Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 1, Pages 345-353, 2018

SEAP Protocol for NFC Technology for Risk Free Penniless (OFF HAND) Remittance

Mrs.D.Sabarmathi[1], S.Naveena[2], N.Priya[3], R. Raj Prathisha[4], M.Saranya[5]

[1]*Assistant Professor, Department of Electronics and Communication Engineering, Sasurie Academy of Engineering, Coimbatore, India.*
[2,3,4,5]*Department of Electronics and Communication Engineering, Sasurie Academy of Engineering, Coimbatore, India.*

Article Received: 27 November 2017 *Article Accepted: 24 January 2018* *Article Published: 30 March 2018*

ABSTRACT

Authentication protocol plays an important role in the short-range wireless communications for the Near Field Communication (NFC) technology. Due to the shared nature of wireless communication networks, there are several kinds of security vulnerabilities. Recently, a pseudonym-based NFC protocol (PBNFCP) has been proposed to withstand the security pitfalls found in the existing conditional privacy preserving security protocol (CPPNFC). However, this paper further analyzes PBNFCP and shows that it still fails to prevent the claimed security properties, such as impersonation attacks against an adversary, who is a malicious registered user having a valid pseudonym and corresponding private key. In order to overcome these security drawbacks, this paper proposes a secure and efficient authentication protocol (SEAP) for NFC Applications using lifetime-based pseudonyms. The proposed SEAP is simulated for the formal security verification using the widely-accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. The simulation results show that SEAP is secure. The rigorous security and performance analysis shows that the proposed SEAP is secure and efficient as compared to the related existing authentication protocols for NFC applications.

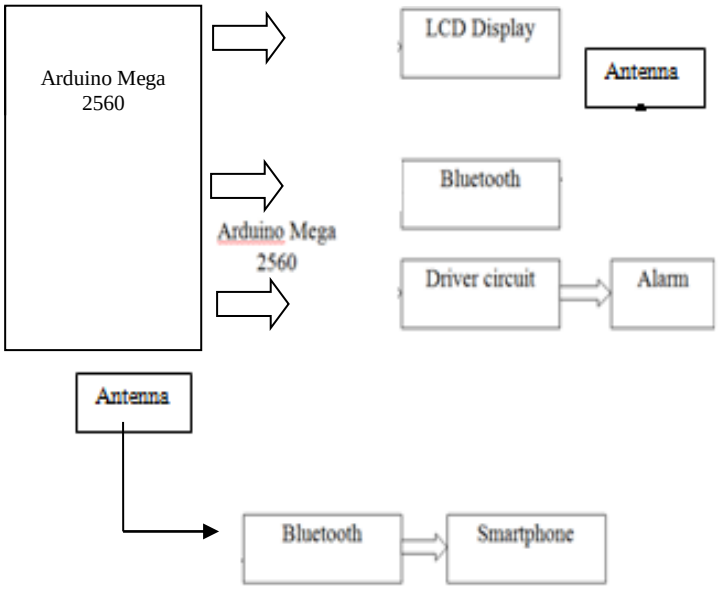
Keywords: Near Field Communication, NFC survey, Internet of Things, ubiquitous computing, Wireless Body Sensors, NFC ecosystem, NFC security, NFC applications, secure element, NFC usability, Critical transaction, Intrusion attacks, Autonomous Security, Mobile communication security, Public key cryptography, Authentication, Integrity and non-repudiation, NEMO ,MNP, MNPP, V2V, RO, Vehicular networks, Security, Performance, Reliability.

1. INTRODUCTION

The rapid development of short-range wireless communication technology, there is a growing demand to design secure and efficient mobile applications, such as service discovery, e-payment, ticketing, and mobile healthcare systems, etc., in the area of the consumer electronics for NFC. A new secure and efficient authentication protocol (SEAP) is presented for the NFC applications using the lifetime-based pseudonyms. The proposed pseudonym and private key pair in SEAP is valid within its lifetime only. Thus, even if a pseudonym and private key pair is unexpectedly revealed to an adversary, he/she can use it within its expiry time on behalf of the corresponding user only. As a result, the vulnerability in this case is limited to then corresponding user only, whereas in PBNFCP, CPPNFC protocol, it causes to the impersonation attacks to any legitimate user in the system when the identity of that user is known to the adversary. Moreover, the size of the proposed pseudonym in SEAP is significantly reduced.

