ASHESI UNIVERSITY COLLEGE

EVALUATION OF MOBILE NETWORK SECURITY IN GHANA

KPETERMENI TOQUOI SIAKOR

2015

Applied Project

ASHESI UNIVERSITY COLLEGE

EVALUATION OF MOBILE NETWORK SECURITY IN GHANA

By

KPETERMENI TOQUOI SIAKOR

Applied Project submitted to the Department of Computer Science,

Ashesi University College

In partial fulfilment of Science degree in Computer Science

2015

Declaration

I hereby declare that this applied project is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature:………………………………………………………………………

Candidate's Name:……………………………………………………………………………….

Date:………………………………………………………………………………………………..

I hereby declare that the preparation and presentation of the applied project were supervised in accordance with the guidelines on supervision of applied project laid down by Ashesi University College.

Supervisor's Signature:……………………………………………………………………..

Supervisor's Name:……………………………………………………………………………….

Date:…………………………………………………………………………………………………

Acknowledgements

I am grateful to God whose grace has enabled me to embark on this project and come to its completion.

I am particularly grateful to my supervisor, Dr. Suzanne Buchele, who despite her busy schedule, agreed to take me as her supervisee. I am grateful for the books and guidance that she provided me to enlarge my understanding of computer security.

I am also grateful to my family, my mentor Bridgette Sexton Beam, and the MasterCard Foundation without whose financial assistance, my education would not be possible.

To the hacker community especially members like Karsten Nohl whose work formed the foundation of this project, I am deeply grateful.

Abstract

Mobile technology is one of the most successful technologies on the African continent. Personal and professional communication as well as critical services like banking and remittances are widely made through mobile networks and platforms in Ghana. However, little is known about the security of the underlying infrastructure and devices consumers use to interact with the mobile network.

The focus of this project is to determine if the core systems of the mobile network operators, the technology infrastructure, and the 2G/3G dongles have exploitable security vulnerabilities, demonstrate some of those exploits, and make recommendations on how to mitigate or eliminate the risk of exploitation.

Contents

List of Figures

Chapter 1: Introduction

1.1 Introduction & Background to the Project

Mobile telecommunications has been hugely successful in bridging the communications gap in Africa. This success has made mobile networks the preferred delivery platform for a plethora of services. Traditional services like insurance, money transfers, and even critical services like emergency response services have been integrated with mobile technology. Mobile communications have also given rise to new services like branchless banking which allows banks to expand their reach without building new architecture

As dependency on mobile networks continues to grow, it is important to assess the security of the infrastructure and associated technologies that make-up the mobile ecosystem.

However, very little scholarly literature has been written on the security implications of using mobile networks and associated technologies for the many services they provide [1]. This paper is my contribution to the much needed body of literature on mobile network security in Ghana and by extension Africa.

1.2 Objectives

The primary objective of this paper is to determine the security and privacy that mobile subscribers can expect from their use of mobile networks.

The secondary objective of this paper is to provide a survey of the security mechanisms in force in the mobile ecosystem in Ghana.

1.3 Outline of Applied Project

Chapter 2 introduces the theoretical basis of mobile communications security and explores the works of other researchers on the topic of mobile network security. The chapter ends with the implications of the research findings on mobile network security in Ghana.

In Chapter 3, the focus is on the architecture of the mobile network and vendor-supplied mobile Internet equipment like 3G USB dongles. The chapter ends with a close look at the physical and logical architectures of SIM cards.

Chapter 4 delves into the practical assessments of mobile network security in Ghana through a multi-layered approach of exploiting perceived vulnerabilities across the mobile spectrum in Ghana. It details the tools and steps carried out to perform the exploits and documents the results.

Chapter 5 ties the theoretical concepts in mobile network security with the practical implementations of exploits and makes recommendations on what can be done to mitigate the risks.

Chapter 2: Background and Related Work

2.1 Chapter Introduction

In this chapter, I will discuss the theoretical basis of mobile communications security. I start with the broader definitions of computer security by discussing the CIA triad (confidentiality, integrity, and availability) and associated mechanisms and policies. Next, I narrow down to the literature about the mobile ecosystem in Ghana and Africa, the security of the mobile network channels, and the security of mobile devices using the CIA triad. Finally, I will discuss what these concepts assure consumers of when using mobile services in Ghana.

It is known that most of the papers that deal with mobile network security are not pure research papers, instead they are papers/presentation slides from hacker conferences. The ones that are pure research papers usually deal with the theoretical cryptanalysis of various ciphers [1]. In this chapter, I present both the theory and the practical implementations of mobile network security in Ghana.

2.2 Computer Security

Computer security is defined as "the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)” [2].

My focus will be on the application of computer security to mobile telecommunications with special attention to the security afforded consumers of mobile network services. As a result, many of my references will be to presentation slides and videos of conferences where the security of mobile networks and devices were tested.

2.2.1 Confidentiality

Confidentiality is defined as “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” [2]. Inherent in the definition are two concepts: data confidentiality and privacy.

Data confidentiality is the assurance that only those duly authorized have access to a specific body of information. Privacy is the assurance that individuals have control over information that is related to them and control over who that information is disclosed to.

I will be looking at the confidentiality of consumer information as well as system information to which only authorized consumers should have access to on a mobile network.

2.2.2 Integrity

Integrity refers to the "trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change" [3]. Integrity covers three concepts: data integrity, origin integrity, and system integrity.

Data integrity refers to the content of the information. It assures that "the information and programs are changed only in a specified and authorized manner" [2]. Origin integrity assures that the source of the data is authentic. System integrity assures that "the system performs its intended function in an unimpaired manner, free from deliberate rate or inadvertent unauthorized manipulation of the system" [2].

My focus will be on the system and origin integrity and whether consumers can trust that system information they receive is only from an authorized source.

2.2.3 Availability

Availability is defined as the assurance that "systems work promptly and service is not denied to authorized users" [2]. A breach of availability is the disruption of access to or the use of information or an information system" [2].

Evaluating breaches of availability are beyond the scope of this paper.

2.2.4 Policies and Mechanisms

The implementation of computer security requires certain policies and mechanisms. A security policy is defined as “a statement of what is, and what is not, allowed” whilst a security mechanism is defined as “a method, tool, or procedure for enforcing a security policy” [3].

2.2.5 Authentication and Access Control

One mechanism to enforce permission policies is access control. This refers to the ability to set limits on access to resources, devices, and application as well as control that access. A sub-mechanism that ensures that access controls work is authentication. By authentication, users are identified and given specific privileges on the computer system or network [2].

2.2.6 Sandboxing

When the concepts of access control are applied to applications by creating an environment where applications can execute predetermined actions and only within that environment, that environment is called a sandbox [3]. Sandboxes are useful for isolating applications where their interaction or unrestricted access may pose security risks.

2.3 The Ecosystem

The mobile landscape in Ghana is divided into two—the mobile network operators (MNO) and the Broadband Wireless Access (BWA) operators. The BWA licenses restrict the operators to rolling out fourth generation (4G) long term evolution (LTE) networks. MNO licenses are restricted to third generation (3G) and voice communications. The regulatory body in charge of mobile telecommunications is the National Communications Authority (NCA) [4].

2.3.1 Mobile Network Operators

Six mobile network operators (MNOs) representing regional and international corporations operate Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA) networks in Ghana [5]. MNOs have operated in Ghana since 1992 starting with first generation (1G) cellular communications and today are moving towards fourth generation (4G) technologies.

The state holds minority shares (30%) in the national carrier, Ghana Telecom Company (GT). GT has since been rebranded into Vodafone Ghana by majority shareholder, the Vodafone Group, with 70% shares [6]. Other operators are the Mobile Telecommunications Network (MTN), which is operated by the Scancom Ghana Ltd., a local subsidiary of the continental MTN Group [7]. Nigerian telecommunications giant, Globacom Ltd., operates the Glo mobile network [8] whilst Sudatel-owned Expresso Telecom, provider of the only CDMA network in Ghana, operates the Expresso mobile network [9]. The pioneer cellular network, Tigo, is operated by Millicom Ghana, a subsidiary of the Luxemburg-based Millicom

[10] whilst Indian international conglomerate, Bharti Airtel, operates the Airtel Ghana mobile network [11].

2.3.2 Broadband Wireless Operators

To encourage competition and overall quality of service in the mobile space in Ghana, the NCA reserved fourth generation (4G) network licenses for newcomers in the telecommunication space in Ghana. In 2011, the NCA issued licenses to three Ghanaian-owned companies authorizing them to roll out Long Term Evolution (LTE) networks in the country. The companies are Surfline Ltd, GoldKey Properties Ltd, and G-Kwiknet Ltd (now Blu Telecom) [12].

2.3.3 Subscribers, Coverage, and Availability

Mobile penetration in Ghana is set at 113% representing over 30 million subscribers in a country with a population of just over 26 million [13]. This is because individuals typically own multiple subscriber identification modules (SIM) cards at a time.

With over 13 million subscribers comprising over 45% of the market, MTN is the largest MNO in Ghana. This is followed by Vodafone (23%), Tigo (13%), Airtel (12%), Glo (4%), and Expresso (~0.4%) [13]. For the purpose of this paper, I will be focused on GSM networks as the CDMA operator (Expresso) accounts for less than 1% of the mobile market.

Combined, the MNOs provide comprehensive mobile coverage of inhabited places in Ghana at various degrees of signal strength and quality. For data communications, all MNOs provide third generation (3G) Internet services in urban centers. In suburban and rural areas, Internet connections often fall back to much slower second generation (2G) General Pack Radio Service (GPRS) or Enhanced Data rates for GSM Evolution (EDGE). This fallback has implications for the security of the communication channel as will be shown in Chapter 4.

The reliability of mobile networks, like their data provisions, vary from urban centers to rural communities. The NCA monitors the quality of service and hands out sanctions to defaulting operators.

2.3.4 Mobile Internet Devices

The growth of mobile penetration in Africa has been accompanied by increased sales of mobile devices for voice, text, and data communications. However, over 80% of mobile subscribers use basic phones without Internet capabilities. Only 11% of the total subscriber base use Internet on their phones. Of this number, half of them use smartphones which enables a richer Internet experience [14]. For the remaining majority, Internet access is possible through the use of 3G dongles for mobile Internet or fixed broadband. These dongles will be the targets of this paper’s security assessment

2.3.5 Operator Services

The services available from the mobile network operators range from short messaging service (SMS), unstructured supplementary service data (USSD), mobile money, mobile broadband, and value added services (VAS). Vodafone also provides fixed wireless and cable connections in addition to their mobile service whilst Airtel provides fixed wireless in addition to their mobile service.

2.3.6 Uses of Mobile Services

Besides the services operators offer consumers, mobile networks power everyday communication, health delivery, banking, education, e-commerce, and potentially the democratic process of elections. For example, rural dwellers get health-related information and health-worker training using mobile phones [15]. All major banks in Ghana provide mobile solutions to customers and schools use mobile networks everyday. In the 2012 election, voters were registered and verified using GSM-enabled biometric devices although I could not verify if the GSM feature was used [16]. There is also a rise in portable GSM-enabled point of service (POS) machines for payments-on-delivery.

2.3.7 Industry Partners

Other partners in the mobile industry are the Ghana Internet eXchange Association (GIXA), tower operators, mobile equipment vendors, and submarine cable operators. Equipment vendors like Huawei supply both internal MNO equipment and consumer devices. This project will look at some of these devices.

2.4 Existing Security Measures

2.4.1 SIM Card Registration

The law passed in 2008 requires that all existing mobile network subscribers register their subscriber identification module (SIM) cards to continue use [17]. It also requires that all new subscribers register their SIM cards upon purchase. This is aimed at assisting crime investigation and protecting the general public.

