An Android Mobile App for Highlighting Security Vulnerabilities in Whatsapp

Iyobor Egho-Promise[1], Isaac Owusu Amoako[2], Jonathan Tamakloe[3], Bamidele Ola[4]

Regional Technical Head, North/BA Regions, GloMobile, Tamale,Ghana[1]

Systems Analyst, EAI Information Systems, Accra, Ghana[2]

Head, IT Dept, Zelus Technologies, Accra, Ghana[3]

Managing Consultant, Technobeacon Consulting Ltd, London, UK[4]

ABSTRACT: In recent times, benefits such as ease of use, ubiquity, widespread prevalence has led to increase in the use of WhatsApp messaging application both for personal and official communication. WhatsApp, since its inception has grown into a global phenomenon, becoming one of the most popular mobile applications (apps) in the world today. With over a billionusers, WhatsApp provides a service that potentially endangers the security and privacy of a significant segment of the human population. In order to address these security concerns, WhatsApp offered full end--to-end encryption (E2EE), which implies all messages, calls, and files, both in a one-on-one and group setting, are potentially secure end to end. This research paper highlights certain security vulnerabilities in WhatsApp web version which can allow an attacker to remotely access the WhatsApp messages of victims. In this research, we developed an android based mobile app that can be used to clone victims WhatsApp application and provide recommendations to remediate this security vulnerability.

KEYWORDS: WhatsApp, security, vulnerability, cloning, man-in-the-middle attack, encryption

I. Introduction

WhatsApp [9], since its inception six years ago, has quickly grown into a global phenomenon, becoming one of the most popular mobile application worldwide as of today. With over a billion users Statt [11], WhatsApp provides a service that can potentially endangers the security and privacy of a significant proportion of the human population. In order to allay fears over security concerns, WhatsApp offers full end-to-end encryption (E2EE), meaning all messages, calls, and files, both in a one-on-one and group setting, are potentially secure from malicious attackers. The introduction of WhatsApp Web (which allows the user to access WhatsApp via a desktop web browser), has led to some potential security vulnerabilities, which is the focus of this study.

The scope of this research is to develop a third-party mobile app "*Whats Peep*" to clone WhatsApp conversations in order to demonstrate security vulnerability in WhatsApp web version. The research targets only Android Operating Systems. The research excludes Apple iOS and other operating systems. This research aims at broadening the knowledge of social media users especially WhatsApp platform on security issues and make them aware of the risk of leaving their mobile devices unattended

The objectives of this research include:

1. Create a third-party Android app to clone WhatsApp chats.
2. Scan WhatsApp`s QR code from the app.
3. Provide recommendation to address the vulnerability.

The problem statement of this research includes highlighting a vulnerability associated with using WhatsApp Web version, which can occur should a malicious attacker have physical access to a potential victim's device. This vulnerability will allow the malicious attacker to deploy a man-in-the-middle attack on their victim to access and gain control of WhatsApp chats.

The research question is: how can WhatsApp web conversations be secured against the security vulnerability highlighted in this research?

The limitation of this research was due to time and resource constraints, only the WhatsApp running on Android operating systems was used in this research.

II. LITERATURE REVIEW

WhatsApp is a popular cross-platform mobile applicationthat allows exchange of messages without payment for traditional mobile phone text messaging. There are an estimated 600 million users Statt [11], and it is uncommon that someone with a smartphone doesn't have this application on it. In the mobile messaging apps marketplace, WhatsApp consistently emerge as one of the most popular. In 2018, WhatsApp reported almost half a billion daily active users, and has been downloaded and installed by over a billion people worldwide. According to [12], WhatsApp provides fast, simple, and secure services at no cost, allowing users to send text messages, voice messages, pictures, documents and other files as well as place voice calls and video calls to other WhatsApp users, it is expected that the unstructured data generated by WhatsApp alone will double in volume within the next 4 years.

This paper discusses WhatsApp security architecture and carries out an analysis of its constituent protocols. We also carried out a literature review of articles on WhatsApp and related concepts, to gain better understanding of the working of the application and its security protocols. Althoughthe WhatsApp mobile version is a very popular app, its computer desktop version, according to [13], is accessible via a web browser or by installing an app for the windows or Apple Mac OS platform, a phone number is required as the primary identification of a user, hence the QR code need to be scanned to authorize the computer.

We also took a closer look at the app security and the measures to put in place to make it stronger without compromising usability. In the following sections, we cover some important security concepts applicable to WhatsApp, understand and evaluate the security architecture, measures taken to ensure user privacy and make recommendations to overcome the security attack.

A. *SECURITY FUNDAMENTALS*

End-to-End Encryption*:* According to [13], end-to-end encryption allows only the communicating parties to access the messages because the medium is encrypted. In theory, according to [13], no eavesdropper can access the cryptographic keys that are required to decrypt a conversation including but not limited to: law enforcement agencies, mobile telecommunications companies, internet service providers, and mobile app developers. An adversary may not be able to access the data transmitted, even after intercepting the traffic, this is feasible because of various properties of the encryption protocols used for making the end-to-end communication encrypted are inaccessible to an unauthorized user [13]. In figureII.A1below, the communication channel between the two phones or computers is encrypted.

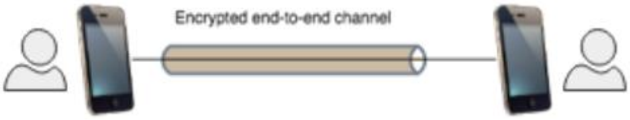


Figure II. A1: E2E encryption between two smartphones.

Signal Protocol: according to [13], enables end-to-end encryption in WhatsApp and used to encrypt both text messages and voice calls using an asynchronous method using a shared key. This protocol isused because it supports plausible deniability and forward-secret asynchronous communications on mobile devices [7].

Plausible Deniability: Deniability or repudiation entails that a message receiver knows the origin of a message but cannot explicitly ascertain the sender’s identity. In effect, the sender can deny being the person who originally sent the message [8]. Signal protocol uses a compact derivative of the Off-the-Record (OTR) protocol to enable this feature. Each participant in a WhatsApp conversation has a long-term identity key that they use to sign an ephemeral key. This ephemeral key is exchanged among members to calculate a shared secret, typically using Diffie–Hellman (D-H) key exchange method. D-H allows the participants to jointly establish a shared secret key, which can then be used to encrypt subsequent communications.

Forward Secrecy: This covers situation in which a user’s mobile phone or desktop encryption keys are compromised, a new key will be generated for every new message, this prevents a malicious actor from deriving the ephemeral keys and using the key to decrypt any previously transmitted message [13]. Signal Protocol according to [13], uses these keys below:

- Identity key pair, a long-term Curve25519 key pair generated at installs time for all asymmetric cryptographic operations.
- Signed pre-Key, a medium term Curve25519 key pair.
- Pre-Keys, also Curve25519 keys but for one-time use. These are used to encrypt the message.

B. *SECURITY ARCHITECTURE*

Every WhatsApp user, according to [13], have a long-term key stored on the memory of their mobile phone or desktop, not immediately accessible to the user, this key is used to create another shared key which a WhatsApp user can securely use to communicate with other user, thereby establishing a secure communication channel between the two users, and this does not change, except one of the parties reinstall WhatsApp or change their device. The following steps (1 to 7)below, describe the key management in the flow diagram shown in Figure II.B1. The initiating client is referred to as the‘initiator’, while he requesting client is the ‘recipient’.