The rigorous informal security analysis shows that SEAP is secure against possible well known attacks including the impersonation and man-in-the-middle attacks. In addition, the simulation results for the formal security verification using the widely accepted AVISPA tool shows that SEAP is secure against the passive and active attacks. SEAP significantly reduces the computation and communication costs, and also provides more security functionalities as compared to the related existing protocols. Due to efficiency and more security functionalities, SEAP is very suitable for the short-range wireless communication applications, such as service discovery, e-payment, ticketing, and mobile healthcare systems, etc., in the area of the consumer electronic devices in the NFC environment.

2. BLOCK DIAGRAM



3. EXISTING SYSTEM

The system allows interfacing between two machines by tapping one with other. Therefore the information is passed from one machine to another say Smartphone to machine. It reduces the time and increases the Reliability.

4. PROPOSED SYSTEM

When information is passing, there is a chances of hacking the information. So we proposed a system called SEAP for NFC that makes very security and access cannot be involved without human acknowledgement.

5. BRIEF METHODOLOGY

The project is designed with the following Hardware and Software

1. Arduino mega 2560
2. LCD Display
3. Driver circuit
4. Smartphone
5. Bluetooth
6. Alarm
7. Arduino IDE

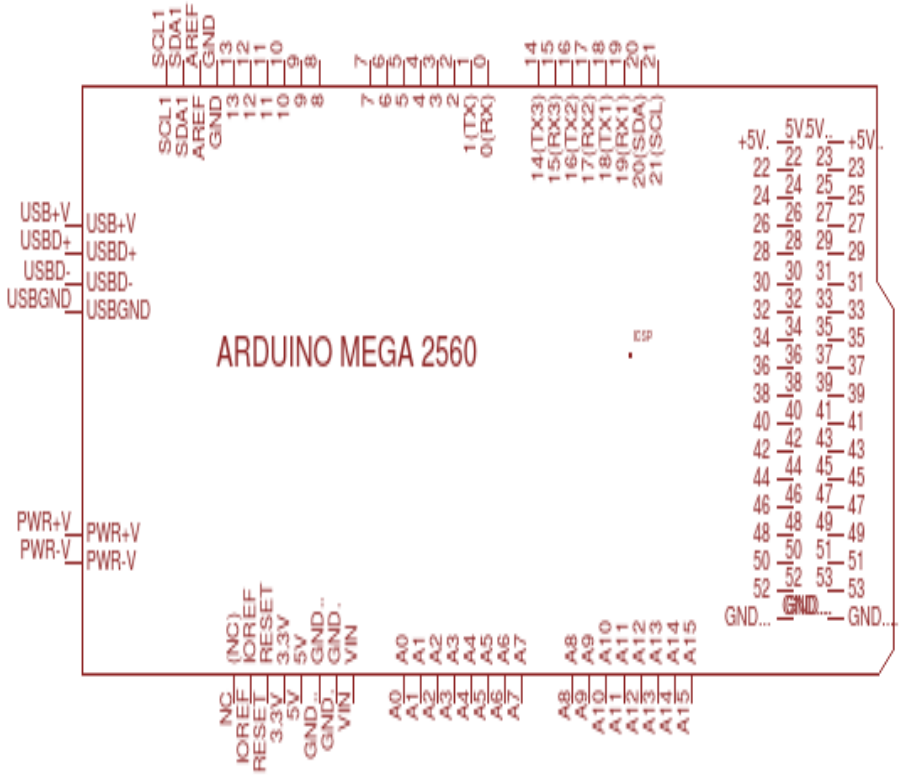
Here our machine act like a debit card machines, customer is connected with this machine via his smart phone. Both the devices can Communicate with Bluetooth. First Arduino will verify customer ID with its unique data, and check the amount balance of customer account. If it is sufficient it transfers the information to PC. And it will stores the database.

If the amount is not sufficient it automatically activates the alarm for indication of decline. Because of SEAP protocol implementation the information cannot be hacked by any one due to the datas in customer id. It increases the reliability of our process.

ARDUINO MEGA 2560

The Arduino Mega 2560 is a microcontroller board based on the ATmega2560 (datasheet). It has 54 digital input/output pins (of which 14 can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Mega 2560 is an update to the Arduino Mega.

The Arduino MEGA 2560 is designed for projects that require more I/O lines, more sketch memory and more RAM. With 54 digital I/O pins, 16 analog inputs. The Arduino MEGA 2560 is designed for projects that require more I/O lines, more sketch memory and more RAM. With 54 digital I/O pins, 16 analog inputs. The Arduino Mega 2560 is programmed using the Arduino Software (IDE), our Integrated Development Environment.



6. MOBILE APP DEVELOPMENT

Mobile app development is a term used to denote the act or process by which a mobile app is developed for mobile devices, such as personal digital assistants, enterprise digital assistants or mobile phones. These applications can be pre-installed on phones during manufacturing platforms, or delivered as web applications using server-side or client-side processing (e.g., JavaScript) to provide an "application-like" experience within a Web browser.

Application software developers also must consider a long array of screen sizes, hardware specifications, and configurations because of intense competition in mobile software and changes within each of the platforms.

7. THUNKABLE

Thunkable is the platform where anyone can build their own mobile apps. Available for Android and IOS. It is a drag and drop platform that allows users to create their own apps. It is easier to use and reduces the time.

8. ARDUINO-IDE

The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects the Arduino and Genuino hardware to upload programs and to communicate with them.

Writing Sketches

Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom righthand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor.

Sketchbook

The Arduino Software (IDE) uses the concept of a sketchbook: a standard place to store your programs (or sketches). The sketches in your sketchbook can be opened from the File > Sketchbook menu or from the Open button on the toolbar. The first time you run the Arduino software, it will automatically create a directory for your sketchbook.

Serial Monitor

Displays serial data being sent from the Arduino or Genuino board (USB or serial board). To send data to the board, enter text and click on the "send" button or press enter. Choose the baud rate from the drop-down that matches the rate passed to Serial. begin in your sketch. Note that on Windows, Mac or Linux, the Arduino or Genuino board will reset (rerun your sketch execution to the beginning) when you connect with the serial monitor.

9. PROTEUS SOFTWARE

The Proteus Design Suite is a proprietary software tool suite used primarily for electronic design automation. The software is used mainly by electronic design engineers and technicians to create schematics and electronic prints for manufacturing printed circuit boards. The micro-controller simulation in Proteus works by applying either a hex file or a debug file to the microcontroller part on the schematic. It is then co-simulated along with any analog and

digital electronics connected to it. This enables its use in a broad spectrum of project prototyping in areas such as motor control, temperature control and user interface design. It also finds use in the general hobbyist community and, since no hardware is required, is convenient to use as a training or teaching tool.

It is a software suite containing schematic, simulation as well as PCB designing.

1. ISIS is the software used to draw schematics and simulate the circuits in real time. The simulation allows human access during run time, thus providing real time simulation.
2. ARES is used for PCB designing. It has the feature of viewing output in 3D view of the designed PCB along with components.
3. The designer can also develop 2D drawings for the product.

10. BLUETOOTH

The introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 megabits per second, although the practical data transfer rate is 2.1 megabits per second. The additional throughput is obtained by using a different radio technology for transmission of the data. NFC was designed for swiping your phone or near field communication device within a couple of inches of the receiver whereas Bluetooth devices are known to hold a solid connection from distances of up to one hundred feet away. Bluetooth operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz including guard bands 2 MHz wide at the bottom end and3.5 MHz wide at the top. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels.

11. EDR provides the following benefits

1. Three times faster transmission speed − up to 10 times (2.1 Mbit/s) in some cases.
2. Reduced complexity of multiple simultaneous connections due to additional bandwidth.
3. Lower power consumption through a reduced duty cycle.
4. The Bluetooth Special Interest Group (SIG) published the specification as "Bluetooth 2.0 + EDR" which implies that EDR is an optional feature.

