Article title: A Comparative Study of Network Securities on Mobile Transaction  
Authors: Geoffrey Tyolaha[1], Moses Israel[2]  
Affiliations: Electrical and Computer Engineering/ Ahmadu Bello University, Samaru, Zaria, Kaduna, Nigeria[1], Mathematics/Computer Science, Federal University of Agriculture Makurdi, Makurdi, Benue, State, Nigeria.[2]  
Orcid ids: 0000-0001-8976-6763[1]  
Contact e-mail: geoffretyolaha@gmail.com  
License information: This work has been published open access under Creative Commons Attribution License http://creativecommons.org/licenses/by/4.0/, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. Conditions, terms of use and publishing policy can be found at https://www.scienceopen.com/.  
Preprint statement: This article is a preprint and has not been peer-reviewed, under consideration and submitted to ScienceOpen Preprints for open peer review.  
Funder: self  
DOI: 10.14293/S2199-1006.1.SOR-.PPZM9FW.v1  
Preprint first posted online: 02 November 2021  
Keywords: Mobile,, Transaction, Security, WLAN Security, Encryption, Security Protocol, Cipher Block, 4G/LTE, LTE end-to-end Security, Wireless Security
A Comparative Study of Network Securities on Mobile Transaction

Tyolaha, Geoffrey Terkura*  Moses Israel

ABSTRACT

In recent years, the number of mobile transactions has skyrocketed. Because mobile payments are made on the fly, many consumers prefer the method to the traditional local payment approach.

The rise in mobile payments has inspired this study into the security of mobile networks in order to instill trust in those who may be involved in the transaction in some way.

This report is a precursor to explain and compare some of the most popular wireless networks that enable mobile payments, from a security standpoint, this research presents, explains, and compares some of the most common wireless networks that enable mobile payments. Threat models in 3G with connections to GSM, WLAN, and 4G networks are classified into four categories: attacks on privacy, attacks on integrity, attacks on availability, and assaults on authentication. In addition, we offer classification countermeasures which are divided into three categories: cryptographic methods, human factors, and intrusion detection methods. One of the most important aspects we analyze is the security procedures that each network employs. Since the security of these networks is paramount, it gives hope to subscribers. In summary, the study aims to verify if mobile payments offer acceptable security to the average user.

Background

M-commerce refers to the practice of conducting online transactions using mobile devices such as cellphones and personal digital assistants (PDAs). This can also be described as a contactless transaction in which devices are not directly connected but users still have access to the internet. [1]
Users can deposit money into an account saved on their phones, communicate balances to other users, including suppliers of products and services, and exchange deposits for conventional money using PIN-secured SMS text messages.

People in Uganda, Botswana, and Ghana were using airtime as a medium for money transfer in 2002, according to researchers at Gamos and the Commonwealth Telecommunications Organization, who were financed by the UK Department for International Development (DFID).[2] Kenyans were carrying airtime to family and acquaintances, who used or resold it. Mel was contacted by game developers. [3] S. Batchelor (Gamos) and N. Hughes (Vodafone CSR) addressed how a money transfer system in Kenya could be developed. Navigation began in 2005 after DFID changed the terms of its funding to Vodafone. A Kenyan student developed mobile software that allows users to share, receive, and store information. People use their mobile devices to make cash withdrawals Safaricom, on the other hand, swayed the student and purchased the project's ownership rights, effectively making them the only owners of the rights. Safaricom launched M-Pesa, a new mobile phone-based payment and money transfer service, in April 2007 as a result of a student software development project in Kenya. [4].

Smartphones, tablets, laptops, and other portable computing devices, as well as the networks to which they connect, are protected from risks and vulnerabilities associated with wireless computing by mobile security. Wireless security is another term for mobile security.

Securing mobile devices has become increasingly important in recent years as the number of devices in use and the applications for which they are used have grown dramatically. The problem is exacerbated by the continued trend toward IT consumerization, which is resulting in an increasing number of employee-owned devices connected to the corporate network. [5]

People nowadays use various mobile devices to connect to the internet and other network services for various purposes, such as the ones described above. With the advancement of technology, almost no system is today without connectivity features. Depending on who you are and what you want to do, these relationships have distinct roles. [6]

This technology creates a distinction in human events based on one's level of involvement in them. This does not negate human involvement; rather, it is a method of dispersing activities that
should have been concentrated in one location. According to research, this technology is used in a wide range of business activities, but it comes at a high price. One might believe that the costs of purchasing technology such as laptops, cell phones, and software are unavoidable. My main issue is the cost of learning how to use the device and the security of your regular transactions. We will be able to learn about the risks associated with using these technologies using this study.

Businesses are set up to meet people's needs while also generating a profit; nevertheless, there are those whose primary goal is to steal crucial items from other businesses. As a result, the study of security in using this medium for transaction has been motivated. [7]

**Aim and Objectives**

The goal of this study is to investigate:

- The notion of mobile payments
- Mobile payment network security.
- The security of four popular wireless networks, GSM, 3G, WLAN, and 4G, will be examined.
- To assess the many mobile security techniques obtainable in the aforementioned networks, as well as their requirements, as well as to comprehend the security success and functioning principle of the hazards associated with them.

**Statement of the Problem.**

Every major technology company wants to implement a mobile payment system. However, mobile payments aren't yet good enough to totally replace traditional payment methods. This is why.

There are numerous mobile payment apps and systems available (eg Intuit Gopayment, Paypal, Google Wallet, Pay with Square, Verifone Sail, etc). Some are administered by banks, some are incorporated into devices and use hardware-based encryption, and others are in the works from companies with excellent intentions but lack the competence to overcome user errors or process flaws. Furthermore, mobile payment systems necessitate a significant amount of maintenance.
As black hats hack or reverse engineer the old ones, minimum security criteria change on a regular basis.

Previously, cash transactions were carried out by physically transporting it from a source point to a destination area without incurring additional costs; however, as transactions grew in volume and the risk of transporting physical cash became apparent, the need for mobile transactions became unavoidable, [13]. Some of the questions to be addressed in order to acquire a better report are listed below.