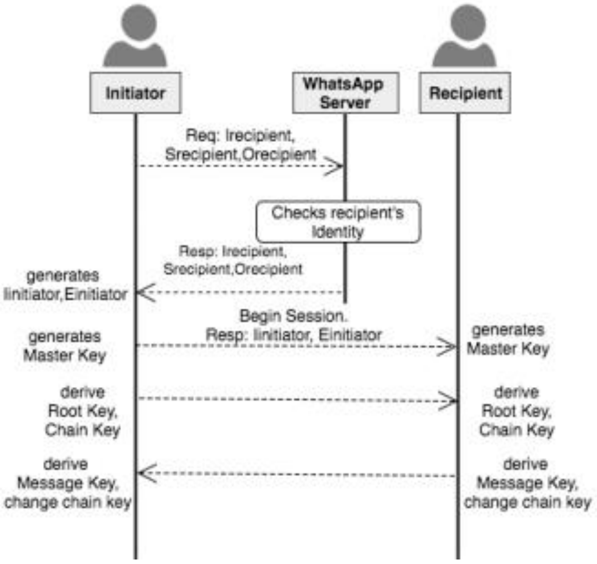

Initiator
WhatsApp Server
Recipient
Req: Irecipient, Srecipient,Orecipient
Checks recipient's Identity
Resp: Irecipient, Srecipient,Orecipient
generates Iinitiator,Einitiator
Begin Session. Resp: Iinitiator, Einitiator
generates Master Key
generates Master Key
derive Root Key, Chain Key
derive Root Key, Chain Key
derive Message Key, change chain key
derive Message Key, change chain key

Figure II.B1: Flow diagram of WhatsApp end-to-end encryption

1. The first step is for the message initiator to request these 3 public keys values: identity key (Irecipient), signed pre-key (Srecipient), single use pre-key (Orecipient) for the message recipient, all these 3 different keys should are generated when a WhatsApp is installed or reinstalled on an existing user device.
2. In the second step, WhatsApp Server retrieves the required public key values to the end client making the request.
3. During the third step, the message initiator will save the public keys earlier requested and subsequently generate a transient key (Einitiator) and loads its identity key (Iinitiator).
4. In the fourth step, the earlier keys generated and requested are now used by the message initiator to compute a shared master key with the message recipient, this shared master key is then used to generate session keys between the two communicating entities.
5. In the fifth step, the WhatsApp servers connects to the message recipient using the member id and then send session information with the initiator (Einitiator, Iinitiator).
6. In the sixth step, the message recipient uses the session information and the shared master key to ascertain message integrity and then delete the single use pre-key (Orecipient).
7. In the final step, the chains generated from the earlier steps are used by the various entities to create an 80-byte key. Using the chain keys generated in previous steps, parties involved in the conversation generate a message key of 80-byte value, which is used to encrypt the message and subsequently advance the chain-key forward step-wise thereby resulting in forward secrecy, any time a message is sent during any session. The design is the chain key will change with every subsequent message, thereby creating the same effect as forward message encryption.

C. *SECURITY AND PRIVACY EVALUATION*

Signal Protocol help mitigate the likelihood of man-in-the-middle attacks (MITM) to a large extent because of the forward secrecy mechanism. If for any reason, a malicious actor is able to decrypt the channel which will be computationally intensive and time consuming, the integrity of the encryption keys can be tracked backwards to the initial shared key. This theoretically guarantees that no MITM attack will be computationally feasible on any of the keys generated afterwards. It is worthwhile to note that although WhatsApp secures messages in transit, the endpoints (Apple iPhones/iPads, Android based devices, etc) on which WhatsApp is installed may not necessarily encrypt data at rest using disk encryption solution.

D. *ANDROID INFRASTRUCTURE*

The Android architecture components, according to [14],include a collection of libraries that can be used to design and develop robust, scalable, testable, fail-safe, and maintainable apps as well asmanaging the user interface (UI) component lifecycle and handling data persistence.
The Android infrastructure implemented on mobile phone is to provide facilities to support and enhance communications, user interaction and also interface with external networks (i.e. the internet) to support the user's mandate which is active communication, teaching and learning; information sharing; online advertisement; friends and family members and strangers communication collaborations; and many others.

E. *ANDROID SOFTWARE STACK*

The Android software stack consists of applications, an operating system, run-time environment, middleware, services, and libraries, depicted in Figure II. E1 below. At every layer of the stack, and its corresponding elements within the layer, are tightly coupled and painstakingly tuned to support optimal application development and execution environment for mobile devices.

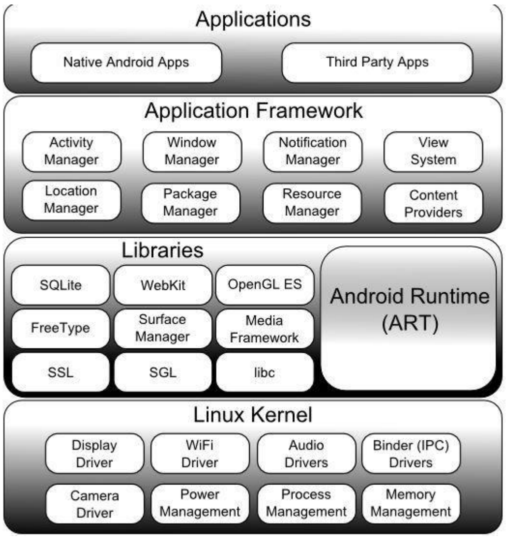


Figure II.E1: Android Architecture

F. *RELATED WORK*

WhatsApp has attracted a lot of attention, for pioneering large-scale usage of end-to-end encryption [13]. In the research literature, Bhatt and Arshad [3], carried out a sociological study on the impact of WhatsApp on youths, Cetinkaya [4], explored the impact of the use of WhatsApp in educating students and examined the opinions of students towards the process, while Church and de Oliveira [5] did a comparison of users behaviors between traditional phone text messaging and WhatsApp mobile Instant messaging, while Kumar and Sharma [6], carried out a survey of the impact and use of WhatsApp in some areas in India, Ali *et al.*, [1] carried out a comprehensive study about the levels and patterns of WhatsApp usage for official work communication using a case study of lecturers in some universities in Malaysia.
Our work is different from the earlier literature because, we focus on the various cryptography protocols that facilitate the security and privacy properties of WhatsApp and WhatsApp Web, so as to re-emphasize users trust in using mobile chat apps without worrying about privacy and security concerns.

III. RESEARCH METHODOLOGY

This study uses a quantitative research method because of its descriptive statistical advantages.
A total sample size of twenty (20) students were selected using a simple random sample method from a total population of fifty (50) from the computer science department of Koforidua Technical University. The total population was grouped into four (4) separate groups according to courses offered and 5 students were chosen from each group. Selection was done based on the number of years of experience of the students, which were categorized into no-

experience, low, medium or high. The method of collecting data in this study was the questionnaire and this was used because we needed a structured for collecting data and questionnaire seemed to be the right choice.
The questionnaire was designed by sending the respondents a set of questions which ranged from option A to D for them to indicate their choice. The questions asked composed of how the user used WhatsApp daily, how often the user updates the App, how often the user inspect his or her App Settings and whether the responder has a lock on his or her device. There was a total of ten questions in the questionnaire. 18 questionnaires were retrieved from the study giving a response rate of 90% and descriptive statistics was used to analyze the results.

IV. REQUIREMENTS ANALYSIS & SYSTEM DESIGN

Requirement is a statement that describes the functionality of a proposed system and the constraint on the system`s development, thus contributing towards the solution of the problem. The set of requirements represents a negotiated agreement among the stakeholders.

A. USE CASE DIAGRAMS

According to Sommerville [10], use case diagram identifies the functionalities provided by a system 'use cases', identifies the users who will interact with the system 'actor' and provides the relationship between users and use cases. A Use Case diagram for WhatsApp mobile is depicted in Figure IV.A1, while, Figure IV.A2 depicts a Use Case diagram for WhatsApp Web version.

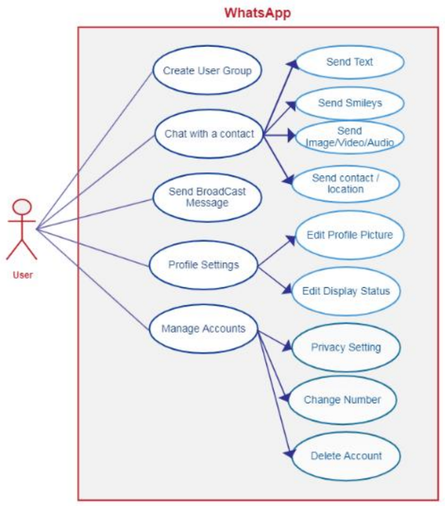


Fig. IV. A1: Use Case diagram for WhatsApp mobile

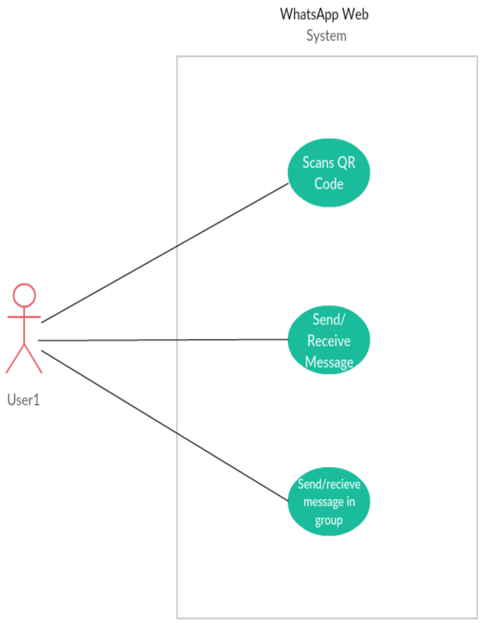


Fig IV. A2: WhatsApp web Use Case diagram

B. CHARACTERIZATION OF CURRENT SYSTEM

WhatsApp web connects directly to the WhatsApp server once the QR code has been scanned using the WhatsApp on the mobile. This serves as an authentication which initiate a handshake between the mobile device and WhatsApp server. This session is kept until the user logout from the App. Users can use WhatsApp main app and WhatsApp concurrently but cannot use the same WhatsApp Id in different concurrent sessions.

C. SYSTEM DESIGN

System design aims at transforming the requirements into complete and detailed system design. The system design is broken down into interface design, database design and process design. The User Interface Designs are depicted Figure IV.C1, Figure IV.C2, Figure IV.C3, and Figure IV.C4.

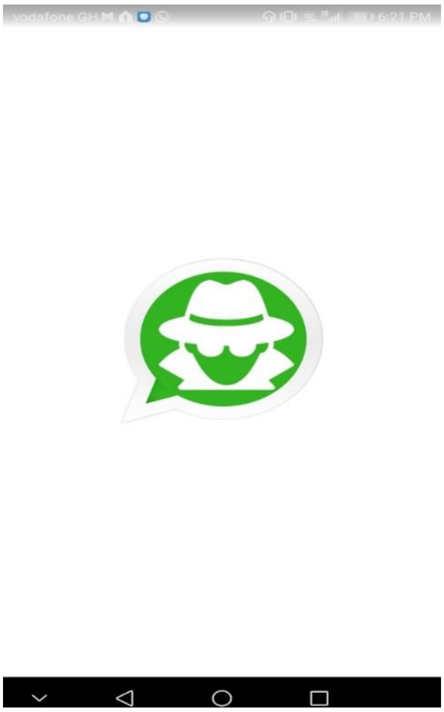
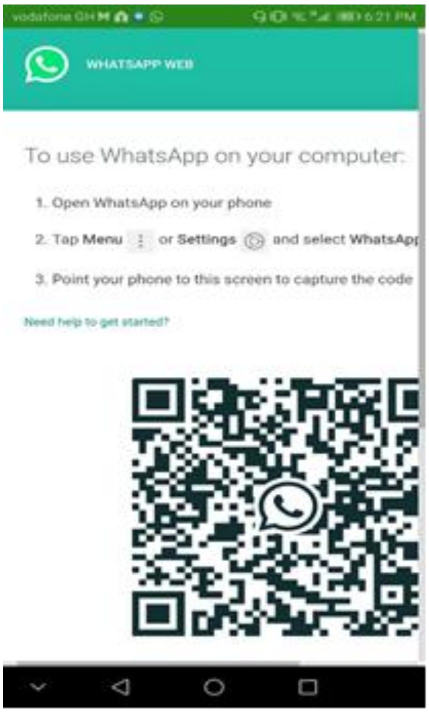


Fig IV. C1: Splash screen

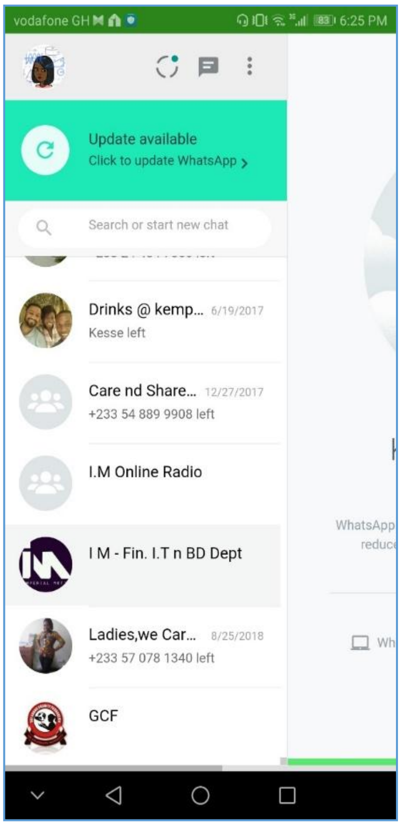


To use WhatsApp on your computer:

1. Open WhatsApp on your phone
2. Tap Menu ⋮ or Settings ⚙ and select WhatsApp
3. Point your phone to this screen to capture the code

Need help to get started?

Fig IV. C2: QR scan screen



Update available
Click to update WhatsApp >

Search or start new chat

Drinks @ kemp... 6/19/2017
Kesse left

Care nd Share... 12/27/2017
+233 54 889 9908 left

I.M Online Radio

I M - Fin. I.T n BD Dept

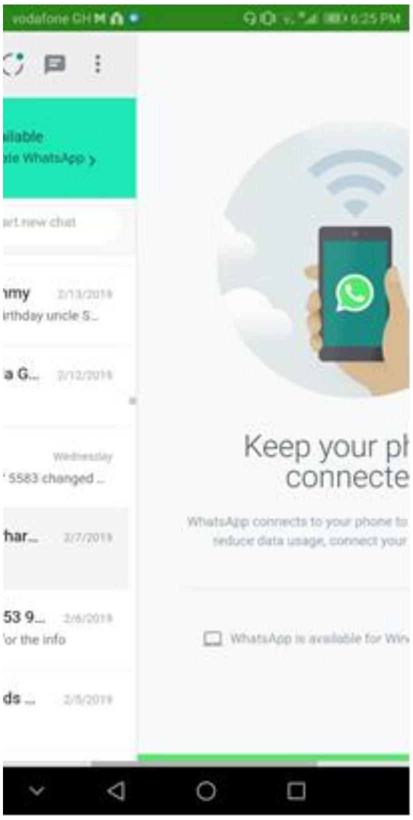
Ladies,we Car... 8/25/2018
+233 57 078 1340 left

GCF

WhatsApp
reduc

Wh

Fig IV. C3: Welcome screen



ilable
ate WhatsApp >

art new chat

ımy 2/13/2019
irthday uncle S...

a G... 2/12/2019

Wednesday
5583 changed ...

