of NFC-enabled contactless payment systems. In Proceedings of the 12th International Conference on Availability, Reliability and Security (pp. 1-10).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY