Mobile Infrastructure Investigation for Protected Mobile Payments

Kamal Ahmad, Qazi Ahmad Faraz, Noor Zaman, Shafiullah, Zaheer Aslam and Rashid Zubair
Gandhara University of Sciences, Peshawar, Pakistan

***Abstract*– Payments through mobiles are a new expedient scheme for customers to carry out transactions, and are envisaged to augment as the amount/number of mobile phone user's boosts. Devices, like cellular phones and Personal Digital Assistants, to erect or make payments are progressively more common, predominantly in Europe and Asia. The Mobile Payment (MP) can be described as any sort of payment transaction that engrosses a mobile device. There is spacious assortment of options available to execute mobile payments just because of the accessibility or availability of network technologies. The main objective of this paper to investigate the mobile infrastructure just for the sake of secure mobile payments.**

***Keywords*–** Mobile Payment, Security, Technology and Protection

I. INTRODUCTION

The network technologies of mobiles have progressed from continuous or analog based systems to discrete or digital based systems and from (CS) circuit switching to (PS) packet switching technologies [1]. This evolution can be described by dissimilar mobile technologies generations, i.e., (1G) first-generation, (2G) second-generation, 2.5G and (3G) third-generation technologies. Merely, 1G is based on analog technology. A number of foremost standards for every generation technology are:

- 1st Generation or 1G: (AMPS) Advance Mobile Phone System in North America, (TACS) Total Access Communication System in United Kingdom, (NTT) Nippon Telegraph & Telephone from Japan, and (CDMAONE) Code Division Multiple Access One.
- 2nd Generation or 2G: (GSM) Global System for Mobile Communication, (CDMA2000) Code Division Multiple Access 2000, (HSCSD) High Speed Circuit Switched Data Technology.
- Half passed second Generation or 2.5G: (GPRS) General Packet Radio System & Enhanced Data Rate for GSM Evolution (EDGE).
- 3rd Generation or 3G: Universal Mobile Telephone Standard (UMTS).

II. SHORT MESSAGE SERVICE

Short Message Service imparts a mechanism for broadcasting dumpy or short messages from wireless to wireless handsets SMS was fashioned as a ingredient/part linked with the GSM Phase 1 standard to fling and take delivery of short or dumpy text messages, having length from 70-160 alphanumeric characters, Binary Message of 8 bits containing 140 characters in length transmit and receive from mobile phones. Short Message Short is a graceful service, as it can accumulate messages incase the destination/target mobile device is powered off and promotes the messages incase when the unit is for a second time in use. Short Message Service applications are deliverance of substitution ring tones, voicemail/fax notifications, group graphics and operator logos, cohesive/unified messaging, individual communication text messaging, and all other information services. Commonly, whichever information which fits into a SMS can be conveyed by a short text message SMS.

Premature idea for SMS usage was proposed for the subscribers to send non-sensitive messages athwart the open GSM network. Reciprocated authentication, text encryption, end-to-end security, non-repudiation were mislaid during the design of GSM architecture.

Spoofing of SMS: This is a kind of attack that entails a 3rd party transferring out Short Message Service messages that emerge to be from an authorized or legit sender. It is likely to be shifting or varying the inventor address value/field in the Short Message Service header to a new alpha-numerical string. It conceals the inventive sender address and the dispatcher can send out hoax messages and carry out masquerading attacks.

Encryption of SMS: Format of the default data for Short Message Service messages is in plaintext. The merely encryption implicated throughout communication is the encryption amid/between the base transceiver station and mobile station. End to end encryption is presently not in use. Encryption algorithm utilized is A5 that is confirmed to be weak or vulnerable. Consequently an extra protected algorithm is required. Short Message Service security mechanism depends on UMTS/GSM signaling plane security mechanism. Short Message Service may possibly be eavesdropped through man-in-the-middle assault/attack while no encryption is functional to Short Message Service transmission.

Mobile payment systems Short Message Services based are by now in use worldwide. There might be definite risks when employing Short Message Service in the imbursement/payment transaction. Short Message Service can be utilized for mobile imbursement/payments endowed with the modified client constructed by SIM toolkit or Java application is exercised for the employment of Short Message Service transaction to offers end-to-end encryption.