har... 2/7/2019

53 9... 2/6/2019
or the info

ds ... 2/5/2019

Keep your pl
connecte

WhatsApp connects to your phone to
reduce data usage, connect your

WhatsApp is available for Win

Fig: IV. C4: Chat window screen

V. IMPLEMENTATION

Xamarin.Forms for App: Xamarin.Forms is a cross-platform natively backed UI toolkit abstraction that allows developers to readily develop graphical UI that can run across Android, iOS, Windows, and Windows Phone.
Xamarin offers two commercial products: Xamarin.iOS and Xamarin. Android.
On iOS, the Xamarin's Ahead-of-Time (AOT) compiler can compile Xamarin.iOSsource code directly to assembly code. On Android, Xamarin's compiler initially compiles source code to Intermediate Language (IL), which is subsequently compiled to native assembly when the application launches.
In both cases, Xamarin applications uses a runtime that automatically allocate memory, collect garbage, and handle underlying platform interoperability.Xamarin applications are built against a subset of the .Net BCL known as the Xamarin Mobile Profile. This is similar to the way Silverlight (and Moonlight) applications are built against the Silverlight/Moonlight .NET Profile.
The Microsoft .Net framework provides tools and technologies required build networked applications, distributed web services, and web Applications. The .Net Framework provides the required compile-time and run-time framework necessary to build and run any language, the two keys are the Common Language Runtime (CLR) and .Net Framework Class Library (FCL).

A. *SAMPLE CODE*

MAinActivity.cs Code

```
using System;
usingAndroid.App;
using Android.Content.PM;
usingAndroid.Runtime;
usingAndroid.Views;
usingAndroid.Widget;
usingAndroid.OS;

namespaceWhatsPeep.Droid
{
   [Activity(Label = "Whats Peep", Icon = "@drawable/icon", Theme = "@style/MainTheme", MainLauncher = false,
ConfigurationChanges = ConfigChanges.ScreenSize | ConfigChanges.Orientation)]
publicclassMainActivity :global::Xamarin.Forms.Platform.Android.FormsAppCompatActivity

   {
protectedoverridevoidOnCreate(Bundle savedInstanceState)
      {

TabLayoutResource = Resource.Layout.Tabbar;
ToolbarResource = Resource.Layout.Toolbar;

base.OnCreate(savedInstanceState);
global::Xamarin.Forms.Forms.Init(this, savedInstanceState);
LoadApplication(new App());
      }
   }
}
```

MainPage.xaml Code

```
<?xml version="1.0" encoding="utf-8" ?>
<ContentPagexmlns="http://xamarin.com/schemas/2014/forms"
xmlns:x="http://schemas.microsoft.com/winfx/2009/xaml"
xmlns:local="clr-namespace:WhatsPeep"
x:Class="WhatsPeep.MainPage">

<AbsoluteLayout>
<WebViewx:Name="webView" Source="https://web.whatsapp.com"
AbsoluteLayout.LayoutBounds="0, 0, 1, 1"
AbsoluteLayout.LayoutFlags="All" />
</AbsoluteLayout>
</ContentPage>
```

Figure V.1: "Whats Peep" mobile app icon

VI. Conclusion

This paper highlights some security vulnerabilities in using WhatsApp web, utilizing Man-In-The-Middle Attack. The research looked at the basic structure of WhatsApp, the security encryption algorithms it uses, how WhatsApp Web uses QR Code for authentication and creates a session token and how a handshake is initiated to establish connection between WhatsApp`s servers and the web browser.

Finally, we created a mobile App "*Whats Peep*" (see Figure V.1) to demonstrate how an attacker can use a custom-built third-party app to sniff or spy on a victim`s WhatsApp conversations.

It is recommended that a user of WhatsApp should frequently be checking the list of connected devices to his or her phone and ensure all the unauthorized devices are log out immediately, this will prevent the WhatsApp conversations from being spoofed. Also, we recommend WhatsApp mandatorily enable its two-step verification setting by making "enable" the default option.