- Define the mobile payment system and its current market impact.
- What makes the mobile payment system stand out?
- Is there any truth to the security of mobile payments and the most common security attacks?
- Can secure mobile payment solutions be implemented? And who is it for?
- Is this technology suitable for the average user?
- What suggestions do you have for a mobile payment system?
- Can this report effectively raise awareness of mobile payment consumers across several platforms?

**Scope/Limitations**

This paper will not cover every aspect of information security; instead, it will focus on three networks: 3G in conjunction with GSM, WLAN, and 4G networks, as well as the security mechanisms employed in each. The paper was written at Ahmadu Bello University in Zaria, Nigeria, and it will serve as a guide for those working in the subject of information security in mobile transactions across various networks. The user of this report must have a basic understanding of computer science, mathematics, and cryptography.
Target Audience

This is primarily aimed at students with a rudimentary understanding of information security in the fields of information technology, computer engineering/science, and telecommunication. It will also be beneficial to individuals who intend to use security technologies for financial gain.

Project Outlines

The first section of this report provides an overview of the study (A Comparative Study of Network Securities on Mobile Transactions), as well as the study's rationale and objective.

The second half of the paper will list some basic security criteria for wireless networks as well as an introduction to particular security methods for the various types of networks examined.

The third section presents an important perspective on wireless network assaults and security concerns in general, with appropriate actions made to prevent the attacks when practicable.

Finally, the offered results are reviewed, and adequate responses to the above-mentioned questions are provided.

Security in 3G in Connection to GSM.

Implementation of 3G/GSM security

- Confidentiality
- Authentication
- Availability and Reliability

The Don Parker security model can be used to implement the aforementioned security requirements so that we can see if it fits the requirements.

- Confidentiality: As the number of networks has grown, so has the usage of insensitive phone communication, necessitating the deployment of a secure channel to send information. End-user ID privacy, user location privacy, and data privacy must all be protected by some form of functionality. "The prevention of unauthorized disclosure of information" [38] is defined as
"confidentiality." The SIM contains the data required to encrypt the radio link between the MS and the BTS. It contains a key, $K_i$, which is later used to encrypt data in some versions of A5.

**Fig1.** COMP 128

According to the study, GSM is based on TDMA, which allows users to share radio channels with up to seven other users. Every frame, each user takes a turn using the shared radio channel, sending and receiving data only during one of the eight available time slots. Numbers are used to identify frames. Two frames are used in a GSM communication, one from the base station to the MS and the other from the MS to the base station. Both frames include bits of information that are supposed to be encrypted. Because the 3G network is based on the GSM network design, each uses the WCDMA encryption technology. Each of these frames contains bits of user data, and it is this data that informs the user.

The session key generated by the COMP128 method is then transferred to the MS and used by a different algorithm, the A5. A5 generates a keystream of bits using the session key and the frame number. The A5 generates a new bit keystream for each new frame to be sent, which is used to encrypt (and decrypt) the frame. The A5 algorithm, which is housed in the device's hardware rather than the SIM, must produce fresh key streams swiftly and continually. [38]

Instead of using the A5/1 stream cipher, 3G networks use the KASUMI block cipher. They're utilized in GSM in a similar way as A5/1, but with a few differences. In KASUMI, for example, the session key is 128-bit rather than 64-bit.

• Authentication: Because 2G and 3G networks are widely connected, anybody can access them from far and wide, their security must be carefully managed. End users must be able to authenticate themselves and prove that they are who they say they are.
In 2G and 3G networks, authentication is performed using two practical objects: the SIM card in the mobile device and the Authentication Center (AUC). One of the SIM's most important security functions is to authenticate the subscriber to the network. This method ensures that the MS seeking service is a valid subscriber, not an intruder, on the network. A challenge-response procedure is used by the network to verify a subscriber's identification. When an MS seeks service, the network issues a mathematical challenge to the MS, which it must successfully answer before access is allowed. A 128-bit value called RAND is sent by the network to the MS as a challenge. Regardless of how good RAND is in the It's unlikely that the security authentication process will be repeated, or that an attacker will be able to create a codebook of (RAND, SRES) pairings and exploit the information to obtain access to services. [38]

When RAND is received by the MS, it is forwarded to the SIM for processing. The SIM uses the A3 method to generate a 32-bit "signed answer" using RAND and the secret 128-bit key Ki. The response, known as SRES, is sent from the SIM to the terminal, where it is subsequently sent to the network. This is Microsoft's reaction to the challenge posed by the network. Meanwhile, the AUC of the network will carry out the same set of tasks. The network calculated its SRES value using the same RAND value and an identical copy of Ki. The network compares the SRES it receives from the MS to its own SRES. If the two values are the same, the network concludes the MS is valid and lets the service to run. If the two values don't match, the network concludes the SIM doesn't have the correct secret key Ki and rejects the MS service. [38]

An eavesdropper recording the SRES response will not be able to effectively reuse it later because the RAND value varies with practically every access attempt. Even if a RAND challenge is reused (and an attacker manages to impersonate a legal subscriber to the network), a GSM network can authenticate the MS as many times as it wants, perhaps multiple times during a connection. The next challenge the MS and SIM get from the network will almost certainly be a fresh one for the attacker, one for which he or she will be unable to compute the correct SRES. It's worth noting that one of the GSM security protocols' pillars is that a subscriber's secret key, Ki, is kept private. Ki is never communicated over the network, even though it is kept in both the SIM and the AuC. [38]

The COMP128 algorithm was intended to be a reference model for GSM implementation, but it has been adopted by practically all GSM operators throughout the world for various reasons.
COMP128 was hacked in April 1998, prompting the development of COMP128-2, a new, more powerful version. However, it is claimed that most operators are still utilizing the old defective algorithm due to the high expense of upgrading COMP128. [38]

Because GSM authentication was determined to have a suitable security level, the authentication method for GSM and 3G networks is identical. However, the GSM algorithm was found to be insufficient, and it was replaced with KASUMI (an algorithm used to provide over-the-air connection privacy in GSM networks by encrypting voice and data for transmission after successful encryption).

- Availability and Dependability: To ensure service reliability, GSM uses an intermittent location updating mechanism. If an HLR or MSC/VLR fails, having each mobile register at the same time to update the database will overburden the system. As a result, the database is updated as new locations are added. The operator controls the enabling of periodic updating and the time between periodic updates, which is a trade-off between signaling traffic and recovery speed. A mobile device is deregistered if it does not register after the update period. The IMSI attach and detach operation is connected to location update. • A disconnect informs the network that the mobile station is inaccessible, avoiding the need to assign channels and send paging messages that are unnecessary. An attachment functions similarly to a location update in that it alerts the system that the phone is once again reachable. On a cell-by-cell basis, the operator controls the activation of IMSI attach/detach. [38]

- Anonymity: Temporary IDs are used in 3G and GSM to offer anonymity. When a user turns on his or her device, a network user’s unique number (IMSI) is used to identify the MS to the network, and then a Temporary Mobile Subscriber Identity (TMSI) is issued and used to identify the MS to the network in future sessions. The network should always encrypt TMSI before sending it to the MS, according to the ETSI specification [38].

The MS receives a TMSI in response to a location update request. The TMSI is only useful within a specific geographic area. To offer an unambiguous identity beyond the location area, it must be paired with the LAI (location area identifier). As a location update request is given by the MS to the network, the TMSI reallocation is usually conducted at least once for each change
of a location region. The temporary identifier is used from then on. It is only feasible to establish
the temporary identifier used by tracing the user. [38]

**WLAN security implementation**

In the standard 802.11x, there are a variety of existing approaches and solutions for addressing
the security requirements of wireless networks. The majority of the solutions rely on encryption,
which has been shown to be a good approach to ensure acceptable security when correctly
implemented.

**WEP**

The IEEE 802.11x standard includes a security mechanism known as WEP (wired equivalent
privacy). It was created with the goal of providing confidentiality and authentication.

WEP provides confidentiality through the use of the RC4 stream cipher and the CRC-32
checksum for integrity. WEP was hacked in 2004 and isn't regarded secure anymore [33]. WEP
has two goals: the first is to prevent casual eavesdropping, and the second is to protect the
wireless network by discarding communications that have been poorly encrypted. Integrity
 checksums are used as a third purpose to avoid transmission manipulation. [40]

The RC4 cipher works by combining the public IV and the secret key into a pseudorandom bit
stream. The plaintext and the produced keystream are encrypted using an XOR14 operation
(indicated with a symbol in the diagram below). Decryption is accomplished by executing an
XOR operation on the IV, secret key to generate an identical keystream.

as well as the ciphertext When two messages are encrypted with the same IV and key, information about both messages is revealed [40]. WEP is widely seen as having failed to
achieve its security objectives.
Basic WEP encryption: RC4 key stream XOR with plaintext [40]

The RC4 cipher generates a stream of encrypted packets using a 40-bit key (also known as WEP-40) and a 24-bit initialization vector (IV) in standard 64-bit WEP. In later versions of WEP, the key size was extended to 104 bits in a 128-bit protocol named (WEP-104). [45]

A 128-bit key is entered by the user as a string of 26 hexadecimal characters in a 128-bit protocol. Four bits of the key are represented by each character. The final 128-bit WEP key is made up of 26 digits of four bits each, for a total of 104 bits. The IV is reserved 24 bits in a 256-bit WEP, while the other 232 bits are entered as 58 hexadecimal characters. [45]

Because of its numerous flaws, WEP should no longer be used for security purposes. WEP keys can be hacked in a matter of hours using software available on the Internet [44]. Another issue with WEP is the key management issue. WEP uses a single key for all users on a specific wireless network, making key protection problematic. WEP keys must be refreshed on a regular basis. WEP security cannot be achieved solely by increasing the key size. Longer keys necessitate more packet interruptions, but active assaults can circumvent this. [44]

• Authentication: There are two methods for authenticating users in WEP: Open System and Shared Key. The user does not need to send credentials to the Access Point during login because Open System authentication is a null authentication mechanism. Any user can authenticate with the Access Point and then attempt to associate, regardless of the WEP keys used. WEP can be used to encrypt data frames after authentication and association. The client must have the correct keys at this point. [45]
A four-way challenge-response handshake is used in Shared Key authentication:

- The user sends a request for authentication to the Access Point.
- The Access Point responds with a challenge in plain text.
- The user must encrypt the challenge text with the set WEP key and transmit it back as part of another authentication request. • The Access Point decrypts the material and matches it to the clear text it sent. The Access Point responds with a positive or negative response depending on the outcome of the comparison.

Knowing a plaintext/ciphertext pair of the required length can be used to deduce the keystream used for the handshake. Monitoring a legal authentication sequence is a pretty simple way to gather this information. [40]

**WPA**

Due to the failure of WEP, a new security protocol has to be developed immediately. WPA (WiFi Protected Access) was created as a stopgap measure to overcome WEP’s severe weaknesses. It was also necessary for WPA to work on existing hardware.

Using the Extensible Authentication Protocol, WPA improves network authentication (EAP). The CRC-32 checksum integrity code used in WEP was superseded by Michael, a message integrity code (MIC). The IV length was raised from 24-bits to 48-bits in WEP, and the Temporal Key Integrity Protocol (TKIP) added to the security. Other enhancements include the use of AES for stronger encryption. [51]

WPA can be utilized for personal use and small companies without the need for a complicated authentication server. This is known as Pre-shared key mode (PSK), and the shared key is a secret key that clients and the AP share. A 256-bit key is used by each wireless network device to encrypt network traffic. This key can be entered as a string of 64 hexadecimal numbers or as an 8 to 63 readable ASCII characters passphrase. PSK is frequently based on symmetric-key approaches, lowering WPA’s overall security level.
**Extensible Authentication Protocol (EAP)**

In WLAN networks, the EAP protocol is used to authenticate users. EAP supports a variety of authentication techniques known as EAP methods, which include password, certificate, and token authentication. It can also include a mix of authentication methods, such as a certificate followed by a password. As a result, rather than being a single authentication technique, it can be thought of as an authentication framework. [41]

**Key Integrity Protocol (TKIP)**

The TKIP protocol was created to improve security and address all known WEP flaws. One of the most essential design goals was to ensure compatibility with older WEP-based gear. The novel Message Integrity Check (MIC) provided by the keyed cryptographic method Michael is used by TKIP. Because of the design restrictions of being backward compatible, TKIP also implements several countermeasures to address security concerns. Replay attacks are not possible with TKIP. To protect against weak-key attacks, TKIP employs a cryptographic per-packet key mixing function that de-correlates the public initialization vector (IV) from weak keys. [40]

| Standard          | WEP          | WPA          | WPA2         |
|-------------------|--------------|--------------|--------------|
| Cipher algorithm  | RC4          | RC4          | AES          |
| Encryption key length | 40bits and 104bits | 128bits | 128bits |
| IV length         | 24bits       | 48bits       | 48bits       |
| Packet key        | Concatenated | Mixing function | Not needed |
| Data integrity    | CRC-32       | MIC          | CCMP         |
| Key Management    | Static       | EAS          | EAS          |
| Header Integrity  | None         | MIC          | CCMP         |
| Replay Attack     | None         | IV Square    | IV Square    |
**Table 1: 802.11 Security Protocols Comparison** [42]

**WPA2**

WPA was only intended to be a stopgap measure to remedy the WEP protocol's security flaws. WPA2, or Robust Security Network, was the name given to the entire protocol (RSN). WPA2 uses AES in counter mode with CCMP instead of the stream cipher RC4 used in WEP. WPA2 necessitates the purchase of new hardware [7].

![Cryptographic Algorithms](image)

**Fig 3 Robust Security Network (RSN)**

The RSN authentication and encryption techniques are a step toward making the 802.11x WLAN standards more secure. It provides security features that solve WEP and TKIP weaknesses and provide comprehensive data integrity and confidentiality protection for the wireless link. RSN is a wireless security network that permits the development of Robust Security Network Associations (RSNA), which are wireless connections that use a number of cryptographic techniques to ensure security threats in the WLAN network. [47] 3.12. The following are RSN's main security features:
• Replay protection • Enhanced user authentication procedures • Cryptographic key management
• Data confidentiality • Data origin authentication and integrity RSN adds new algorithms when a new danger is recognized, making it versatile by design. [47] 3.13.CBC-MAC CBC-MAC CBC-MAC CBC-MAC CBC-MAC (CCMP)

CBC-MAC, often known as CCMP, is a counter mode15 technique that includes the AES encryption used in WPA2. It protects data with 128-bit AES, which encrypts data in 128-bit packets using the block chaining1 (CBC) mode and ensures data integrity with a MAC16 (Message Authentication Code). A 48-bit IV is used by CCMP. Three factors make up the input to CCM mode:

- A payload consisting of authenticated and encrypted data
- A header, which is associated data, for authentication but not encryption
- A unique value called a nonce, assigned to the payload and the associated data.

**Encryption and Cryptography**

The quality of encryption and cryptography is essential for effective security procedures. It will be easier if you have a solid understanding of cryptography and how it works. We'll focus on the above-mentioned security techniques in this section. For more cryptography research, see [48].

The study of concealing information is known as cryptography. It is a strategy in which algorithms provide a security service to safeguard data integrity, ensure the validity of the data source, and provide data secrecy.

Confidentiality is provided through encryption techniques. They convert data, also known as a message or plaintext, into coded text, known as ciphertext, and prepare it for secure transmission over a network. An unauthorized entity will not be able to read the message this way. The message's recipient must have access to confidential information that is not available to the public. A key is the name for this secret. [49]

There are various types of encryption algorithms for various reasons; however, many other encryption algorithms are based on two major encryption techniques. Symmetric-key ciphers and
public-key (also known as asymmetric) ciphers are the two types of systems. Cryptanalysis is the study of breaking an encryption method or message.

**Figure 4: An Encryption Scheme Family tree [49]**

An encryption scheme consists of three algorithms in both symmetric and asymmetric schemes:

- A key generation method
- An encryption technique for converting plaintext to ciphertext
- A decryption algorithm for recovering plaintext from ciphertext [49]

**Cryptography's Objectives**

Confidentiality is a method of ensuring that information is only available to those who are allowed to see it [15]. Confidentiality is sometimes known as secrecy or privacy. Confidentiality can be achieved in a variety of ways, ranging from physical security to mathematical techniques that render data incomprehensible. A transaction on the Internet, for example, necessitates the transmission of personal information (such as account number and personal number, ID) from the buyer to the merchant across a public network. The system tries to keep this information private by encrypting it during transmission, limiting where it can appear (in databases, log files, backups, printed receipts, and so on), and restricting access to the storage locations. A breach of
confidentiality has occurred if an unauthorized party acquires the card number in any way. To prevent unwanted access to sensitive information, it must be encrypted. [15]

- Integrity: data integrity refers to the prevention of unlawful data change. There must be certain procedures in place to detect data tampering by unauthorized entities in order to ensure data integrity. When a computer virus infects a computer and manages to edit or delete some files, for example, integrity is compromised. Encryption aids in the verification of data's origin; changed data has a different source than the original. [15]

- Authentication: When we want to know where information or an entity came from, we use authentication. The two parties involved in a transaction or communication must be able to appropriately identify themselves to each other or to a third party. The information supplied across a channel should be validated in terms of its source, date of origin, data content, and time of transmission, among other things. Because of these factors, entity authentication and data origin authentication are the two most used types of cryptography. As previously stated, data integrity is implicitly provided through data origin authentication. [50]

**Symmetric Key Cryptography**

Symmetric-key Cryptography is an encryption process in which the sender and receiver use the same key.