The national regulator, NCA, enforced this law by requiring MNOs to deactivate SIM cards that were not registered after a specified period of time whilst bearing the cost of the SIM registration process. The registration process requires a state-issued legal identification document like a voter ID card, passport, or driver’s license.

The mechanism chosen by the MNOs was to authorize mobile credit vendors to register subscribers after inspecting the above documents. The MNOs also maintained desks to cater to subscribers who walked into their offices to get their SIM cards registered. At the end of the year-long exercise, 17 million subscribers registered their SIM cards with 2.5 million subscribers outstanding who risked deactivation if they did not register in the 90-day grace period provided [18].

Sensing fraudulent activities during the 2011 registration exercise, the government of Ghana ordered a re-run of the SIM registration in 2014 [19]. MNOs have, however, been reluctant to carry out the re-registration exercise because of the costs involved. As at the time of this writing, the re-registration process has not begun. Later that year, the government gave a new directive restricting the number of SIM cards a person can register to 10 in an effort to combat SIM box fraud [20], however, I was unable to establish if this directive is in operation.

A further step to validate user registration is using the mobile money registration process. Even with a registered SIM card, government issued IDs are required for mobile money registration. The vendors of SIM cards are not necessarily mobile money merchants so this second layer of ID check improves the validation process.

A new development in the ecosystem is an effort by the government to validate subscriber registration using the proposed Interconnect Clearing House (ICH). The ICH will serve as the intermediary node through which all mobile traffic in the country are routed [21]. MNOs are resisting the implementation of the ICH on performance, security, and cost basis. The ICH is not in full operation at the time of this writing to allow me to study the security implications of routing all mobile traffic through one clearing house.

It has been argued, however, that there has not been sufficient debate on the impact of SIM card registration on consumers' privacy and whether it is creating surveillance states. In a paper on the emerging dynamics of SIM card registration regulations, Donavan and Martin argue that although the evidence is inconclusive, the security benefits of SIM registration are modest at best. For example, they found a weak link between SIM registration and crime detection in Tanzania [22].

2.4.2 Securing the Operator

It was not possible to study the full infrastructure setup at mobile network operator offices and base stations for this project. However, by studying the Internet-facing equipment at their offices, I gained some insights into the security that is deployed to keep their computer systems secure from external threats. In studying those devices, I did not attempt to break into their systems using any intrusion techniques, but simply looked out for devices that implemented default or no authentication on the services that were open to the public Internet.

A majority of the equipment studied implemented some form of authentication on their network equipment but for a few exceptions. The most secure devices are inaccessible from the public Internet, but rather require encrypted connections like virtual private networks to access them. These devices restricted access to only traffic from the internal network. The less secure devices had open ports configured with default or no authentication. This gives attackers total administrative control over those devices.

2.4.3 Securing the Channel

GSM mobile networks are secured using one or a combination of the A5 suite of ciphers that were first developed in the 1980s and have been improved over the years. The cipher suite comprises of stream and block ciphers for encrypting over-the-air traffic in mobile networks. These exact specifications of A5/0, A5/1, and A5/2 were developed and kept in secret until they were leaked [23]. Subsequent ciphers have been developed openly by the Third Generation Partnership Project (3GPP) comprised of members across the globe.

From A5/0 to KASUMI

The A5/0 cipher does not implement encryption. It was developed for export to countries with trade restrictions on encryption technology. The A5/1 cipher, however, became the standard for securing GSM data. The A5/1 is a stream cipher with a key size of 56 bits in standard implementations. The A5/1 cipher is used to secure communication over second generation (2G) networks.

The A5/2 cipher, like the A5/1 cipher, is a stream cipher that was intentionally weakened for export. However, barely a month after it was released, it was broken showing that the cryptanalysis required would be trivial [24]. Today, mobile networks are prohibited from implementing A5/2; instead, no encryption is implemented in the absence of stronger ciphers [25].

The A5/3 cipher was developed by the 3GPP to secure communications on third generation (3G) networks and to upgrade 2G network security. Also known as KASUMI, the A5/3 cipher is a block cipher that uses 128-bit key sizes [31]. The cipher can be implemented for GPRS and EDGE for securing user and signaling data over the air interface.

The f8 and f9 algorithms are improvements to the KASUMI cipher for ensuring confidentiality and integrity. The confidentiality algorithm, f8, is a stream cipher that uses a KASUMI-based key generator to encrypt/decrypt data blocks of sizes ranging from 1 to 20,000 bits in length [34]. The integrity algorithm f9 was designed based on the KASUMI block cipher for ease of implementation and compatibility with the f8. The f9 algorithm uses an integrity key to computer the message authentication code (MAC) on an input message [34].

2.4.4 Securing the 3G Dongle

Out of the box, 3G dongles are locked to the network provider. The software on the dongles are also modified to conceal their real names. In some cases, even the model of the dongle is modified to make it appear different. For example, Vodafone markets their Huawei E303s-2 dongle as Huawei K4201.

This makes it difficult to unlock as one cannot unlock a device based on a fake model. Whilst this does not provide any real security to either the consumer or the MNO, they protect some limited protection of the MNOs interests.

2.4.5 Securing the SIM Card

Subscriber Identification Module (SIM) cards are the smartcards used as the primary means of identifying mobile users. These cards come in two forms: the much older SIM card and the more recent Universal SIM (USIM). For our purposes, SIM card here refers to USIMs.

At the physical level, the hardware of the SIM card is designed to avoid tampering. Attempting to open the CPU chip, for example, will cause it to break. The same holds true for the flash memory which stores the encryption keys. The flash memory, or EEPROM, implements a file-system (7816-4) that supports access controls and secure messaging [35]. Generally, however, the security of the hardware is based on obscurity. [36]

During the manufacturing process, each SIM card gets a key (Kc) burned onto it that is used to encrypt communications. That key is provided to MNOs who purchase and resell the SIM cards to their subscribers for two-way encrypted communications [37]. This key has typically been a DES or 3DES key although more recent SIM cards use AES keys.

SIM cards also implement some form of a Java Virtual Machine that provides sandboxing to keep applications isolated from each other. Software updates to the SIM card require the Kc to make any updates/changes to the SIM card.

Chapter 3: Architecture and Design

3.1 Overview

In this chapter, I will be looking at the architecture of the mobile Internet devices. First, I will provide a general overview of the network architecture in which these devices operate. I will then take an in-depth look at 3G USB dongles from a hardware and software perspective. Finally, I will conclude with the architecture of SIM cards.

3.2 Network architecture

The mobile network comprises of the core network and base stations that connect end users to the mobile network. The core network is also connected via a high speed link to the public Internet and to other networks. In Ghana, all mobile network operators are also Internet service providers so they have access to the national fiber backbone that converge at the Ghana Internet Exchange.

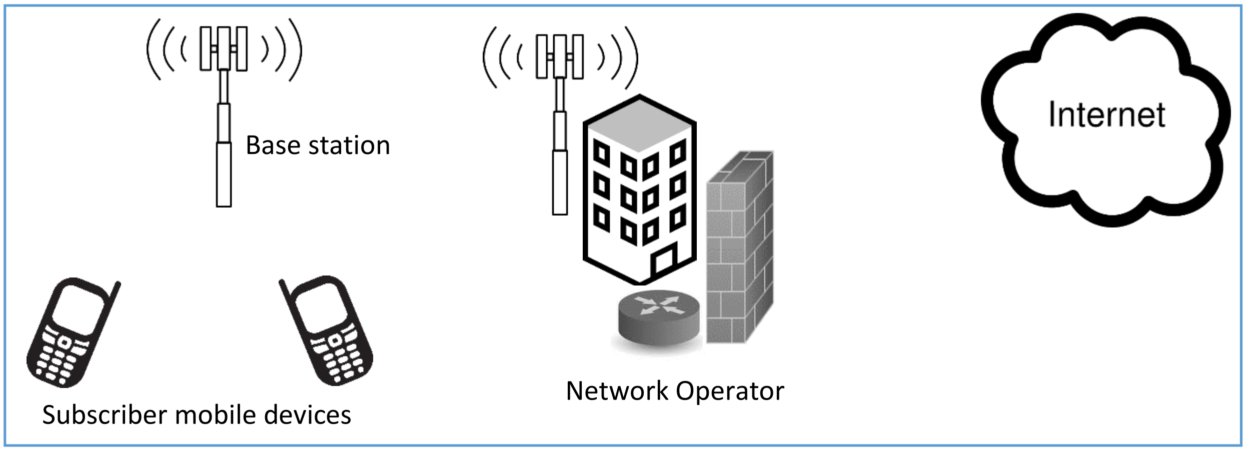


Figure 1: Simplified diagram of mobile network architecture

Today, all MNOs are interconnected via a mesh network connecting various offices across the country. Local (on-net) voice and SMS traffic are handled in the originating network whilst off-net traffic is routed over this mesh network. However, USSD traffic is handled only within the originating home network.

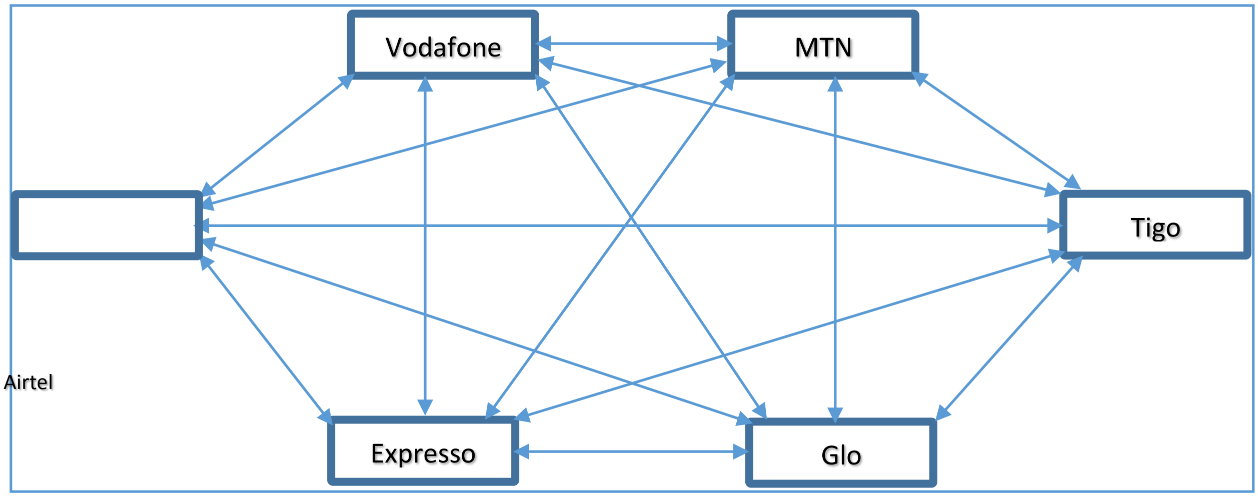


Figure 2: Simple diagram of MNO interconnection

The major networks implement Huawei telecommunications equipment for their in-house telecommunications infrastructure whilst renting space on masts operated by private tower companies. Not much has been written about the physical infrastructure of MNOs in Ghana.

3.3 Device architecture

Consumers can access mobile broadband through Internet-enabled phones, USB dongles/wingles, or mobile Wi-Fi (MiFi) devices. Besides phones, mobile broadband devices are almost exclusively made by two companies, Huawei and ZTE.

For the purpose of this paper, I obtained three USB modems all made by Huawei, E303s-1 from Tigo [38], E303s-2 (marketed as K4201) from Vodafone [38], and EC167 from Expresso Telecom [39]. All three devices come SIM-locked to the operator out-of-the-box.

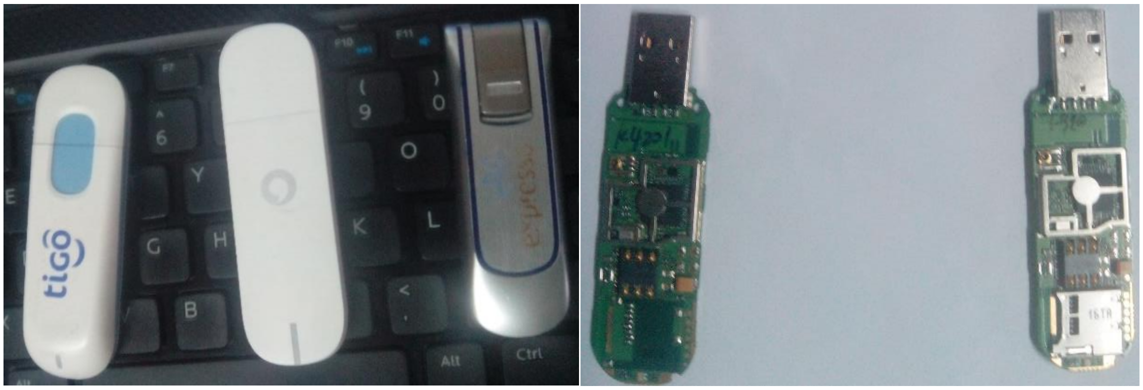


Figure 3: Huawei E303s-1, E303s-2, and EC167 (left) and E303s-1 and E303s-2 without external covers (right)

3.3.1 Physical Architecture

A close look at the E303s-1 modem shows that it comes built with three Hisilicon chips Hi6331rbc, Hi6731arbc, and Hi6481rbc. For storage, it includes a Samsung K521F57ACA-B060 NAND-based multi-chip package (MCP) which stores the 3G dongle drivers and firmware. The total storage capacity of the MCP is not known except that it ranges from 0.013 gigabytes to 0.5 gigabytes according to the Samsung's website [40]. The emulated CDROM on the modem of size 30MB shows up when the modem is connected to a PC. The modem also includes a physical SD card reader onboard. When an SD card is inserted, the USB dongle can now serve as storage device.

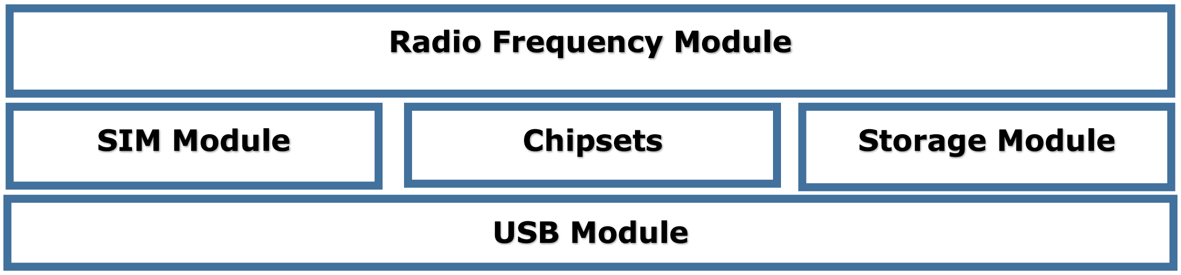


Figure 4: Physical architecture of Huawei E303s-1 USB dongle

3.3.2 Logical Architecture

At the logical level, the modem contains drivers for Windows, Linux, and Mac OS. Using the USB mode switching ability, the dongle can emulate a combination of modem, SD card reader, and CDROM devices or individual devices when plugged to a computer. USB devices are designed to connect different pieces of hardware using a single module. What determines the devices that are connected is the USB mode that is set. The mode can be set to make the USB device emulate a storage drive, a keyboard, a printer, etc.

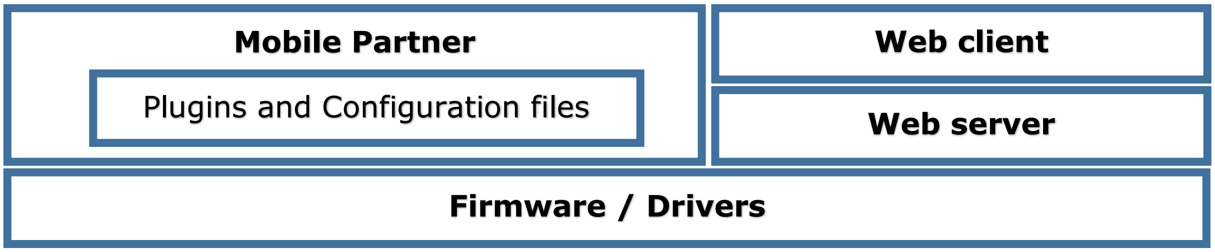


Figure 5: Logical architecture of USB dongle

Mobile Partner

Mobile Partner is the primary vendor software that comes bundled with the dongle, customized to show the colors and logo of the MNO the dongle serves. It provides the graphical user interface for performing actions like making calls, sending SMS, reading SMS, and configuring mobile access point (APN) settings. The Mobile Partner software is bundled with drivers and stored in an image file on the modem that emulates a CDROM when the dongle is inserted into the PC's USB port. The CDROM image is read-only and also contains an installation script for Linux and a Mac OS version of Mobile Partner in addition to Windows.

When installed, Mobile Partner adds processes that run whenever the modem in inserted into a PC. A process like OUC.exe, for example, runs when the modem is inserted with administrative user privileges (system) to search for new updates to the modem software.

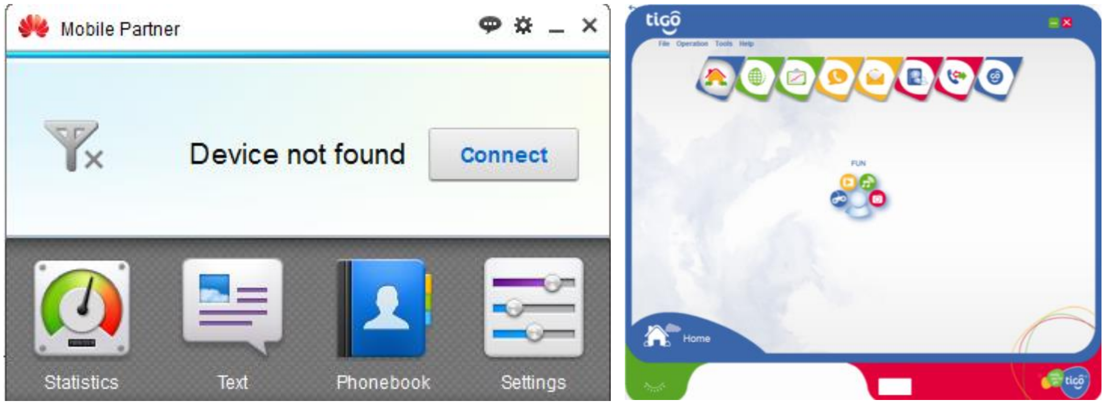
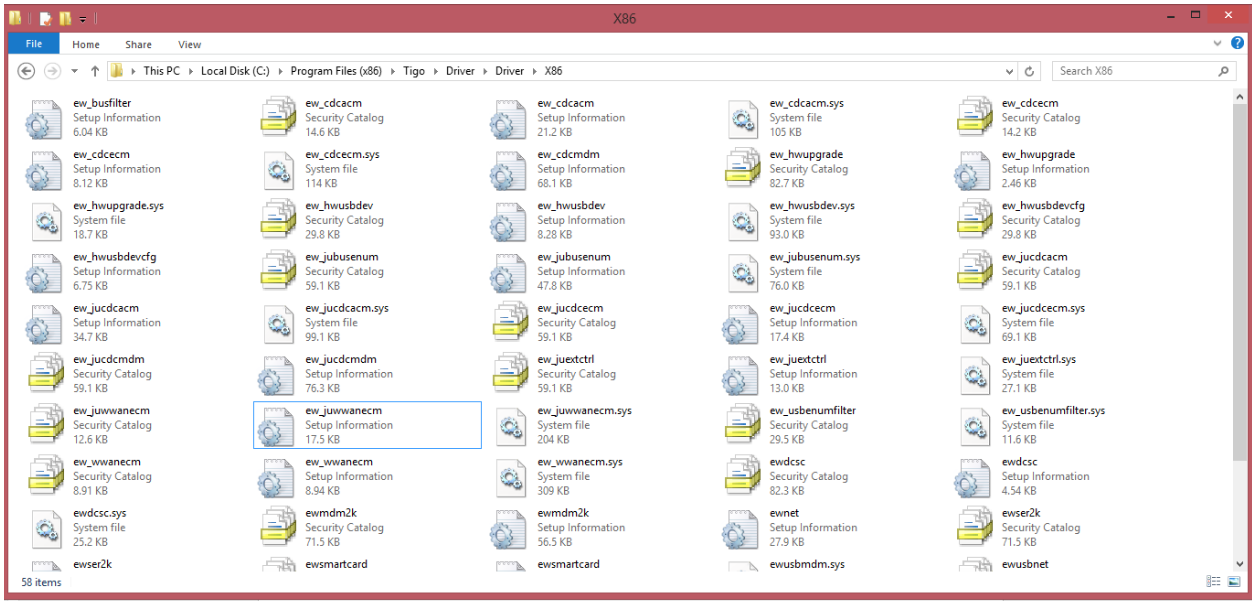


Figure 6: Unbranded Mobile Partner (left) and Tigo-branded Mobile Partner (right)

Drivers

The CDROM image includes several drivers that enable the dongle to emulate different devices like personal computer/smartcard (PCSC) readers, USB modem, wireless wide area network (WWAN) controller, network driver interface specification (NDIS), Bluetooth adapter, GPS device, and a virtual serial port.



This PC › Local Disk (C:) › Program Files (x86) › Tigo › Driver › Driver › X86

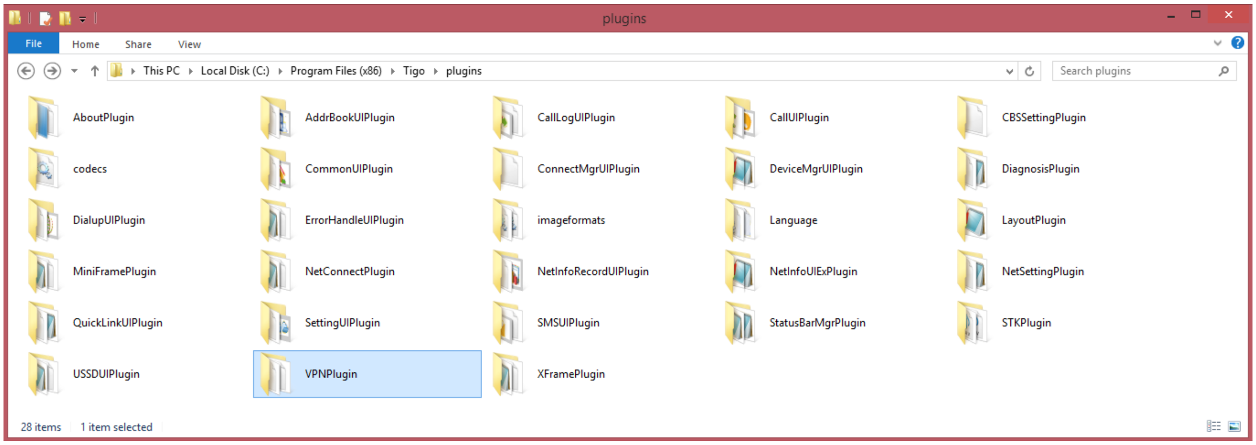
ew_busfilter Setup Information 6.04 KB	ew_cdcacm Security Catalog 14.6 KB	ew_cdcacm Setup Information 21.2 KB	ew_cdcacm.sys System file 105 KB	ew_cdcecm Security Catalog 14.2 KB
ew_cdcecm Setup Information 8.12 KB	ew_cdcecm.sys System file 114 KB	ew_cdcmdm Setup Information 68.1 KB	ew_hwupgrade Security Catalog 82.7 KB	ew_hwupgrade Setup Information 2.46 KB
ew_hwupgrade.sys System file 18.7 KB	ew_hwusbdev Security Catalog 29.8 KB	ew_hwusbdev Setup Information 8.28 KB	ew_hwusbdev.sys System file 93.0 KB	ew_hwusbdevcfg Security Catalog 29.8 KB
ew_hwusbdevcfg Setup Information 6.75 KB	ew_jubusenum Security Catalog 59.1 KB	ew_jubusenum Setup Information 47.8 KB	ew_jubusenum.sys System file 76.0 KB	ew_jucdcacm Security Catalog 59.1 KB
ew_jucdcacm Setup Information 34.7 KB	ew_jucdcacm.sys System file 99.1 KB	ew_jucdcecm Security Catalog 59.1 KB	ew_jucdcecm Setup Information 17.4 KB	ew_jucdcecm.sys System file 69.1 KB
ew_jucdcmdm Security Catalog 59.1 KB	ew_jucdcmdm Setup Information 76.3 KB	ew_juextctrl Security Catalog 59.1 KB	ew_juextctrl Setup Information 13.0 KB	ew_juextctrl.sys System file 27.1 KB
ew_juwwanecm Security Catalog 12.6 KB	ew_juwwanecm Setup Information 17.5 KB	ew_juwwanecm.sys System file 204 KB	ew_usbenumfilter Security Catalog 29.5 KB	ew_usbenumfilter.sys System file 11.6 KB
ew_wwanecm Security Catalog 8.91 KB	ew_wwanecm Setup Information 8.94 KB	ew_wwanecm.sys System file 309 KB	ewdcsc Security Catalog 82.3 KB	ewdcsc Setup Information 4.54 KB
ewdcsc.sys System file 25.2 KB	ewmdm2k Security Catalog 71.5 KB	ewmdm2k Setup Information 56.5 KB	ewnet Setup Information 27.9 KB	ewser2k Security Catalog 71.5 KB
ewser2k	ewsmartcard	ewsmartcard	ewusbmdm.sys	ewusbnet

58 items

Figure 7: Drivers common to all Huawei dongles

Plugins

The Mobile partner also uses a suite of plugins for performing tasks like making phone calls, reading and sending SMS, setting virtual private network (VPN) connections, and making a data connection.


plugins
File
Home
Share
View
This PC ▸ Local Disk (C:) ▸ Program Files (x86) ▸ Tigo ▸ plugins
Search plugins

AboutPlugin	AddrBookUIPlugin	CallLogUIPlugin	CallUIPlugin	CBSSettingPlugin
codecs	CommonUIPlugin	ConnectMgrUIPlugin	DeviceMgrUIPlugin	DiagnosisPlugin
DialupUIPlugin	ErrorHandleUIPlugin	imageformats	Language	LayoutPlugin
MiniFramePlugin	NetConnectPlugin	NetInfoRecordUIPlugin	NetInfoUIExPlugin	NetSettingPlugin
QuickLinkUIPlugin	SettingUIPlugin	SMSUIPlugin	StatusBarMgrPlugin	STKPlugin
USSDUIPlugin	VPNPlugin	XFramePlugin		

28 items 1 item selected

Figure 8: Plugin files common to Huawei dongles

Configuration Files

There are a couple of configuration files that determine how the modem functions. With these files one can, for example, configure when the Mobile Partner software runs, and what authentication method and credential to use when connecting to the mobile network for Internet access.

3.4 SIM Cards

The Subscriber Identification Module (SIM) is a smartcard for communicating on GSM networks. They are "fully programmable computer systems" with a real-time operating system. [41] In recent times, SIM cards have also been referred to as Universal Integrated Circuit Cards (UICC) because of the enhanced functionality made possible by higher specifications. The design of the SIM card follows the design of smart cards generally referred to as Java Cards because they are designed to run sandboxed Java virtual machines (JVM) for hosting multiple applets [38].

3.4.1 Physical Architecture

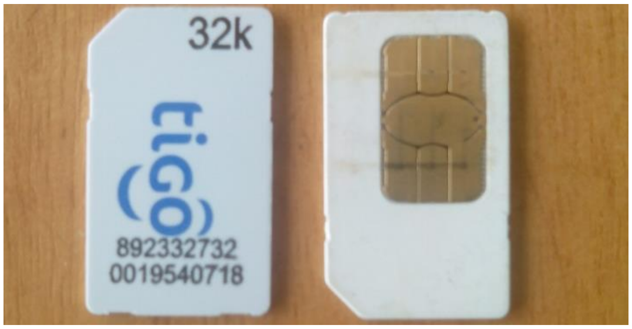


Figure 9: SIM Card

Each SIM card has a central processing unit (CPU). Modern SIM cards have at least a 16-bit sized reduced instruction set computing (RISC) CPU onboard. The CPUs clock between 5 and 20 megahertz. They also contain volatile random access memory (RAM). Internal RAM size ranges from 1kilobyte to 4 kilobytes and external RAM (XRAM) is for reserved applications. The read-only memory (ROM) onboard ranges from sizes of 6 kilobytes to over 100 kilobytes and store the core operating system (described below). In addition, SIM cards also contain flash storage to persist data. Flash storage sizes range from a few kilobytes to 2 Gigabytes and are typically printed on the SIM cards [36].

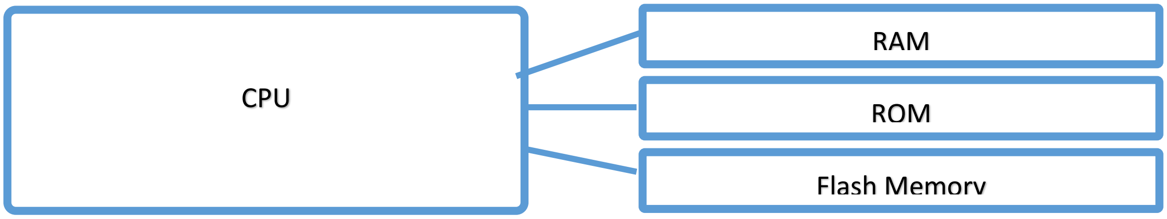


Figure 10: Hardware architecture of SIM card

Between the SIM card and the host, SIM cards are connected via a serial half-duplex communication interface running at rates between 9.6kbps and 115kbps. Modern SIM cards also contain stand-alone hardware for speedily verifying encryption/cipher signatures and generating random numbers to strengthen the encryption process without depending on the CPU [36].

3.4.2 Logical Architecture

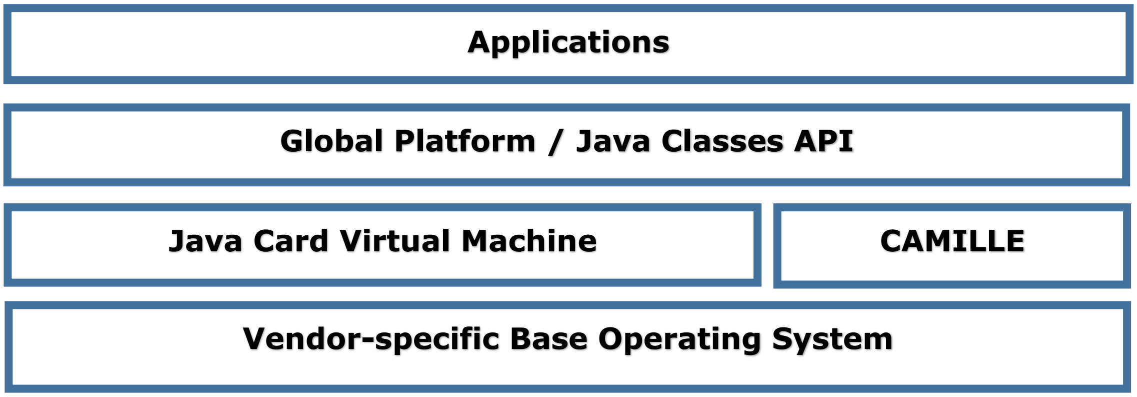

Applications
Global Platform / Java Classes API
Java Card Virtual Machine
CAMILLE
Vendor-specific Base Operating System

Figure 11: Logical architecture of SIM card

SIM cards follow the standardized design of the Java Card called the Java Card Open Platform. At the low level are a vendor-specific operating system written in Assembly or C for application management, serial communication, fast encryption libraries, a real-time kernel, etc. [36].

Above the operating system is an implementation of a JVM called the Java Card Virtual Machine (JCVM). The JCVM provides a sandbox for running applets by compiling the applet code into a compact version of Java bytecode and then executing it in the virtual machine. There are alternatives to JCVM such as CAMILLE that skip the Java bytecode step and compile directly into machine code using register-based operation codes (op-codes), thereby improving speed. However, CAMILLE takes up more space because of its extensive use of registers, making it unsuitable for space-conscious SIM manufacturers [36].

Above this layer are two application programming interfaces (API) that provide system level functionality without giving upper layers direct access to the JCVM through the use of libraries and system calls. These APIs are the Java Classes API and the GlobalPlatform API and are used together in SIM applications development. The Java classes API provide a collection of Java packages that serve as the foundation of SIM applications. The Java classes API combined with the JCVM make up the Java Card Runtime Environment (JCRE). The GlobalPlatform API is a language-agnostic collection of classes developed by the Open Platform Foundation that can also be used by approaches not using JCVMs [36].

The topmost layer is for applications. Examples of such applications are mobile money applications, banking applications, value added services, and roaming control. Applications can be pushed from MNOs to subscribers to ensure that all subscribers have the latest services using over the air (OTA) updates. The most popular method of pushing out OTA updates by sending multiple binary SMS is being replaced by the use of TCP/IP over GPRS. However, once the SIM card is sold to the subscriber (card holder), only applets can be updated—not the underlying software layers [36].

Chapter 4: Exploits and Results

4.1 Overview

To evaluate the security that consumers can expect from the network, I took a multi-layered approach of exploiting perceived vulnerabilities across the mobile spectrum from the SIM card hardware through to the computer systems of the MNOs. Many of these exploits have been created and demonstrated by members of the hacker community in mostly European environments. It is my attempt to replicate some of those here as well as look out for conditions unique to our mobile network environment.

4.2 Attempted Exploits

4.2.1 Attacking 3G Dongles

Purpose: For this exploit, my aim is to determine if USB 3G dongle are susceptible to cross site scripting (XSS) attacks.

Target: The self-service software on Vodafone Huawei K4201 dongle

Limitation: In this exploit, I did not attempt to exploit the hardware as I did not have sufficient information about the architecture to determine exploitation vectors.

Exploit Potential

Security researchers have exploited the self-care software on dongles to retrieve administrator credentials using cross site scripting attacks [42].

In 2013, two Russian security researchers, Nikita Tarakanov and Oleg Kupreev, revealed that the USB dongles have insecure software on them. These vulnerabilities demonstrated the many possible attack vectors these devices provide [43]. Their attack requires physical access to the modem.

Other researchers have also demonstrated that the USB module in the modems can be exploited to turn the modem into malicious human interface devices (HID) like keyboards for logging user input [44]. They accomplished this by flashing the USB devices with modified firmware that identified the USB device to the computer as whatever the attacker chooses from the list of possible USB device modes. Their attack also requires physical access to the modem.

The Proof of Concept (PoC) of a cross site scripting attack on the Vodafone self-service software is found in Appendix B.

4.2.2 Impersonating the MNO to Send OTA Updates

Purpose: For this exploit, my aim was to determine what types of communication were allowed over the mobile network channel and whether I can impersonate an operator to send binary SMS to other subscribers.

Target: All mobile networks and Internet enabled phones.

Limitation: This exploit requires the user's consent to save the received configuration files in their phone. However, it seeks to demonstrate that other OTA messages including binary SMS are not filtered on the network.

Binary SMS have been used to obtain keys (Kc) from SIM cards remotely [41].

Exploit Potential

OTA updates have been used by security researchers to successfully extract the encryption signatures that are used to secure SIM cards [41].

In 2013, a team of researchers at SR Labs in Germany demonstrated that SIM cards can be rooted remotely using OTA messages. The technique requires sending a binary SMS to a mobile device requesting the SIM to perform some unauthorized action. Mobile devices typically forward such SMS to the SIM directly. The SIM recognizes that the command received is not properly signed and replies with an error and a DES crypto signature. The attacker then uses existing methods of breaking 56-bit DES signature, using things like rainbow tables. With the key, the attacker can now properly sign commands and send them over via binary SMS. Successful attacks included rooting the SIM card, running Java viruses to break out of sandboxing to read all of memory content like mobile banking and mobile payment encryption keys, etc. [41].

The Proof of Concept (PoC) of impersonating an MNO to send OTA updates is found in Appendix C.

4.2.3 Exploiting MNO Core Systems

Purpose: In this exploit, my aim was to determine if there are vulnerable entry points into MNO’s internal network from the public Internet.

Targets: All Internet-facing devices belonging to mobile network operators.

Limitation: I limited this exploit to identifying services with either weak or no authentication setup because I did not seek/obtain the permission of MNOs to penetrate their internal network. I also did not attempt to penetrate the MNOs internal network from other services like SMS or USSD.

The Proof of Concept (PoC) is found in Appendix D.

4.3 Potential Exploits

4.3.1 Exploiting SIM Cards and Eavesdropping on Calls

Purpose: The aim of this exploit would be to remotely extract the encryption key of the SIM card that comes from the manufacturer. A secondary aim is to listen in on phone calls on the network.

Target: All SIM cards on GSM networks

Limitation: I did not have the necessary computing power to crack the keys efficiently. In addition, I also did not have specialized equipment.

Tools

Hardware: GSM base station (mini would do) or HackRF device, high-end PC with graphics processor

Software: OpenBTS, Air Probe

Exploit Potential: Extracting the SIM card’s encryption key allows one to gain total impersonating ability over the SIM card. Using regular SMS, the attacker can carry out the same exploits that are described under the OTA update exploit potential [42]. Despite A5/1 being the most secure of the three 2G ciphers, it has been successfully cryptanalyzed to show serious weaknesses that allow things like eavesdropping on GSM calls [26], impersonation [27], and user tracking [28]. It is documented that the cipher, was originally designed with a key size of 128 bits, was weakened to use 56-bit key sizes to allow eavesdropping by security services [29]. Documents released by NSA whistleblower, Edward Snowden, show that the NSA has been able to decrypt A5/1 GSM traffic for some time [30].

There have been both theoretical and practical cryptanalysis attempted on the KASUMI cipher [32]. It is been proven theoretically that the KASUMI cipher can be successfully cryptanalyzed, however, the practicality of such attacks remains very difficult for the standard implementation of the cipher [33].

Chapter 5: Conclusions and Recommendations

5.1 Overview

Whilst mobile communication remains a vital part of the daily lives of Ghanaians and Africans, there are critical security lapses in the ecosystem as this project has shown. The security of these communications vary from operator to operator but generally show many signs of weakness. Many of the vulnerabilities discovered and exploited in this paper have fixes that are documented. This chapter seeks to connect the discovery of vulnerabilities with solutions to improve security and mitigate the risk of system compromise.

5.2 MNO Core Network

The internal networks of all MNOs in Ghana have Internet-facing computing devices, some of which still maintain their default access configurations. These configurations pose serious security risks because the default access credentials, if any, are readily available online. Of the devices encountered in this assessment, many of those with default or no authentication display explicit warnings about their state to prompt network administrators to change them. Clearly, these prompts were not heeded.

The second vulnerability is the sheer number of ports that are open to the public Internet on each device found. Some devices had as many as 14 ports running various services. Some of these ports were unprotected, thereby, giving access to anyone with knowledge of their existence. The many open ports provide many options to an attacker to gain access to the internal networks of MNOs. The most prominent culprit is the Telnet port (Port 23) which does not provide end-to-end encryption and also comes unauthenticated in its default configuration.

In addition, even for ports implementing encryption, many of them displayed headers that gave out revealing information of the device they ran on. The header information included things like the version number of the services running on them as well as and the operating system. A quick lookup of these version numbers on a search engine will show vulnerabilities, if any, to which the software is susceptible.

5.3 OTA Updates

The exploits demonstrated in this paper show that network filtering is either non-existent or ineffective in restricting critical services to mobile network operators or authorized organizations. The filtering also seems non-existent on inter-network communications as the exploit worked across different networks. This makes it possible for remote attacks on mobile devices, networks, and even SIM cards. The same mechanism that MNOs use to update SIM cards is readily available to anyone on the network without authentication or authorization.

5.4 Network and SIM Card Encryption

Whilst the exact type of cipher to encrypt mobile communications in Ghana was not determined, one can infer from the presence of second generation (2G) technologies that weak forms of encryption (A5/0 or A5/1) are in use. Considering that the more secure KASUMI (A5/3) ciphers that secure third generation (3G) technologies are not backward compatible with 2G technologies, one can postulate that wherever 2G technologies exist, communications are insecure. Determining the exact nature of encryption in use on 2G networks in Ghana will be a subject of further study.

Furthermore, whilst this paper did not explore the encryption implemented in SIM cards used in Ghana, SIM cards are an important target of exploits. Given that many SIM cards implement weak encryption standards like 56-bit DES, one can assume that the SIM cards in circulation are also vulnerable.

5.5 Device Security

Internet-enabled devices like the Huawei 3G USB dongles have vulnerabilities that not only compromise the security of the communications through them, but also the security of the devices they connect to. Cross-site scripting vulnerabilities enable impersonation attacks whilst USB exploits open up a plethora of possible attacks on the host device.

5.6 Recommendations

The bright side of this security assessment is that many of the vulnerabilities listed have relatively easy solutions. Even for the vulnerabilities that require huge financial or time investments to fix, there are immediate steps that can make them less susceptible to exploit. My recommendations on fixing these vulnerabilities and/or mitigating the risk of exploit start with the proverbial low-hanging fruits and move up to the top of the tree.

The first step is to assess the configurations of network devices to ensure that the default configurations are modified and the unused ports are closed. This should also include all critical ports that do not implement encryption like FTP and Telnet. Once done, a full security audit of the network infrastructure can follow to give an accurate picture of the network.

The second step is to edit out revealing information in headers of applications that are open to the public Internet. Whilst this does not solve the underlying problem of unpatched software, it introduces ambiguity about that particular system. A more concrete solution is to patch the applications so that its known vulnerabilities are addressed.

Network filtering of binary SMS only to authorized parties greatly reduces the risk of the remote attacks that are possible through this means.[41] Individuals or organizations who need to send or receive binary SMS and other OTA updates should register with an MNO or the national regulator to be able to do so. SIM cards can be registered and authorized to perform this function.

MNOs should also demand that device manufactures of 3G USB dongles supply patches to known vulnerabilities on the devices. Some of these vulnerabilities are the dongle software's susceptibility to cross site request forgery (CSRF) and cross site scripting (XSS). There are no known solutions to USB exploits as it affects the core USB protocol [41].

On SIM card security, MNOs should replace the SIM cards that implement 56-bit DES encryption with newer SIM cards implementing AES encryption. This can start by selling new SIM cards to new subscribers and extend to carrying out a nationwide SIM replacement exercise.

Communication on the network can be secured by upgrading to third generation (3G) technologies implementing the KASUMI (A5/3) cipher. This usually requires a replacement of base station equipment as the KASUMI cipher is not compatible with 2G technologies which is very expensive.

5.7 Future Work

This paper is a maiden attempt to assess security in mobile communications in Ghana. The primary focus is to evaluate that security that subscribers can expect from using mobile networks. It also surveys the mobile ecosystem from both technical and non-technical angles of security. Due to the limitations of time and equipment, it was not possible to assess potentially vulnerable systems and equipment or replicate some known vulnerabilities. Additionally, as I wrote this paper, new developments started to emerge in the mobile telecommunication sector that would be interesting to assess.

Further research is needed to provide in-depth knowledge of the security and privacy structures of each stakeholder in the mobile ecosystem. These areas include, but are not limited to:

1. Security implications of the proposed Interconnect Clearing House (ICH)
2. Security assessment of fixed broadband and fixed wireless equipment and networks provided by mobile network operators
3. Internal security controls at mobile network operator stations and offices
4. Security assessment of SIM cards in Ghana
5. Security assessment of other mobile Internet devices like smartphones and mobile Wi-Fi (MIFI) devices used in Ghana
6. Security assessment of mobile payment systems
7. Security implications of using GSM-enabled biometric identification systems in Ghanaian elections
8. An extension of any of the above to the rest of the continent.

REFERENCES

[1]M. Nagy and I. Kotuliak, 'Enhancing security in mobile data networks through end user and core network cooperation', *Proceedings of International Conference on Advances in Mobile Computing & Multimedia - MoMM '13*, 2013.

[2]W. Stallings, *Cryptography and network security*. Boston: Prentice Hall, 2011.

[3]M. Bishop, *Computer security*. Boston: Addison-Wesley, 2003.

[4] Nca.org.gh, 'What We Do - National Communication Authority', 2015. [Online]. Available: http://nca.org.gh/19/142/What-We-Do.html. [Accessed: 17- Apr- 2015].

[5] Nca.org.gh, 'News - National Communication Authority', 2015. [Online]. Available: http://nca.org.gh/73/34/News.html?item=419. [Accessed: 17- Apr- 2015].

[6] Vodafone360.com, 'Acquisition of a 70% Stake in Ghana Telecom - Vodafone', 2015. [Online]. Available: http://vodafone360.com/content/index/media/group_press_releases/2008/acquisition_of_a_70.html. [Accessed: 17- Apr- 2015].

[7] Modern Ghana, 'Areeba soon to be MTN Ghana', 2015. [Online]. Available: http://www.modernghana.com/news/137909/1/areeba-soon-to-be-mtn-ghana.html. [Accessed: 17- Apr- 2015].

[8] Vibeghana.com, 'Glo Mobile Ghana launches Ghana network |', 2015. [Online]. Available: http://vibeghana.com/2012/04/30/glo-mobile-ghana-launches-ghana-network/. [Accessed: 17- Apr- 2015].

[9]M. Boateng, 'Expresso takes over Kasapa Telecom, pledges good services', Business.myjoyonline.com, 2015. [Online]. Available:

http://business.myjoyonline.com/pages/news/201011/55897.php. [Accessed: 17- Apr- 2015].

[10] Ppi.worldbank.org, 'Mobitel Ghana (Tigo) - Individual Project Information - Private Infrastructure Projects - The World Bank & PPIAF', 2015. [Online]. Available: http://ppi.worldbank.org/explore/PPIReport.aspx?ProjectID=1563. [Accessed: 17- Apr- 2015].

[11] Modern Ghana, 'Bharti Airtel acquires Zain for $10.7bn', 2015. [Online]. Available: http://www.modernghana.com/news/263921/1/bharti-airtel-acquires-zain-for-107bn.html. [Accessed: 17- Apr- 2015].

[12] Ghanaweb.com, 'NCA denies telcos 4G license', 2015. [Online]. Available: http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=268506. [Accessed: 17- Apr- 2015].