III. UNSTRUCTURED SUPPLEMENTARY SERVICES DATA

A mechanism of disseminating information via a GSM Network, USSD proffers a real-time connection during a session [2]. Turnaround reaction times for interactive applications are less for USSD than Short Message Service for the reason that the session-based feature of USSD. USSD message be capable of up to 182 alphanumeric characters in length. USSD permits interactive services among a MS and applications horded by the (MO) Mobile Operator. These messages are compiled of numbers and the *, # keys, and allocate users to easily and hastily acquire information/access services as of the Operator. The primary USSD services were called Phase 1 or MAP 1 and are only capable to surpass information from the handset to the unstructured supplementary services data application with substantiation.

There was as a result no session apprehended flanked by the handset and the application. Phase 2 (or MAP 2) Unstructured supplementary services data added the capacity for launching a session as a substitute of a once-off transaction. This intended that the handset and the unstructured supplementary services data application possibly will at present have the nominal counterpart of a dialogue. GSM handsets beared USSD commencing the earliest days of GSM, so contrasting SMS, each particular GSM handset in the globe props up USSD. Phase 2 has been shored up for years and above 99% of handsets presently in exercise can utilize sessions on the USSD bearer.

Unstructured supplementary services data is a session oriented service, and can hold up a sequence of swap of information. Phase 2 unstructured supplementary services data also permits communication/messages to be pressed onto a MS. It is quite a few times quicker than MO SMS messages in view of the fact that there is no store and forward of messages. The USSD gateway sustains an untie/open HTTP interface. In general the unstructured supplementary services data functionality is putted into operation in the following modes:

- Drag/pull Mode, will grip Mobile instigated USSD Requests.
- Push Mode will grip network instigated USSD Requests.

Nearly all handsets also prop up NI unstructured supplementary services data (network initiated USSD), as well called “unstructured supplementary services data Push". With NI unstructured supplementary services data, the network be capable of moving forward information to the subscriber's handset. Another vital verity regarding unstructured supplementary services data, is so as to messages from handsets always road to the residence network.

This concludes that if you are roaming in a different network, then dialing an unstructured supplementary services data string on your phone will forever route to the application on your abode/home network. If you are exercised to entrée a meticulous service in your abode/home network, after that you will as well be able to way in it from a different country. On the further hand, roaming subscribers from additional networks cannot way in unstructured supplementary services data services on a host network.

No separate security owned by USSD instead it depends on UMTS/GSM signaling plane security mechanism.

The solutions of unstructured supplementary services data are by now in use for mobile payments across the world. Some evaluate of encryption or message truthfulness/integrity corroboration is obligatory to grant a protected unstructured supplementary services data based imbursement/payment system. USSD cannot endow with supplementary security on its own. A different application is used for the consumption of USSD transaction to endow with end-to-end encryption.

IV. GENERAL PACKET RADIO SERVICE

High-speed packet data technology, being positioned in GSM networks worldwide. This will significantly augment the services accessible to the end user of mobile information/data computing. [4] GPRS permits for the transferring and getting of data at much elevated speed than accessible today. Data diffusion/transmissions speeds depart/go from 9.6 kbps to a notional highest alacrity/speed of up to 171.2 kbps are attainable with general packet radio service by means of all eight timeslots simultaneously. It utilizes its radio resources when users are in fact sending or receiving data, for that reason the available radio resource can be alongside common/shared among quite a few mobile data users, to a certain extent dedicating a radio channel to a solitary/single user for a specific/fixed period of time. This well-organized exercise of limited radio resources indicates that huge numbers of general packet radio service users can potentially contribute the same bandwidth and be dole out from a single cell.

The core network of GPRS is an incorporated part of the GSM network; it is layered over the fundamental GSM network, with added nodes to gratify for packet switching. GPRS also make exercise of a few of the accessible GSM network elements; a few of these contain existing Base Station Subsystems (BSS), Mobile Switching Centers (MSC), Authentication Centers (AUC), and Home Location Registers (HLR). Some of the additional GPRS network elements to the obtainable Global System for Mobile network include; general packet radio service Support Nodes (GSN), general packet radio service tunneling protocol (GTP), Access points, and the (Packet Data Protocol) PDP Context. General packet radio service fortification functionality is the same to the vacant GSM protection/security. From a defense/security point of view the identical merits and dumpy/short comings of GSM relates to GPRS service. At session instigation, a user is legitimated by means of surreptitious information enclosed on a smart card called a Subscriber Identity Module (SIM). Validated data is swap and corroborated with records accumulated in the HLR network node. The microwave links to the BSSs are comprehensively utilized after the operator unbolts/opens its service. Voice and cipher keys Kc can be seized on such links. In order to evade the attack, the operators ought to substitute the weak A3/A8 algorithm with a brawny/strong one.

