Secure Hybrid Mobile Application Containers

Swathy M Sony

Abstract— A secure hybrid application container and its deployment mechanism helps to provide secure data transfer by implementing hybrid mobile application container inside the mobile phone which highly useful in large organization for data transfer and communication. Hybrid mobile application describes an application created to run on a mobile device and components are defined using HTML5 and CSS3 and JavaScript. Hybrid mobile application combines the best parts of native applications and web applications. Mobile application container itself is a secure mobile application in which entry is strictly restricted to authenticated users with help of login id, strong password and smart card. The data moving in and out of the mobile application always in encrypted form using self-encryption scheme. Main feature of containerization is separation of personal and organizational data of a person. Container composed of various plug-in, container application and application manager. The system provide multiple levels of authentication mechanism that secures access to the applications and data residing within container.

Index Terms— Container, Demilitarized Zone, Firewall, Hybrid Mobile Application, Near Field Communication, Radio Frequency, Self Encryption Scheme

1 Introduction

Hybrid mobile application describes an application created to run on a mobile device where the application logic is primarily written in JavaScript and the user interface components are defined using HTML5 and CSS3 [6]. The most frequently used hybrid framework is Apache Cordova more commonly known as PhoneGap [2] [4]. Increasingly large organizations are allowing employees to use their own mobile devices for their work purposes, it has created a set of challenges for the IT teams within these organizations. A major challenge is to allow the employee freedom to use the phone for personal tasks and IT Management enforced policy, yet still protect enterprise data and applications. In order to do this some type of separation mechanism needs to be introduced in order to ensure that there are no data leakages or security intrusions. Protection is delivered in the form of a virtual container [1] that applications can run inside, their data is containerizing at the application level. This is accomplished by wrapping a layer of protection around the enterprise deployed apps, which separates the corporate data from the employee's private information and consumer applications.

2 Materials and methods

The main methodologies followed in order to implement a secure mobile container is explained.

2.1 Hybrid Mobile Application

A hybrid app is essentially a web app, built using HTML5 and JavaScript that is then wrapped inside a thin native container that provides access to native platform features like camera, contact list and so on [2] [3].

2.1 Mobile Application Containers

When employees use their personal mobile devices for business purposes, enterprise apps and data become vulnerable if the right management policies are not in place. The aim of containerization is to separate personal and corporate data through a series of technological features. This can include things such as; encryption, authentication, and other measures to protect from data leakage. Mobile application container itself is a mobile application. By developing container, corporate information can be protected in cases where the employee loses the device or in any number of other scenarios. Container components represented in Fig 1.

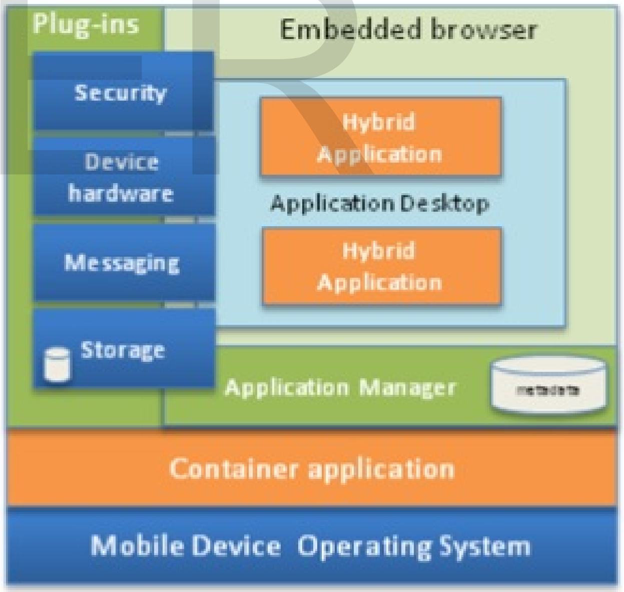

Fig 1 : Container Components

3 Security Requirements

3.1 Non Repudiation

Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

3.2 Availability

Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.

3.3 Data Integrity

Data integrity, in the context of networking, refers to the overall completeness, accuracy and consistency of data. Data integrity must be imposed when sending data through a network. This can be achieved by using error checking and correction protocols [5].