**Cipher Blocks**

A block cipher is a symmetric-key encryption technique that divides the plaintext message into fixed-length bits or pieces (called blocks) and encrypts each block separately. Leftover fragments are padded to the appropriate block size, and each block must meet the prescribed size. The block cipher, for example, breaks a 38-byte frame into two 16-byte blocks and one 6-byte block if the predefined block size is 16 bytes per block. To match the 16-byte block size, the 6-byte block is padded with 10-bytes of padding18. [43

Block ciphers are used in many well-known symmetric-key encryption schemes. The Data Encryption Standard (DES), created by IBM and released as a standard in 1977, was an early and extremely significant block cipher design. Substitution ciphers, transposition ciphers, and
product ciphers, which combine the two, are three types of block ciphers. [48]

Figure 5: An Example of a Block Cipher
A stream cipher is a symmetric-key encryption system that can be thought of as very simple block ciphers with one block length. A stream cipher encrypts data by producing a keystream from the secret key and using the keystream to perform an XOR operation on the plaintext data. The keystream can be whatever size required to match the plaintext frame being encrypted. [43]

Figure 6: An Example of a Stream Cipher [43]
Stream ciphers can be thought of as an approximation of the one-time pad (OTP)\textsuperscript{19}, a known unbreakable cipher. Due to the difficulty of implementing an OTP system, a stream cipher employs a considerably smaller and more convenient key size, and stream ciphers use pseudorandomness.

Rather than using an OTP genuine random key, you can generate your own key. A stream cipher generates a pseudorandom keystream that may be coupled with the plaintext digits in the OTP in the same way. That is not to say that stream ciphers have the same level of security as an OTP encryption system, or even that they are secure at all.

**4G Wireless Security**

In the previous chapter, we reviewed the security of 2G/3G and WLAN networks, as well as how safe mobile transactions using these networks are. We also discussed various compromises that were mandated, as well as all of the remedies that were devised to increase the security of each network. Because the 4G network is fully operational in many parts of the world, security will play an essential role in this study. The security action on the 4G network is summarized here.

The security architecture for 4G LTE (Long Term Evolution) was created by 3GPP from the start, with security principles in mind and a design based on five security feature groups [57].

(i) Network access security, which ensures that the user has secure access to the service.

(ii) Network domain security, which safeguards network elements as well as signaling and user data transmission.

(iii) Controlling secure access to mobile stations through user domain security.

(iv) Application domain security, which allows for secure communication at the application layer.

(v) Security visibility and configuration provide the user with the ability to verify that security features are operational.
Security and Privacy in 4G/LTE Network, LTE network architecture [77]

4G/LTE Security Requirements

From a general perspective, the security architecture for 4G/LTE systems should be able to protect connections between UEs and MMEs, as well as between rudiments in landline networks and mobile stations, according to the following security standards.

(i) improved robustness over 3G

(ii) user identity confidentiality

(iii) strong user and network authentication

(iv) data integrity

(v) confidentiality, and

(vi) security interoperability with other radio networks

In any mobile device that uses 4G/LTE wireless technology, every connection between UEs and MMEs, as well as between all elements in the wireless network and mobile station, should be secured. The 4G/LTE security is greatly strengthened to meet these needs by introducing (1) advanced key hierarchy, (2) extended authentication and key agreement, and (3) supplemental interworking security for the NEs [77]. As detailed below, the requirements are divided into major building pieces and LTE end-to-end security [78].
The following ingredients are important building blocks:

Security and hierarchy are crucial.

The following are five important LTE techniques for connecting EPS and UTRAN: (1) non-access section (NAS) traffic between the UE and MME is protected with KANS encryption and veracity keys, (2) traffic between the UE and eNodeB is encrypted with KUP encryption, and (3) the Radio Resource Control (RRC) between the UE and eNodeB is protected with KPRC encryption and integrity keys.

Management positions of importance

The three functions of LTE key management are key establishment, distribution, and generation. Because mobile devices with IP-based infrastructure regularly contact different wireless networks, key management systems that prevent key theft are critical in 4G/LTE wireless technology. In 4G/LTE networks, the Authentication and Key Agreement (AKA) procedure is used to create and validate keys.

Protection from tampering, encryption, and integrity

In LTE, the authentication process is updated on a frequent basis by swapping sequence numbers in the encryption mechanism's message. While transmitting communication between LTE nodes, the IPsec protocol and tunnels are also utilized to declare the confidentiality of customers' data.

User identities that are one-of-a-kind

LTE has a variety of mechanisms for identifying and discouraging attackers from learning mobile user identities, making it difficult for them to launch DoS attacks or track mobile user profiles. The following are the identifier mechanisms: (1) international mobile equipment identification (IMEI), which is a permanent single identifier for each mobile, (2) M-TMSI, which is a temporary identifier that describes the UE inside the MME, and (3) C-RNTI, which is a single and temporary UE identity when a UE is coupled with a cell.
**LTE end-to-end security** encompasses the following elements:

**Authentication and Key Agreement (AKA)**

The AKA creates encryption and integrity keys that are responsible for originating multiple session keys, ensuring 4G/LTE security and privacy. The serving network authenticates a user's identity to the network, and the UE certifies the network signature through this method. LTE security is primarily concerned with authenticating UEs and wireless networks.

**Signaling confidentiality and integrity**

When the RCC and NAS layer signaling is appropriately encrypted and access control is integrity-protected, security is guaranteed. Crypturing and integrity protection are carried out at the Packet Data Convergence Protocol (PDCP) layer in LTE RCC. The NAS-layer, on the other hand, achieves security by encrypting NAS-level signaling. The above protective connections apply to every trusted UE connection between AGW and eNodeB.

**Confidentiality of user plane**

The user plane of LTE features a security feature that encrypts data/voice between the UE and the eNodeB. Between eNodeB and AGW, encryption is performed at the IP layer using IPsec-based tunnels, albeit no integrity protection is provided for the user plane due to performance and efficiency concerns. The PDCP layer is used to encrypt and decode the user plane while communication is being transmitted between the eNodeB and the UE.

**Discussion/Conclusions and Recommendations**

Here, we will focus solely on the issues raised in the previous sections of the presentation, draw an appropriate conclusion, and make recommendations. Some of the presentation's questions will be addressed, as well as the current market condition for mobile payment systems and their financial components.
Payments via mobile devices

Mobile consumers benefit from the development of new technologies and secondary execution; nevertheless, investors and service providers have yet to fully apply the process. The following are some of the reasons:

Adapting to new technology has become a significant issue. Users' familiarity with newly introduced technology is a challenge for marketers.