[13] Nca.org.gh, 'News - National Communication Authority', 2015. [Online]. Available: http://www.nca.org.gh/73/34/News.html?item=419. [Accessed: 17- Apr- 2015].

[14] Infodev.org, 'Making Mobile Apps Work at the Base of Pyramid | infoDev', 2014. [Online]. Available: http://www.infodev.org/articles/making-mobile-apps-work-base-pyramid. [Accessed: 16- Apr- 2015].

[15] Grameenfoundation.org, 'Maternal and Infant Health | Grameen Foundation | Connecting the World's Poor to Their Potential', 2015. [Online]. Available: http://www.grameenfoundation.org/what-we-do/health/maternal-and-infant-health. [Accessed: 16- Apr- 2015].

[16] Genkey.com, 'Voter Verification | Genkey', 2015. [Online]. Available: http://www.genkey.com/en/solutions/biometric-validation/voter-verification. [Accessed: 16- Apr- 2015].

[17] Parliament of the Republic of Ghana. 2008. The Electronic Transactions Act of Ghana. Available: http://www.nca.org.gh/downloads/regdocs/NCA_Electronic_Communications_Act_775.pdf. [Accessed: 16- Apr- 2015].

[18]M. Boateng, 'SIM Registration, the law and the arguments', Business.myjoyonline.com, 2015. [Online]. Available: http://business.myjoyonline.com/pages/news/201202/82125.php. [Accessed: 16- Apr- 2015].

[19] Myjoyonline.com, 'Ghana News - Govt orders re-run of SIM registration', 2015. [Online]. Available: http://www.myjoyonline.com/business/2014/march-13th/govt-orders-re-run-of-sim-registration.php. [Accessed: 16- Apr- 2015].

[20] V. Kai-Mensah, 'Phone users banned from acquiring more than 10 sim cards - citifmonline', citifmonline, 2014. [Online]. Available: http://citifmonline.com/2014/09/02/phone-users-banned-from-acquiring-more-than-10-sim-cards/#sthash.EZbT6emI.dpbs. [Accessed: 16- Apr- 2015].

[21] Nca.org.gh, 'News - National Communication Authority', 2015. [Online]. Available: http://www.nca.org.gh/73/34/News.html?item=391. [Accessed: 16- Apr- 2015].

[22]K. Donovan and A. Martin, 'The rise of African SIM registration: The emerging dynamics of regulatory change', *First Monday*, vol. 19, no. 2, 2014.

[23]A. Mahalanobis and J. Shah, 'An Improved Guess-and-Determine Attack on the A5/1 Stream Cipher', *Computer and Information Science*, vol. 7, no. 1, 2013.

[24]E. Barkan, E. Biham and N. Keller, 'Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication', *J Cryptol*, vol. 21, no. 3, pp. 392-429, 2007.

[25] 3gpp.org, '3GPP specification CRs: 43.020', 2015. [Online]. Available: http://www.3gpp.org/DynaReport/43020-CRs.htm. [Accessed: 17- Apr- 2015].

[26]K. Nohl and C. Paget, 'GSM – SRSLY?', Berlin, Germany, 2009.

[27]K. Nohl and L. Melette, 'Defending Mobile Phones', Berlin, Germany, 2011.

[28]T. Engel, 'SS7: Locate. Track. Manipulate.', Berlin, Germany, 2014.

[29] Aftenposten, 'Sources: We were pressured to weaken the mobile security in the 80's', 2014. [Online]. Available: http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html. [Accessed: 17- Apr- 2015].

[30] Washington Post, 'By cracking of A5/1 cellphone code, NSA has capability for decoding private conversations', 2015. [Online]. Available: http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html. [Accessed: 17- Apr- 2015].

[31] 3gpp.org, '3GPP specification: 35.202', 2015. [Online]. Available: http://www.3gpp.org/DynaReport/35202.htm. [Accessed: 17- Apr- 2015].

[32]E. Barkan, E. Biham and N. Keller, 'Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication', *J Cryptol*, vol. 21, no. 3, pp. 392-429, 2007.

[33]O. Dunkelman, N. Keller and A. Shamir, 'A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony', *J Cryptol*, vol. 27, no. 4, pp. 824-849, 2013.

[34]N. Shaker, H. Issa, K. Shehata and S. Hashem, 'Design of F8 Encryption Algorithm Based on Customized Kasumi Block Cipher', *IJCCE*, pp. 398-402, 2013.

[35] Iso.org, 'ISO/IEC 7816-4:2013 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange', 2015. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54550. [Accessed: 17- Apr- 2015].

[36]P. Edsbäcker, 'SIM cards for cellular networks', Undergraduate, Mid Sweden University, 2010.

[37] The Intercept, 'The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle', 2015. [Online]. Available: https://firstlook.org/theintercept/2015/02/19/great-sim-heist/. [Accessed: 17- Apr- 2015].

[38] Consumer.huawei.com, '【E303 Specifications 】 - Huawei Dongles - Huawei Official Site', 2015. [Online]. Available: http://consumer.huawei.com/en/mobile-broadband/dongles/tech-specs/e303-en.htm. [Accessed: 17- Apr- 2015].

[39] Imei.info, 'HUAWEI EC167 - Full phone specification - IMEI.info', 2015. [Online]. Available: http://www.imei.info/phonedatabase/12422-huawei-ec167/. [Accessed: 17- Apr- 2015].

[40] Memorylink.samsung.com, 'Samsung Memory Link', 2013. [Online]. Available: https://memorylink.samsung.com/ecomobile/mem/ecomobile/product/productOverview.do?topMenu=P&subMenu=mcp&partSetNo=MCP&partSetLabel=NAND%20based%20MCP. [Accessed: 17- Apr- 2015].

[41] Srlabs.de, 'Rooting SIM cards | Security Research Labs', 2015. [Online]. Available: https://srlabs.de/rooting-sim-cards/. [Accessed: 17-Apr- 2015].

[42]S. Gordeychik and A. Zaitsev, '#root via SMS: 4G IP access security assessment', Tokyo, Japan, 2014.

[43]O. Kupreev and N. Tarakanov, 'From China With Love', Amsterdam, Netherlands, 2015.

[44]K. Nohl, 'BadUSB — On accessories that turn evil', Las Vegas, USA, 2014.

Appendix A: Technical Terms and Acronyms

1G – First Generation Wireless Telephone Technology: analog

2G – Second Generation Wireless Telephone Technology: digital

GSM – Global System for Mobile

CDMA – Code Division Multiple Access

GPRS – General Packet Radio Service: 2.5G

EDGE – Exchanged Data rates for GSM Evolution: 2.75G

EGPRS – EDGE General Packet Radio Service: 2.9G

3G – Third Generation

UMTS – Universal Mobile Telephone System

CDMA200 – Code Division Multiple Access 2000

HSDPA – High Speed Downlink Packet Access: 3.5G

HSPA+ – High Speed Packet Access Plus = HSDPA + HSUPA (U is uplink): 3.75G

LTE – Long Term Evolution

True 4G – True Fourth Generation = LTE-Advanced or Mobile Wimax

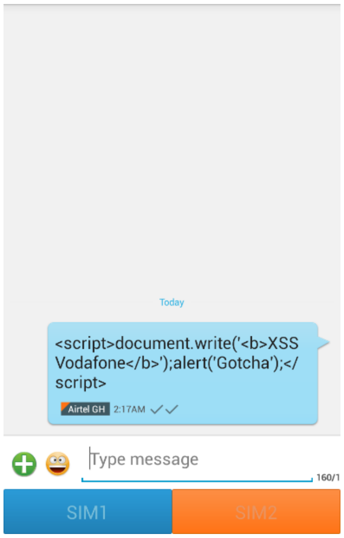
Appendix B: Exploiting USB Dongle Software with Cross Site Scripting (XSS)

Tools

Any mobile phone that can send SMS

Steps

1. I sent a simple JavaScript code to show an alert box and display a message as an SMS

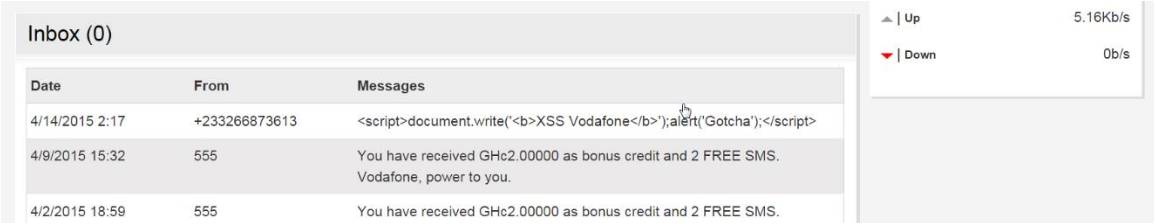


Today

<script>document.write('<b>XSS Vodafone</b>');alert('Gotcha');</script>

Airtel GH 2:17AM

2. On the Vodafone self-service portal on the modem, the message displays as below:

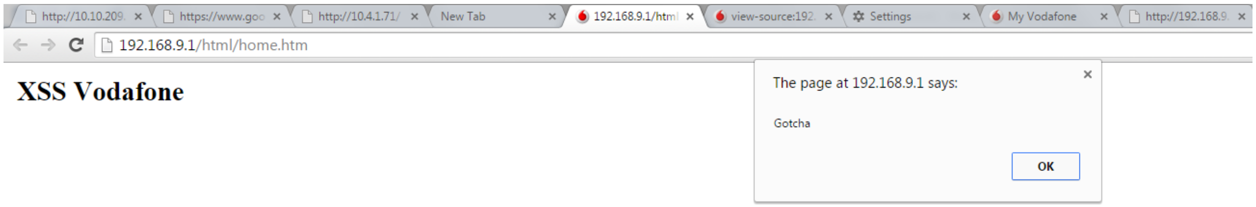


Inbox (0)

Date	From	Messages
4/14/2015 2:17	+233266873613	<script>document.write('<b>XSS Vodafone</b>');alert('Gotcha');</script>
4/9/2015 15:32	555	You have received GHc2.00000 as bonus credit and 2 FREE SMS. Vodafone, power to you.
4/2/2015 18:59	555	You have received GHc2.00000 as bonus credit and 2 FREE SMS.

Up	5.16Kb/s
Down	0b/s

3. When the user clicks the message in the Vodafone self-care portal, the browser runs the script to show the alert box and display the message.



XSS Vodafone

The page at 192.168.9.1 says:

Gotcha

4. Whilst this attack is harmless, it demonstrates that the self-service portal of Vodafone is susceptible to cross site scripting which can be used to cause more harm.