References

1. Ali, R. M., Mahomed, A. S.B, Yusof, R. N. R., Khalid, H., and Afzal, M. I., 'Hey there! I am Using WhatsApp: A Study on the Levels and Patterns of WhatsApp's Official Usage among Malaysian University Academicians', International Journal of Asian Social Science, Asian Economic and Social Society, Vol. 9, Issue 12, pp. 657-671, 2019.
2. Ansari, A. and Hasan, M., 'Use of social networking sites in library and information centers', National Conference Library Information Science & Information Technology for Education, pp. 84-89, 2015.
3. Bhatt, A. and Arshad, M., 'Impact of WhatsApp on youth: A Sociological Study', IRA-International Journal of Management & Social Sciences, ISSN: 2455-2267, Vol. 4, Issue 2, pp. 376-386, 2016.
4. Cetinkaya, L., 'The Impact of WhatsApp Use on Success in Education Process', The International Review of Research in Open and Distributed Learning, Vol. 18, Issue 7, 2017.
5. Church, K. and de Oliveira, R., 'What's up with WhatsApp? Comparing mobile instant messaging be-haviors with traditional SMS', Proceedings of the 15th ACM International Conference on Human-computer Interaction with Mobile Devices and Services, pp. 352-361, 2013.
6. Kumar, N. and Sharma, S., 'Survey Analysis on the usage and Impact of WhatsApp Messenger', Global Journal of Enterprise Information System, Vol. 8, Issue 52, 2017.
7. Ludwig K., 'End-to-End WhatsApp: An Opinionated Series on Why Signal Protocol is Well-Designed', 2016. Available at: https://www.praetorian.com/blog/whatsapp-end-to-end-encryption-why-signal-protocol-is-well-designed
8. Open Whisper Systems, 'Simplifying OTR deniability', 27 July 2013. Available at: https://whispersystems.org/blog/simplifying-otr-deniability/.
9. WhatsApp.com, 2019. Available at https://www.whatsapp.com/features/.
10. Sommerville, I., Software Engineering. 10th edition, Pearson, 2015.
11. Statt, N., 'WhatsApp has grown to 1 billion users', The Verge, 2019. Retrieved from http://www.theverge.com/2016/2/1/10889534/whats-app-1-billion-users-facebook-mark-zuckerberg

12. WhatsApp Records Capture - A Case Study.
Available at: https://www.dpconline.org/blog/idpd/whatsapp-records-capture
13. Nidhi, R. & James Hendler, J. "WhatsApp Security and Role of Metadata in Preserving Privacy."International Conference on Cyber Warfare and Security, Academic Conferences International, Jan. 2017, p. 269.
Android Architecture Components. Available at:https://developer.android.com/topic/libraries/architecture

BIOGRAPHY

Egho-Promise Ehigiator Iyobor (PhD) is an IT, Telecom & Management Consultant, Trainer and a writer with over 20 qualifications ranging from PhD ICT, M.Sc. IT, MBA, B.Sc. Computer Science, HND Accounting, HND Electrical/Electronic Engineering, CCNA, MCP, etc. He is currently the Regional Technical Head of Glo Mobile Telecommunications North/BA Regions. He researches Mobile Communications.

Isaac Owusu Amoako holds a Bachelor's degree in Information Technology (IT) from the Koforidua Technical University, Koforidua, Ghana and currently a Systems Analyst/Software Developer with EAI Information Systems in Accra, Greater Accra Region, Ghana

Jonathan Tamakloe holds a Bachelor's degree in Information Technology (IT) from theKoforidua Technical University, Koforidua, Ghana and currently, Head, IT Dept, Zelus Technologies in Accra, Greater Accra Region, Ghana.

Bamidele Ola is Managing Consultant of Technobeacon Consulting Ltd, a UK based Information Security consultancy. He has over 18 years corporate work experience in Information Security and is currently a PhD student in IT (Information Security specialty) at the University of the Cumberlands, Kentucky, USA. He researches Information Security, Software Engineering, and Machine Learning.