Though internet transactions, whether wired or wireless, are still relatively new, they are becoming more common. Because of their multiple advantages, wired transactions done at our houses cannot be restrained if we examine online payments and ignore other forms of transactions.

In comparison to others, they are less expensive.

In comparison to other types of devices, wired devices have fewer security risks. Wireless solutions face all of the same threats as wired systems, as well as additional threats.

Adaptability is not a concern because wired technology predates wireless technologies.

When compared to wireless, the average user is familiar with the security procedures of wired connections and devices.

Mobile payments are not suited for major transactions in their current condition because they lack adequate security.

Individuals in the information technology trade company are more exposed and threatened since the internet is a worldwide field where diverse types of people use it.

The fact that the transaction is taking place over a long distance is not a barrier to committing a crime. There is no international law enforcement agency capable of quickly prosecuting such perpetrators.
Technology

Is the number of functions provided by mobile solutions sufficient to satisfy the average customer?

The technology given by 4G is significantly faster than that offered by 3G in terms of data transmission speed. In the case of GSM, EDGE-enabled mobile handsets do not provide adequate speed. Taking into account the 802.11g standard, which has a download speed of 54 Mps. One of the most significant advantages of WLAN has always been data throughput. We have a highly diversified situation in terms of service range and coverage.

GSM networks that have been in use for a long time have the best service coverage and geographic distribution of base stations. In many countries where they are accessible, 3G networks are comparable to GSM in terms of coverage, although 4G has the least coverage of the three networks and has yet to be fully implemented in some.

Due to the high cost of switching one network to another, several countries have remained on the previous network, although with limited services.

| Features | 2G | 3G | 4G |
|----------|----|----|----|
| Standard | GSM, iDEN-MPS | WCDMA_CDMA 2000 | Single unified standard, ITU IMT Advanced |
| Data rate | 14.4kbps | 2Mbps | 100Mbps |
| Services | Digital voice, Short Messaging | High-quality audio, video, data | Dynamic information access with higher multimedia quality, wearable devices |
| Technology          | Digital cellular | Broad bandwidth | Unified IP, IP, CDMA, IP technology, seamless combination of broadband, LAN/WAN/PAN, WLAN |
|--------------------|------------------|-----------------|----------------------------------------------------------------------------------|
| Core network       | PSTN             | Packet Network  | Internet                                                                         |
| Multiplexing       | TDMA, CDMA       | CDMA            | CDMA                                                                              |

Security and Privacy in 4G/LTE Network, Table 3: Characteristics of 2G, 3G, and 4G technologies.

**Security**

The security requirement of a user's privacy is one element that motivates an ordinary user of mobile payment systems.

The news of worldwide cyber-crime has made users of technology, particularly the average user, more cautious. We need to trust that personal information shared over the internet will not end up in the wrong hands.

Network Analysis and Comparison

The goal of this project is to assess the security of various wireless networks used in business transactions. According to the findings, as the generation of networks grows, security flaws that could be a deterrent to mobile users improve.

2G, 3G, WLAN, and 4G are the different types of wireless connections. Although GSM was designed to be a more secure communication channel than prior analog voice transmission, it was discovered that GSM traffic was not as safe as planned. This isn't to say that GSM can't be used for successful business transactions; all it takes is someone with a good understanding of
the network's design to break into it for bad purposes. The secret COMP128 algorithm, which is used for authentication and encryption in GSM, was discovered and cracked by the United States. As a result, businesses should choose 3G and WLAN, which will provide better results than a 2G network. When comparing 3G and 4G networks, however, the shortfall of 3G networks is evident; it just isn't fast enough, giving 384kbps for users on the move and 2mbps if they are stationary, which falls short of what the end-user has grown to expect these days. Some regard 3G as a stopgap until a fully integrated IP network emerges that can provide speeds of 100mbit/s to 1Gbit/s both indoors and outdoors, with premium quality and strong security. As previously said, whether the network is fast or slow, our main concern is that 4G networks provide significantly better security than 3G networks.

The issue isn't that wireless solutions are fully unsafe; no solution is. There is no such thing as complete security, and this holds true for all systems, whether they be mobile payment systems, medical systems, or military systems. For a medical system to be acceptable, it would need to have a very high level of security and fail tolerance. For mobile payments, not losing our personal information is an acceptable level of security.

Conclusions

It's time to draw some conclusions after evaluating security requirements, issues faced by each network, and discussing the findings:

The existing market position for mobile payments is less than what investors and service providers projected prior to network implementation. There are a number of reasons behind this, including user reception, mobile transaction costs, and the availability of other traditional alternatives.

Is there a good level of security in a mobile payment system for the ordinary user? Yes, but only in terms of user awareness. Many threat attacks can be averted if the user is aware of the dangers and understands the security systems at work. Time and effort invested in learning the most significant components of security involved in a certain system result in a better overall experience and future time, effort, and money savings.
In terms of technology and available functions, the current state of mobile devices still has potential for advancement in order to meet user demands.

During the transition from 1G to 4G, security protection has advanced significantly.

However, our research shows that the combination of using an open IP-based design and the sophistication of security hackers means that security vulnerabilities in 4G networks remain a major worry. Analyzing security concerns in 4G wireless, as well as the rapid development of solutions for attack detection and mitigation, require special attention.

Recommendations

Because security is a never-ending job, all hands must be on deck to improve mechanisms as the network evolves, and hackers worked diligently to undermine the fundamental notion of these networks.

One strategy is to focus on a single network and explain its components, security procedures, and threats in detail. Another strategy is to focus solely on security assaults, explain them in detail, and conduct actual tests to validate their outcomes.

In schools, hospitals, banks, government parastatals, and commercial institutions, adequate attention should be paid to the research of the security of mobile payment networks to inform people about the risk involved in accessing messages sent to you by any of these devices.

To avoid a fraudulent act, services for keeping a financial database of any corporation should be contracted with a proper business agreement.

Adequate attention should be given to the study of security of mobile payment networks both in schools, hospitals, banks, government parastatals and private institutions to intimate people on the risk involved in accessing messages sent to you through any of these devices.