Ultimate Solutions for GPRS are already in exercise for mobile payments across the world. Application level security is supposed to use to supply end to end transaction protection/security. Yet though nearly all of the mobile

phones shore up general packet radio service, not all the phone user stimulates the general packet radio service connection and in nearly the entire countries general packet radio service is very pricey.

V. CODE DIVISION MULTIPLE ACCESS

A proprietary standard for mobile communication, wherever GSM is an open standard. CDMA was forged by Qualcomm and improved by Ericsson. Both standards are in rivalry for supremacy in the cellular world. code division multiple access is a spread spectrum technology, which implies that it broadens/spreads the information enclosed in a fastidious signal of concentration in excess of a greatly superior bandwidth than the original signal [6]. A CDMA call initiate at 9.6 kbps standard rate, which is then extend to a broadcasted rate of thereabout 1.23 Mbps.

By plan, CDMA 2000 1xRTT technology constructs eavesdropping very tricky, whether deliberately or unintentionally. Unique to code division multiple access 2000 1xRTT systems, is the 42-bit PN (Pseudo-Random Noise) Sequence called Long Code to knott data and voice. On the frontward/forward link (network to mobile), data is knotted at a rate of 19.2 Kilo symbols per second (Ksps) and on the reverse link, data is twisted at a rate of 1.2288 Mega chips per second (Mcps) [7]. The code division multiple access 2000 1xRTT network security protocols rely on a 64-bit authentication key (A-Key) and the Electronic Serial Number (ESN) of the mobile. A random binary number called RANDSSD, which is engendered in the HLR/AC, also takes part in a role in the verification procedures.

The A-Key is programmed into the mobile and is accumulated in the Authentication Center (AC) of the network. In accumulation to verification/authentication, the A-Key is exercised to spawn the sub-keys for voice solitude and message encryption. CDMA 2000 1xRTT employs the standardized CAVE (Cellular Authentication and Voice Encryption) algorithm to engender/generate a 128-bit sub-key called the "Shared Secret Data" (SSD). The A-Key, the ESN and the network-supplied RANDSSD are the inputs to the CAVE that breeds/generates SSD. The SSD has two parts: SSD_A (64 bit), for producing verification/authentication signatures and SSD_B (64 bit), for generating keys to scramble/jumble voice and encrypt signaling/data messages. The SSD be capable to be shared with roaming service suppliers/producers to permit confined/local verification/authentication.

A brand new SSD can be spawned when mobile revisits to the abode/home network or roam to a dissimilar/different system. Third Generation technologies (3G) append extra safety measures protocols, together with the use of 128-bit privacy and authentication keys. For CDMA2000 networks, innovative algorithms like locked/secure Hashing Algorithm-1 (SHA-1) are being utilized for hashing and integrity, and the Advanced Encryption Standard, AES (Rijndael) algorithm for message encryption. The AKA (Authentication and Key Agreement) protocol will be exercised for every liberate/releases following CDMA2000 Release C. The AKA protocol will also be used in WCDMA-MAP networks, along with the Kasumi algorithm for encryption and message integrity.

The concern solutions of CDMA are by now in exercise for mobile imbursement/payments. Code Division Multiple Access is better/superior to 2nd Generation technology to Global System Mobile. Code Division Multiple Access is not broadly used compared to GSM worldwide.

VI. CONCLUSION

In this paper, we have studied and investigated the mobile infrastructure just for the sake of secure mobile payments. We have discussed the different issues regarding mobile payment security and suggested some solutions to minimize these problems.

REFERENCES

[1] State of the Art Review of Mobile Payment Technology - David McKitterick and Jim Dowling
[2] The Future Mobile Payments Infrastructure - Institute for Communications Research Systems @ Work Pte. Ltd.
[3] Security of Mobile Banking - Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison
[4] GSM and GPRS Security - Chengyuan Peng
[5] http://www.truteq.com/tips/ussd/
[6] The Future Mobile Payments Infrastructure A Common Platform for Secure M-Payments
[7] CDMA 2000 1xRTT Security Overview