HC-05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup.

Serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR (Enhanced Data Rate) 3Mbps Modulation with complete 2.4GHz radio transceiver and baseband. It uses CSR Bluecore 04-External single chip Bluetooth system with CMOS technology and with AFH(Adaptive Frequency Hopping Feature). It has the footprint as small as 12.7mmx27mm. Hope it will simplify your overall design/development cycle.

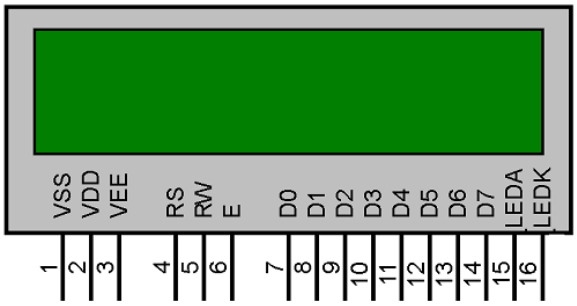
The Bluetooth module HC-05 is a MASTER/SLAVE module. By default the factory setting is SLAVE. The Role of the module (Master or Slave) can be configured only by AT COMMANDS. The slave modules cannot initiate a connection to another Bluetooth device, but can accept connections. Master module can initiate a connection to other devices

12. LCD DISPLAY

A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in colour or monochrome.

Features of 16×2 LCD module

1. Operating Voltage is 4.7V to 5.3V
2. Current consumption is 1mA without backlight
3. Alphanumeric LCD display module, meaning can display alphabets and numbers
4. Consists of two rows and each row can print 16 characters.
5. Each character is build by a 5×8 pixel box
6. Can work on both 8-bit and 4-bit mode
7. It can also display any custom generated characters
8. Available in Green and Blue Backlight



13. DRIVER CIRCUIT

In electronics, a driver is an electrical circuit or other electronic component used to control another circuit or component, such as a high-power transistor, liquid crystal display (LCD), and numerous others.

They are usually used to regulate current flowing through a circuit or to control other factors such as other components, some devices in the circuit. The term is often used, for example, for a specialized integrated circuit that controls high-power switches in switched-mode power converters. An amplifier can also be considered a driver for loudspeakers, or a voltage regulator that keeps an attached component operating within a broad range of input voltages.

NPN transistor act as a driver to open circuit if buzzer rises. The Bipolar Junction Transistor or simply BJT is a three layer, three terminal and two junction semiconductor device. Almost in many of the applications these transistors are used for two basic functions such as switching and amplification.

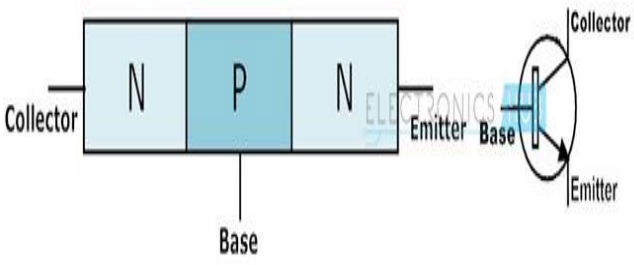
Transistor as a Switch

A transistor is used for switching operation for opening or closing of a circuit. This type solid state switching offers significant reliability and lower cost as compared with conventional relays. Both NPN and PNP transistors can be used as switches. Some of the applications use a power transistor as switching device, at that time it may necessary to use another signal level transistor to drive the high power transistor.