In the case of managing financial database of any organization, such services should be contracted with a good business agreement to avoid fraudulent act.
Abbreviations

3GPP: 3rd Generation Partnership Project
AES: Advanced Encryption Standard
AP: Access point
ATM: Automated Teller Machine
CDMA: Code Division Multiple Access
CKK: Complementary Code Keying
EDGE: Enhanced Data rates for GSM Evolution
GPRS: General Packet Radio Service
GPS: Global Positioning System
GSM: Global System for Mobile Communications
HSPA: High Speed Packet Access
IEEE: Institute of Electrical and Electronics Engineers
IMS: IP Multimedia Subsystem
IP: Internet Protocol
LTE: Long Term Evolution
MITM: man-in-the-middle attack
PCMCIA: Personal Computer Memory Card International Association
PGP: Pretty Good Privacy
PIN: Personal Identification Number
PRNG: Pseudo-Random Number Generator
RNG: Random number generator
SIM: Subscriber Identity Module
SMS: Short Message Service
SSL: Secure Socket Layer
TLS: Transport Layer Security
UMTS: Universal Mobile Telecommunications System
VPN: Virtual Private Network
WAP: Wireless Application Protocol
WEP: Wired Equivalent Privacy
WiMAX: Worldwide Interoperability for Microwave Access
**WLAN:** Wireless Local Area Network  
**WPA:** WiFi Protected Access  
**AAA** Authentication Authorization and accounting

---

**List of Reference**

1. Tiwari, R., Buse, S., and Herstatt, C: From Electronic to Mobile Commerce: Opportunities through Technology Convergence for Business Services, in: *Asia Pacific Tech Monitor, Vol. 23, No. (Issue: Sept-Oct. 2006), pp. 38–45, New Delhi.*, p.40 [1]

2. Saylor, Michael (2012). *The Mobile Wave: How Mobile Intelligence Will Change Everything.* Perseus Books/Vanguard Press. p. 202; 304. ISBN 978-1593157203 [2]

3. "Redirecting". www.mcel.co.mz. Retrieved 2017-08-23.[3]

4. "Ericsson launches mobile phone banking services". Reuters.com. Retrieved 2012-12-16.[4]

5. 1. A.Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, 1996, CRC Press. [5]

6. https://www.ptsecurity.com/ww-en/about/news/286211/ [6]

7 Ahmed Ali A study of security in wireless and mobile payments LiTH-ISY-EX--10/4157--SE 2010-06-30 [7]

8.https://www.mobilepaymentstoday.com/articles/the-problems-weighing-down-mobile-payments/ april 26, 2016

9. Yong Li, Yin Chen, and Tie-Jun MA, “Security in GSM”, Retrieved March 18, 2008, from http://www.gsmsecurity.net/gsm-security-papers.shtml.

10. N. T. Trask and M. V. Meyerstein, “Smart Cards in Electronic Commerce”, A SpringerLink journal on BT Technology, Vol. 17, No. 3, 2004, pp. 57-66.

11. N T Trask and S A Jaweed, “Adapting Public Key Infrastructures to the Mobile Environment”, A SpringerLink journal on BT Technology, Vol. 19, No. 3, 2004, pp. 76-80.

12. Korotayev A., Zinkina J. On the structure of the present-day convergence. *Campus-Wide Information Systems. Vol. 31 No. 2/3, 2014, pp. 139-152*

13. Kumar, Ravi, Comparison of Current On-line Payment Technologies, 2006, [13]
14. A.Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, 1996, [14]
15. Definitions from Wikipedia, http://en.wikipedia.org, Link [15]
16. Passive & Active Attacks Against Wireless LAN’s, Mohteshim Hussain, University of Hertfordshire, England, UK, [16]
17. "Ericsson Money Services brings connected mobile money to Europe". Ericsson.com. Retrieved 2012-12-16.[17]
18. Vacca John, Loshin Peter, Electronic commerce 4th edition, 2002, Charles River Media, [18]
19. Tan, Koontorm Center. "Phishing and Spamming via IM (SPIM)". Retrieved December 5, 2006.[19]
20. Kumar, Ravi, Comparison of Current On-line Payment Technologies, 2006, [20]
21. Baker, Emiley; Wade Baker; John Tedesco (2007). "Organizations Respond to Phishing: Exploring the Public Relations Tackle Box". Communication Research Reports. 24 (4): 327. doi:10.1080/08824090701624239[21]
22. "Millersmiles Home Page", Oxford Information Services. Archived from the original on July 21, 2007. Retrieved January 3, 2010. [22]
23. Aleksandar Tudzarov,Toni Janevski “Functional Architecture for 5G Mobile Networks”, International Journal of Advanced Science and Technology Vol. 32, 2011.[23]
24. Aman Aryaputra, Bhuvaneshwari.N, “5G- The Future of Mobile Network”, in the proceedings of the World Congress On Engineering and Computer Science 2011, Vol II,WCECS 2011, October 19-21, 2011.[24]25. Nascimento, Andrea, et al. "A characterization of mobility management in user-centric networks", Smart Spaces and Next Generation Wired/Wireless Networking. Springer Berlin Heidelberg, pg.314-325, 2013.[25]
26. Federico Boccardi, Robert W. Heath Jr., Angel Lozano, Thomas L. Marzetta, Petar Popovski “Five Disruptive Technology Directions for 5G”, IEEE Communications Magazine, 2014.[26]
27. Findahl, Olle, Svenskarna och Internet, 2009, World Internet Institute, [27]
28. Yousef, Paul, GSM-security: a survey and evaluation of the current situation, 2009, [28]
29. Feig, Nancy (2007-06-25). "Mobile Payments: Look to Korea". Banktech.com. Retrieved 2011-09-19.[29]
30. Adesina, A.A and Ayo, C.K. (2010). An empirical investigation of the level of user’s acceptance of e-banking in Nigeria. Journal of Internet Banking and Commerce 15: 1-13

31. IJRIT International Journal of Research in Information Technology, Volume 3, Issue 5, May 2015, Pg. 421-427 Adnan Majeed, IJRIT-423 [31]