3.4 Confidentiality

Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

3.5 Authentication

Authentication is a process that ensures and confirms a users identity. Authentication is one of the five pillars of information assurance (IA). The other four are integrity, availability, confidentiality and non-repudiation

3.6 Authorization

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. System administrators (SA) are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

4 Security Implementations

Three levels of security implemented in the system along with a highly restricted firewall implementation. Demilitarized zone provide secure access to the system with external network. And first level of security is establishing a strong and secure device password for the mobile phone. Password should be minimum length of fifteen character which includes character, digits and special characters. It must be periodically changed for security reason. Second level is establishing security for container. A specified login and strong password should be there for access the container. After providing the container login details tap the NFC enabled device with smart card, then a screen for providing smart card password will appear. After entering the password only enter to container is allowed, otherwise access is denied. Entire working flow of the system represented in the Fig 2.

Steps:

(1) : Device Password
(2) : Login to the container
(3) : Using smart card & its password user is authenticat ed
(4) : Data transfer is occurred only above 3 steps are valid and user is authenticated

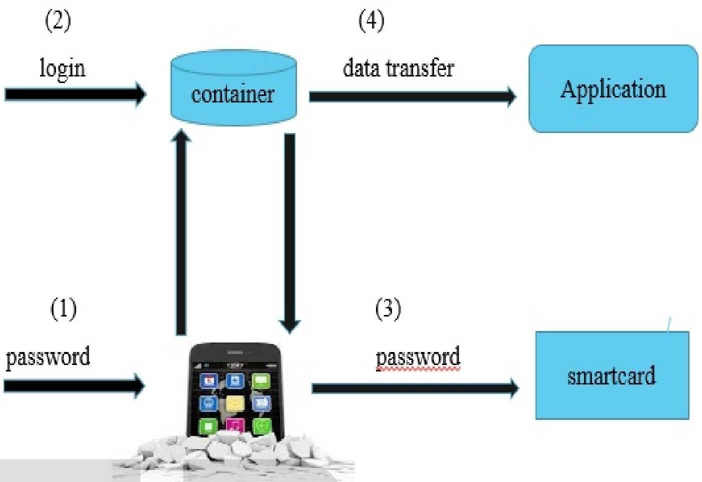

Fig 2 : Working Flow of the System

4.1 Smart Card

A smart card is a credit card sized plastic card with an embedded computer chip.The chip can either be a microprocessor with internal memory or a memory chip with non-programmable logic [7]. They can be programmed to accept, store and send data. Smart cards provide tamperresistant storage for protecting sensitive information like private keys, account numbers, passwords, and other forms of personal information. All smart cards have essentially the same physical interface to the outside world, the smart card reader. Smart card shown in Fig 3.

Fig 3 : Smart Card

To use a smart card an end user simply inserts it into a read / write device where it remains for the duration of a session or transaction. Contact smart cards must be inserted into a smart card reader device where pins attached to the reader make contact with pads on the surface of the card to read and store information in the chip. Smart card working is shown in Fig 4.

Contact-less smart cards contain an embedded antenna instead of contact pads attached to the chip for reading and writing information contained in the chip's memory. Contact-less cards do not have to be inserted a smart card reader. Instead, they need only be passed within range of a radio frequency acceptor to read and store information in the chip. These cards have an antenna embedded inside the microchip that allow the card to communicate with an antenna coupler unit without physical contact. NFC enabled mobile phone used to access the datas from the card.