NPN Transistor as a Switch

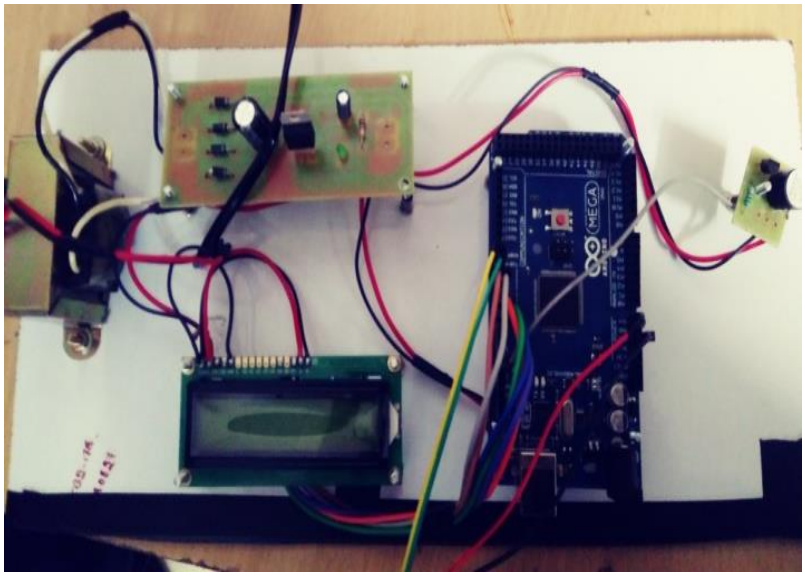
Based on the voltage applied at the base terminal of a transistor switching operation is performed. When a sufficient voltage (Vin > 0.7 V) is applied between the base and emitter, collector to emitter voltage is approximately equal to 0. Therefore, the transistor acts as a short circuit. The collector current Vcc/Rc flows through the transistor.

Similarly, when no voltage or zero voltage is applied at the input, transistor operates in cutoff region and acts as an open circuit. In this type of switching connection, load (here LED lamp) is connected to the switching output with a reference point. Thus, when the transistor is switched ON, current will flow from source to ground through the load.



14. RESULT

By using an app one can send the required amount and the Authorised person only get the App. The Status of the Transaction will be viewed in the Display. Any third person cannot access the transaction without the human Acknowledgement.



REFERENCES

[1] Gartner, "Market Insight: The Outlook on Mobile Payment," Market Analysis and Statistics, May 2010.

[2] Juniper Research, "NFC Mobile Payments & Retail Marketing-Business Models & Forecasts 2012-2017," May 2012.

[3] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 1953-1966, Jun. 2015.

[4] R. Want, "Near field communication," IEEE Pervasive Comput., vol.10, no.3, pp. 4 - 7, July. 2011.

[5] V. Patil, N. Varma, S. Vinchurkar, and B. Patil, "NFC based health monitoring and controlling system," in Proc. IEEE Global Conference on Wireless Computing and Networking, Lonavala, India, pp. 133-137, Dec. 2014.

[6] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," Wireless Pers. Commun., vol. 71, no. 3, pp. 2259-2294, Aug. 2013.

[7] W. Lumpkins and M. Joyce, "Near-Field Communication: It Pays: Mobile payment systems explained and explored," IEEE Consum. Electron. Mag., vol.4, no.2, pp.49-53, Apr. 2015.

[8] F. Michahelles, F. Thiesse, A. Schmidt, and J. R. Williams, "Pervasive RFID and near field communication technology," IEEE Pervasive Comput., vol. 6, no. 3, pp. 94-95, July. 2007.

[9] V. Coskun, K. Ok, and B. Ozdenizci, Near Field Communication (NFC): From Theory to Practice, London: Wiley. ISBN: 978-1-1199- 7109-2, Feb. 2012.

[10] J. Ondrus and Y. Pigneur, "An assessment of NFC for future mobile payment systems," in Proc. International Conference on the Management of Mobile Business, Toronto, Canada, pp. 43-43, July 2007

[11] ISO/IEC 15946-1:2008, "Information technology - Security methods- Cryptographic methods based on elliptic curves - Part 1: General," Apr. 2008.

[12] ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange between systems - NFC Security - Part 1: NFC-SEC NFCIP-1 security service and protocol," ISO/IEC, May 2010.

[13] ISO/IEC 13157-2:2010, "Information technology Telecommunications and information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.

[14] S. Kannadhasan, M. Isaivani, and G. Karthikeyan, "A Novel Approach Privacy Security Protocol Based SUPM Method in Near Field Communication Technology," in Proc. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Kumaracoil, India,

[15] vol. 324, pp. 633-643, Nov. 2014.