Appendix C: Exploiting Over the Air (OTA) Updates

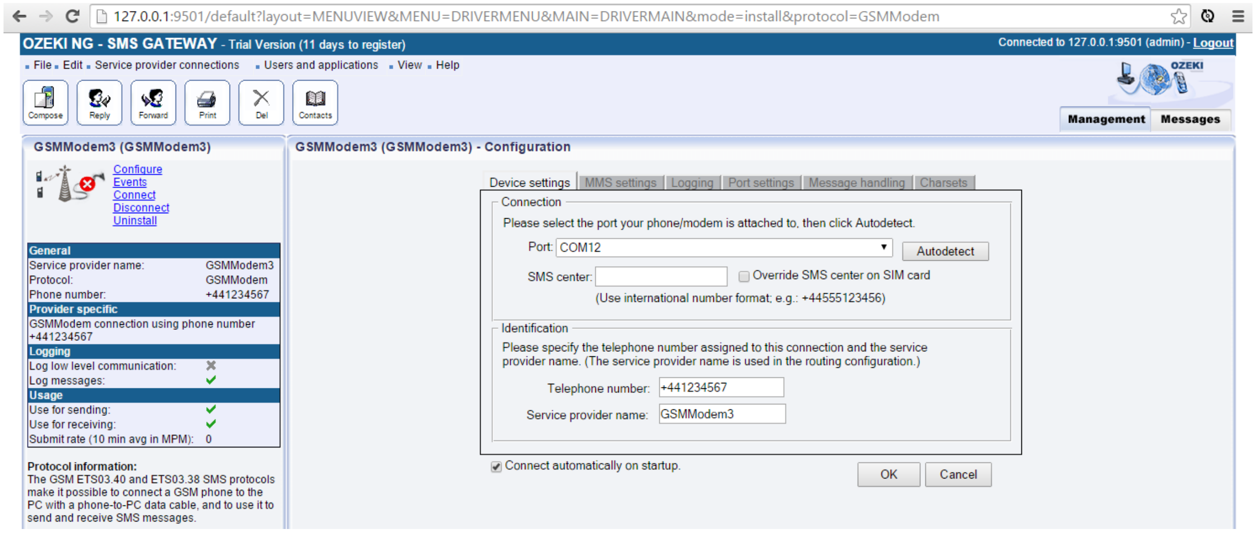
Tools

Software: SMS gateway (OzekiNG SMS gateway v4.6.2)

Hardware: Modem (Huawei E303 USB dongle)

Steps

1. Install OzekiNG SMS gateway (free trial)
2. Connect modem and install modem software (some variation of mobile partner)
3. Run OzekiNG Service Monitor
4. Open web browser and visit: http://127.0.0.1:9501
5. Login with default credentials (admin/abc123)
6. From Service Provider Connections menu, choose “Add service provider connection”
7. In the right content area, click “Install” next to the “GSM/GPRS Modem Connection” option
8. Click “Auto-detect” next to the name of the COM port chosen


127.0.0.1:9501/default?layout=MENUVIEW&MENU=DRIVERMENU&MAIN=DRIVERMAIN&mode=install&protocol=GSMModem
OZEKI NG - SMS GATEWAY - Trial Version (11 days to register)
Connected to 127.0.0.1:9501 (admin) - Logout
File
Edit
Service provider connections
Users and applications
View
Help
Compose
Reply
Forward
Print
Del
Contacts
Management
Messages
Configure
Events
Connect
Disconnect
Uninstall
Device settings
MMS settings
Logging
Port settings
Message handling
Charsets
Autodetect
OK
Cancel

GSMModem3 (GSMModem3)

General
Service provider name: GSMModem3
Protocol: GSMModem
Phone number: +441234567

Provider specific
GSMModem connection using phone number +441234567

Logging
Log low level communication: ✗
Log messages: ✓

Usage
Use for sending: ✓
Use for receiving: ✓
Submit rate (10 min avg in MPM): 0

Protocol information:
The GSM ETS03.40 and ETS03.38 SMS protocols make it possible to connect a GSM phone to the PC with a phone-to-PC data cable, and to use it to send and receive SMS messages.

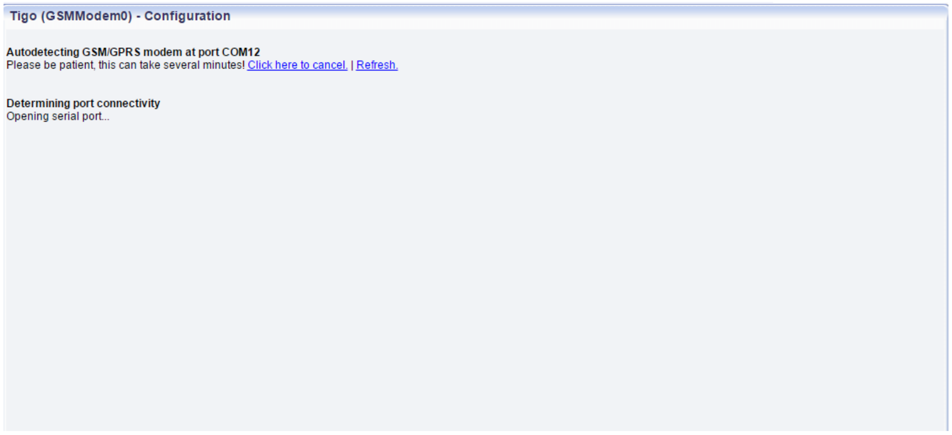
GSMModem3 (GSMModem3) - Configuration

Connection
Please select the port your phone/modem is attached to, then click Autodetect.
Port: COM12
SMS center: □ Override SMS center on SIM card
(Use international number format; e.g.: +44555123456)

Identification
Please specify the telephone number assigned to this connection and the service provider name. (The service provider name is used in the routing configuration.)
Telephone number: +441234567
Service provider name: GSMModem3

☑ Connect automatically on startup.

9. If it detects the modem, it will show you full details of the modem. For example

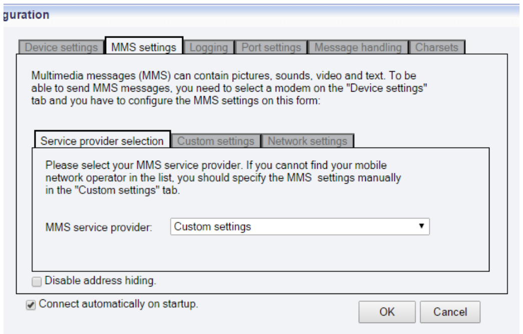


Tigo (GSMModem0) - Configuration

Autodetecting GSM/GPRS modem at port COM12
Please be patient, this can take several minutes! Click here to cancel. | Refresh.

Determining port connectivity
Opening serial port...

10. Now configure the following fields with the details of your network provider. The following are for the Tigo network and SIM card I used. You can leave all other settings to their default value.



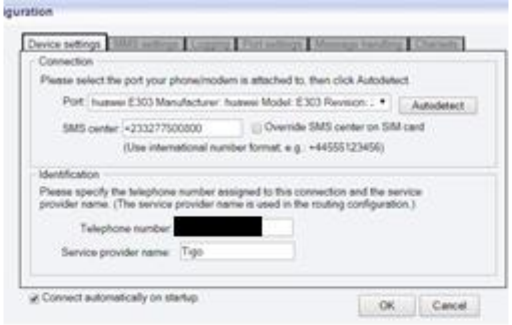
Multimedia messages (MMS) can contain pictures, sounds, video and text. To be able to send MMS messages, you need to select a modem on the "Device settings" tab and you have to configure the MMS settings on this form:

Please select your MMS service provider. If you cannot find your mobile network operator in the list, you should specify the MMS settings manually in the "Custom settings" tab.

MMS service provider: Custom settings

□ Disable address hiding.

☑ Connect automatically on startup.



Connection

Please select the port your phone/modem is attached to, then click Autodetect.

Port: huawei E303 Manufacturer: huawei Model: E303 Revision: ..

SMS center: +233277500800 □ Override SMS center on SIM card

(Use international number format, e.g.: +44555123456)

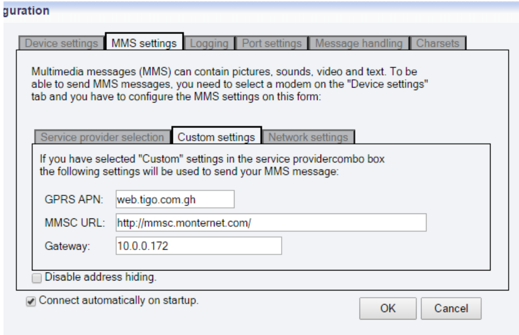
Identification

Please specify the telephone number assigned to this connection and the service provider name. (The service provider name is used in the routing configuration.)

Telephone number: [redacted]

Service provider name: Tigo

☑ Connect automatically on startup.



Multimedia messages (MMS) can contain pictures, sounds, video and text. To be able to send MMS messages, you need to select a modem on the "Device settings" tab and you have to configure the MMS settings on this form:

If you have selected "Custom" settings in the service providercombo box the following settings will be used to send your MMS message:

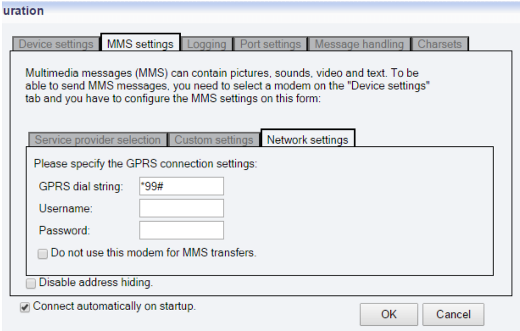
GPRS APN: web.tigo.com.gh

MMSC URL: http://mmsc.monternet.com/

Gateway: 10.0.0.172

□ Disable address hiding.

☑ Connect automatically on startup.



Multimedia messages (MMS) can contain pictures, sounds, video and text. To be able to send MMS messages, you need to select a modem on the "Device settings" tab and you have to configure the MMS settings on this form:

Please specify the GPRS connection settings:

GPRS dial string: *99#

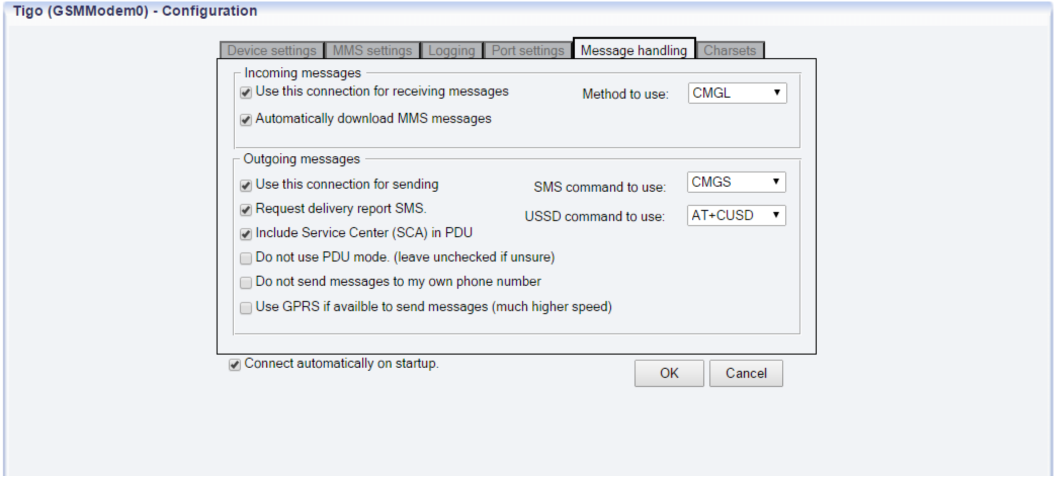
Username:

Password:

□ Do not use this modem for MMS transfers.

□ Disable address hiding.

☑ Connect automatically on startup.



Incoming messages

☑ Use this connection for receiving messages — Method to use: CMGL

☑ Automatically download MMS messages

Outgoing messages

☑ Use this connection for sending — SMS command to use: CMGS

☑ Request delivery report SMS. — USSD command to use: AT+CUSD

☑ Include Service Center (SCA) in PDU

□ Do not use PDU mode. (leave unchecked if unsure)

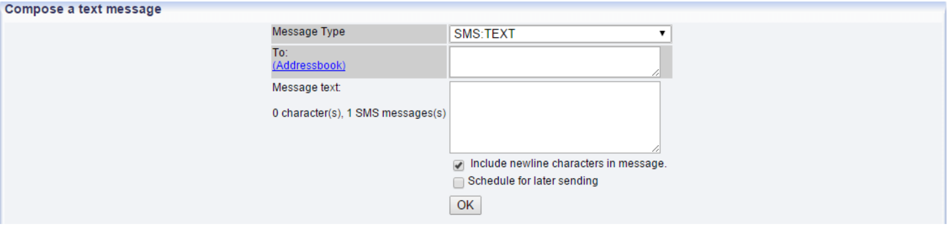
□ Do not send messages to my own phone number

□ Use GPRS if availble to send messages (much higher speed)

☑ Connect automatically on startup.