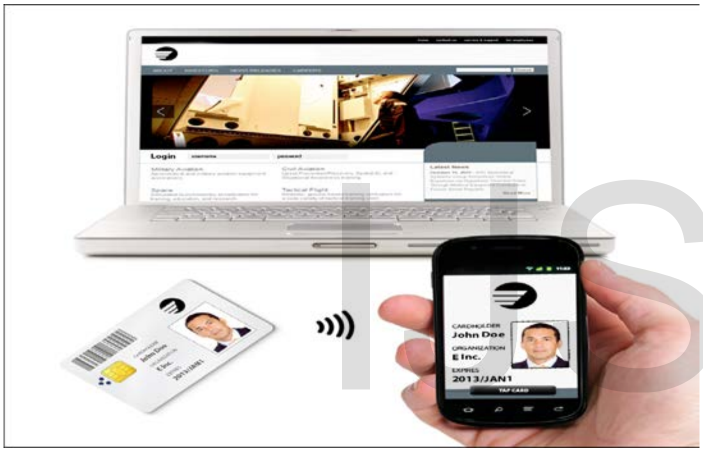

Fig 4 : Working Of Smart Card

4.2 Near Field Communication

4.2.1 Reader

Usually a microcontroller-based (for example NFC enabled phones) with an integrated circuits that is capable of generating radio frequency at 13.56 MHz with other components such as encoders, decoders, antenna, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation. The reader continuously emits RF carrier signals, and keeps observing the received RF signals for data. Following figure shows how phone generates RF signal and how tag antenna get power from it.

4.2.2 Tag

An RFID device incorporating a silicon memory chip connecting to external antenna. Tag does not have its own power source. The passive tag absorbs a small portion of the energy emitted by the reader (phone), and starts sending modulated information when sufficient energy is acquired from the RF field generated by the reader.

4.2.3 Data Transfer

The reader continuously generates an RF carrier sine wave, watching always for modulation to occur. Detected modulation of the field would indicate the presence of a tag. A tag enters the RF field generated by the reader. Once the tag has received sufficient energy to operate correctly, it divides down the carrier and begins clocking its data to an output transistor, which is normally connected across the coil inputs. The tags output transistor shunts the coil, sequentially corresponding to the data which is being clocked out of the memory array. Shunting the coil causes a momentary fluctuation (dampening) of the carrier wave, which is seen as a slight change in amplitude of the carrier. The reader peak-detects the amplitude modulated data and processes the resulting bit stream according to the encoding and data modulation methods used.

4.2.4 Working Principle

A radio frequency (RF) sine wave generated by the reader (phone) is used to transmit energy to the tag and retrieve data from the tag. When the NFC in the device is active then it continuously generates periodic sine wave signal at frequency 13.56 MHz center frequency. If there is any tag within the area of magnetic flux generated by the sinewave, tag gets energy from the magnetic fluxes and create counter frequency or change the frequency properties of the original sine wave generated by phone. The changes are detected by the phone and phone knows that there is a tag nearby.

The range where communication is considered to be close coupled is between 0 and 1 cm. This means that the tag has to be placed either in the reader or more or less pressed against the reader device. The benefit from these short distances is that a rather large amount of energy can be extracted from the magnetic field by the tag. More energy is available for signal processing in the tag at this distance without the need for a power supply in the tag. Close coupling is also preferred for systems with high security requirements. Following figure shows some simplified relation between NFC applications to NFC hardware.

4.3 Self Encryption Scheme

The message is encrypted and the cipher text is stored on the mobile device, whereas the key stream is stored separately. This makes it computationally not feasible to recover the original data stream from the cipher text alone. Sensitive data is broken into two parts using SE, first is major part- cipher text second is minor part- key stream [8]. The major part (Part A: cipher text) is stored in the mobile device carried by the company employee. The minor part (Part B: key stream) is protected in the secure server of the company. Self encryption scheme is shown in Fig 5.

Cipher text is created by applying xor operation with the plain text and keystream. Part A is encrypted using part B. When the user needs to access the data, he or she has to input a correct PIN to pass the authentication procedure. Then the server will send part B to decrypt part A and merge them together to recover the original plain text. When a mobile device is lost, at most the adversary can access the part A, from which it is computationally infeasible to get meaningful information. Encrypts the plain text and decrypts the cipher text using a key stream. The length of the key stream depends on the user's security requirements. The complexity can be increased by taking large number of key stream for encrypting the plain text. When a user want to decrypt the data, the user must give a request to the server first. After sending the request the server ask the security pin for the user to provide secure transaction of datas. When user send his secure pin to server, server will check the pin and then user is authenticated. After that server will send the key for decrypting the data.