32. www.businessdayonline.com [32]

33. "Tokenisation : What's next after PCI?" (PDF). indiamicrofinance.com. Retrieved 2017-01-07.[33]

34. "FRB: Current Use of Mobile Banking and Payments". Federalreserve.gov. 2013-08-02. Retrieved 2017-01-07. [34]

35. "Gartner: Over $172B In Mobile Payments In 2012; SMS, Web Most Popular Routes". TechCrunch.com. 2012-05-29. Retrieved 2017-01-07. [36]

36. Sattarova Feruza Y. and Prof.Tao-hoon Kim Privacy, Protection, Access Control, Assurance and System Security Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007[36]

37. Yousef, Paul, GSM-security: a survey and evaluation of the current situation, 2004, [37]

38. Gollmann, Dieter, Computer security 2ed, 1999, John Wiley & Sons, [38]

39. Brumley, Billy, A3/A8 & COMP 128, Helsinki University of Technology, 2004,[39]

40. Borisov, Nikita & Goldberg, Ian & Wagner, David
http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf,[40]

41. http://en.wikipedia.org/wiki/File:Wep-crypt-alt.svg[41]

42. Multiple authors, Handbook of wireless local area networks, 2005,

43. IEEE standards 802.11i, 2004, site: http://standards.ieee.org
44. Rao, K. Ramamohan (Kamisetty Ramamohan), Wireless multimedia communications, 2009,

45. Maxim, Merritt, Wireless security, 2002,

46. Halvorsen, Finn Michael & Haugen, Olav, Cryptanalysis of IEEE 802.11i TKIP, 2009, [40]

47. Frankel, Eydt, Owens and Scarfone, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, National institute of standards and technology, 2007,

48. Wobst, Reinhard, Cryptology unlocked, 2007, John Wiley & Sons,

49. http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm

50. "Web Proforum Tutorials." International Engineering Consortium. Retrieved from http://www.uky.edu/~jclark/mas355/WAP on 3/21/2017.

51. "An Undirected Attack Against Critical Infrastructure" (PDF). United States Computer Emergency Readiness Team (Us-cert.gov). Retrieved 28 September 2014.

52. "Defining Malware: FAQ", technet.microsoft.com. Retrieved 10 September 2009.

53. Gostev, Alexander, Mobile Malware Evolution: An overview Part 3, Kaspersky Labs, 2009, http://www.securelist.com/en/analysis?pubid=204792080

54. Thuraisingham, Bhavani M, Database and applications security : integrating information security and data management, 2005,

55. CNSS Instruction No. 4009 dated 26 April 2010

56. "Mobile payment apps – a fresh perspective on online finances". February 2014

57. 3rd Generation Partnership Project, "TS 33.401: System Architecture Evolution (SAE); Security architecture. Network, ver.11.2.0, release 11.," 3GPP, 2011.

58. N. Seddigh, B. Nandy, R. Makkar J.F. Beaumont Security Advances and Challenges in 4G Wireless Networks 2010 Eight Annual International conference on privacy, security and trust
59. ITU-R M.1645: Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000
60 “UMTS LTE Network Architecture”, Technical specification TS 23.002, version 8.4.0 (Release 8), 3GPP
61 Zhang and Y. Fang, “Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol”, IEEE Transactions on Wireless Communications, Vo. 4, No. 2, March 2005
62. M. Shin, A. Mishra, J. Ma, and W. Arbaugh, “Wireless Network Security and Interworking”, The Proceedings of IEEE on Cryptography and Security 2005
63. http://www.securityfocus.com/news/10271
64. http://www.igr-inc.com/html/downloads/free_white_papers/3G_MobileSecurity_Jan07.pdf
65. Definitions from Wikipedia, http://en.wikipedia.org
66. R. Baldemair et al., “Evolving wireless communications: Addressing the challenges and expectations of the future,” IEEE Veh. Technol. Mag., vol. 8, no. 1, pp. 24–30, Mar. 2013.
67. T. Rappaport, Wireless Communications: Principles and Practice. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.
68. T. Halonen, J. Romero, and J. Melero, Eds., GSM, GPRS and EDGE Performance: Evolution towards 3G/UMTS. New York, NY, USA: Wiley, 2003.
69. J. G. Andrews, A. Ghosh, and R. Muhamed, Fundamentals of WiMAX. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007.
70. B. Furht and S. A. Ahson, Eds., Long Term Evolution: 3GPP LTE Radio and Cellular Technology. Boca Raton, FL, USA: CRC Press, 2009, ch. 12, pp. 441–443.
71. S. Sesia, I. Tou_k, and M. Baker, Eds., LTE: The UMTS Long Term Evolution. New York, NY, USA: Wiley, 2009.
72. K. R. Santhi, V. K. Srivastava, G. SenthilKumaran, and A. Butare, “Goals of true broad band's wireless next wave (4G_5G),” in Proc. IEEE 58th Veh. Technol. Conf., vol. 4 Oct. 2003, pp. 2317–2321.
73. C.-X. Wang et al., Cellular architecture and key technologies for 5G wireless communication networks,” IEEE Commun. Mag., vol. 52, no. 2, pp. 122_130, Feb. 2014.
74. M. Fallgren et al., Scenarios, Requirements and KPIs for 5G Mobile and Wireless System, document ICT-317669-METIS/D1.1, Apr. 2013.

75. Industry Proposal for a Public Private Partnership (PPP) in Horizon 2020 (Draft Version 2.1), Horizon 2020 Advanced 5G Network Infrastructure for the Future Internet PPP. [Online]. Available: http://www.networks-etp-eu_/leadadmin/user_upload/Home/draft-PPP-proposal.pdf

76. Yongsuk Park, Member, IEEE, and Taejoon Park, Member, IEEE A Survey of Security Threats on 4G Networks 2007

77. Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert JP (2015) Practical attacks against privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:151007563

78. Seddigh N, Nandy B, Makkar R, Beaumont JF (2010) Security advances and challenges in 4G wireless networks. In: 2010 eighth annual international conference on privacy security and trust (PST). IEEE, Ottawa, ON, pp 62–71