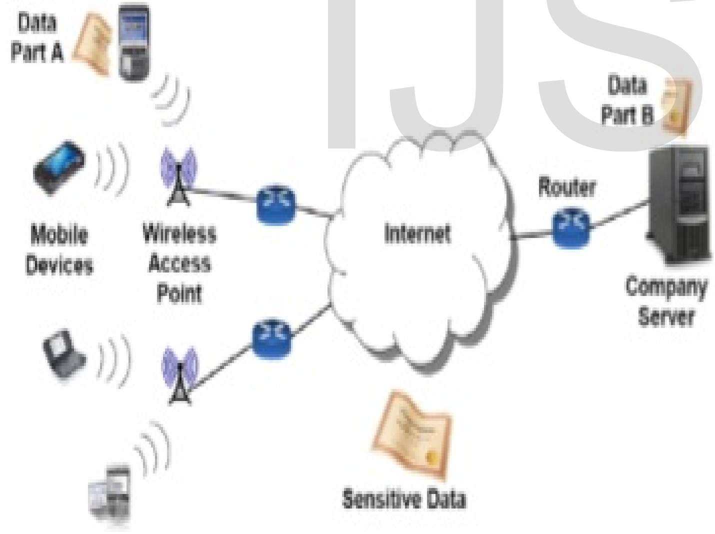

Fig 5: Self Encryption Scheme

5 Conclusion and Future Works

Phones are being used as computers by more people and for more purposes. Smart phones are generally cheaper than computers, more convenient because of their portability. The paper presents an extensible hybrid mobile application container solution. The container solution offers benfits to three distinct groups within a large organization the application developers, the IT management group, and the organizations general employees. As the number of vulnerabilities and, hence, of attacks increase, there has been a corresponding rise of security solutions are defined. Mobile application container itself is a secure application in which entry is strictly restricted to authenticated users with help of login id, strong password and smart card. The data moving in and out of the mobile application always in encrypted form using self-encryption scheme.

Main advantage of containerization is separation of personal and organizational data of an employee. Container components includes plug-in, container application and application manager. The system provide multiple levels of authentication mechanism that secures access to the applications and data residing within container. It provides more security and reliability for the proper communication of the system and the users. A container for hybrid mobile applications implementation provides more security for the systems in a user friendly approach.

The system can be improved by applying more effective and complex encryption scheme to protect the data that are dealing with. The complexity can be increased by taking large number of key stream for encrypting the plain text. As the complexity in number of keys and encryption scheme is increased then the attack can be reduced in an effective manner. And more works can be done to reduce the time delay of accessing the datas in the system. The system with more security and faster access can be developed by future works.

References

[1] David Jaramillo, Robert Smart, Borko Furht, Ankur Agarwal, *A secure extensible container for hybrid mobile applications*, IEEE, 2013.

[2] A. Rohit. Ghatol Yogesh Patel, *Beginning PhoneGap Mobile Web Framework for JavaScript and HTML5*, Apress, 2012.

[3] Allen. L. Lundrigan, V. G. Sarah, Pro *Smartphone Cross-Platform Development*, Apress, 2010.

[4] Avinash Shrivasi, Anandakumar Pradeshi, *Implementation of cross-platform mobile application using phonegap framework*, International Journal of Computer Science and Engineering,
Vol 3, Issue 3, page 23-30, May 2014.

[5] *Is It Finally Time to Worry about Mobile Malware*, vol 41, no 5, page 12-14, 2008.

[6] Hasan Yousaf, Mustafa Zaidi, Najmi Haider, W. U. Hasan, I. Amin, *Smart Phones Application development using HTML5 and related technologies: A trade off between cost and quality*, International Journal of Computer Science, Vol 9, Issue 3, No 3, 2012.

[7] *Mobile Devices and Identity Applications*, A Smart Card Alliance Identity Council Publication, September 2012.

[8] Shinn Ku, Yu. Chen, *Self-Encryption Scheme for Data Security in Mobile Devices*, CCNC, Las Vegas NV, USA, page 10-13,2009

About Author

Swathy M Sony, currently persuing master's degree program in Computer Science & Engineering in Jyothi Engineering College, Cheruthuruthy institute which is under the Calicut University located in Kerala, India. This work completed successfully by guidance of Asst. Prof. Ms. Swapna B Sasi.
Email : swathykrishna02@gmail.com