11. Click “Connect in the left sidebar to ensure that the modem is detected. The red X should disappear once you are connected.

12. Click “Compose” to go to the message view



Compose a text message

Message Type: SMS:TEXT

To: (Addressbook)

Message text

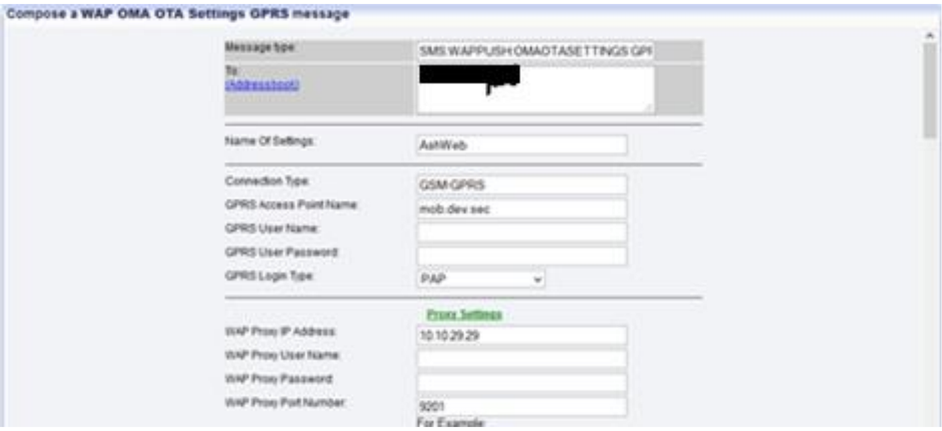
0 character(s), 1 SMS messages(s)

☑ Include newline characters in message.

□ Schedule for later sending

13. In the left side bar, scroll down to see all the types of SMSes that can be sent. For this demonstration, I will send an Open Mobile Alliance Over-The-Air configuration for a GPRS connection. So click on OMA OTA and then click GPRS Connection

14. In this field, fill the following fields: To, Name of Settings, Connection Access Point Name, GPRS user and password (if required), WAP Proxy Settings (if required). Then scroll down and click "Send"



Compose a WAP OMA OTA Settings GPRS message

Message type: SMS:WAPPUSH:OMAOTASETTINGS:GPI

To: (Addressbook) [redacted]

Name Of Settings: AshWeb

Connection Type: GSM-GPRS

GPRS Access Point Name: mob.dev.sec

GPRS User Name:

GPRS User Password:

GPRS Login Type: PAP

WAP Proxy IP Address: 10.10.29.29

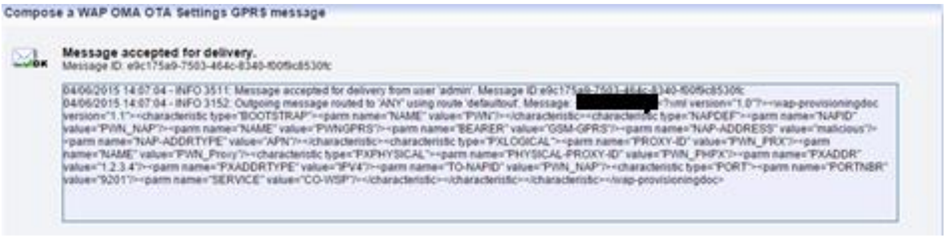
WAP Proxy User Name:

WAP Proxy Password:

WAP Proxy Port Number: 9201

For Example:

15. The message is formatted using WebXML standard to look like this

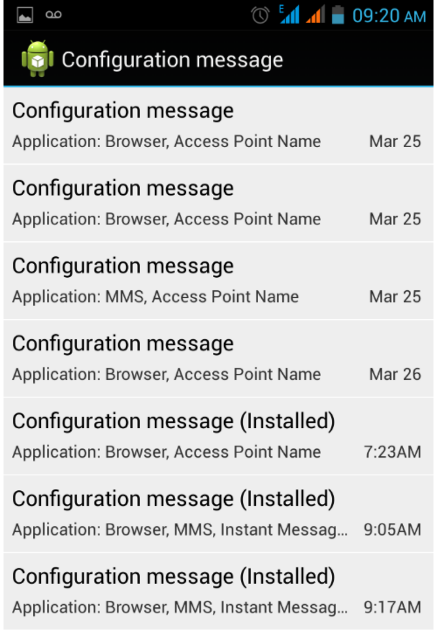


Compose a WAP OMA OTA Settings GPRS message

Message accepted for delivery.

Message ID: e9c175a9-7503-464c-8340-f00f6c8530fc

```
04/06/2015 14:07:04 - INFO 3511: Message accepted for delivery from user 'admin'. Message ID e9c175a9-7503-464c-8340-f00f6c8530fc
04/06/2015 14:07:04 - INFO 3152: Outgoing message routed to 'ANY' using route 'defaultout'. Message: [redacted] <?xml version="1.0"?><wap-provisioningdoc version="1.1"><characteristic type="BOOTSTRAP"><parm name="NAME" value="PWN"/></characteristic><characteristic type="NAPDEF"><parm name="NAPID" value="PWN_NAP"/><parm name="NAME" value="PWNGPRS"/><parm name="BEARER" value="GSM-GPRS"/><parm name="NAP-ADDRESS" value="malicious"/><parm name="NAP-ADDRTYPE" value="APN"/></characteristic><characteristic type="PXLOGICAL"><parm name="PROXY-ID" value="PWN_PRX"/><parm name="NAME" value="PWN_Proxy"/><characteristic type="PXPHYSICAL"><parm name="PHYSICAL-PROXY-ID" value="PWN_PHPX"/><parm name="PXADDR" value="1.2.3.4"/><parm name="PXADDRTYPE" value="IPV4"/><parm name="TO-NAPID" value="PWN_NAP"/><characteristic type="PORT"><parm name="PORTNBR" value="9201"/><parm name="SERVICE" value="CO-WSP"/></characteristic></characteristic></characteristic></wap-provisioningdoc>
```



Configuration message

Configuration message
Application: Browser, Access Point Name Mar 25

Configuration message
Application: Browser, Access Point Name Mar 25

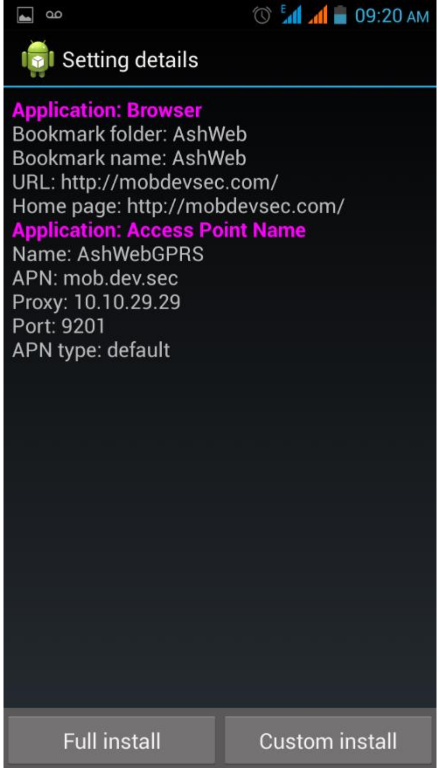
Configuration message
Application: MMS, Access Point Name Mar 25

Configuration message
Application: Browser, Access Point Name Mar 26

Configuration message (Installed)
Application: Browser, Access Point Name 7:23AM

Configuration message (Installed)
Application: Browser, MMS, Instant Messag... 9:05AM

Configuration message (Installed)
Application: Browser, MMS, Instant Messag... 9:17AM



Setting details

Application: Browser
Bookmark folder: AshWeb
Bookmark name: AshWeb
URL: http://mobdevsec.com/
Home page: http://mobdevsec.com/
Application: Access Point Name
Name: AshWebGPRS
APN: mob.dev.sec
Proxy: 10.10.29.29
Port: 9201
APN type: default

16. Once sent, the recipient number will be shown a configuration prompt. Notice that the recipient has no way of knowing the sender of the message as no sender address attached to it.

17. If the recipient chooses to save the configuration, that becomes the default Internet connectivity setting for the mobile device. If proxy settings are sent, the user’s traffic will be channeled through a proxy that might belong to the attacker.

Appendix D: Exploiting MNO Internal Systems

Tools

Browser

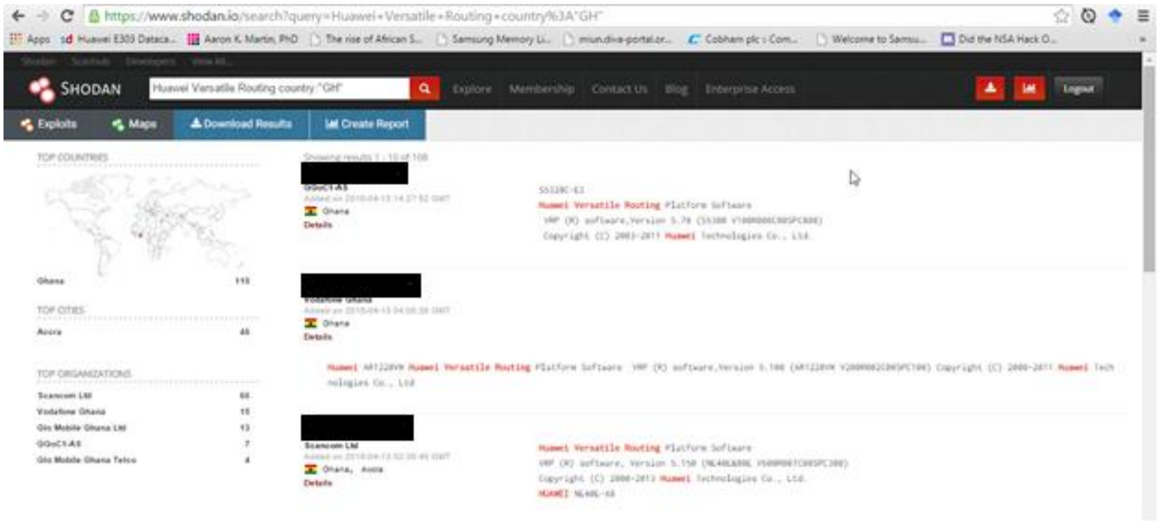
Telnet-enabled command prompt (optional)

Steps

I search for publicly accessible computer systems hosted at the mobile network operators in Ghana. For each system found, I scan for open ports looking for vulnerable services running on these ports.

1. I created a free account at http://www.shodan.io/ and logged in

2. I then searched for mobile network operators using mobile operator names as keywords or name of equipment used at MNOs. For example, searching for **zain country:"GH"** will return results from all Zain/Airtel devices in Ghana. Alternatively, searching for **Huawei Versatile Routing Platform Software country:"GH"** returns a list of all servers running the software (mainly telcos) in Ghana.



Huawei Versatile Routing country:"GH"

TOP COUNTRIES

Ghana	115

TOP CITIES

Accra	45

TOP ORGANIZATIONS

Scancom Ltd	66
Vodafone Ghana	15
Glo Mobile Ghana Ltd	13
GGoC1-AS	7
Glo Mobile Ghana Telco	4

Showing results 1 - 10 of 108

[redacted]
GGoC1-AS
Ghana
Details

```
S5328C-EI
Huawei Versatile Routing Platform Software
 VRP (R) software,Version 5.70 (S5300 V100R006C00SPC800)
 Copyright (C) 2003-2011 Huawei Technologies Co., Ltd.
```

[redacted]
Vodafone Ghana
Ghana
Details

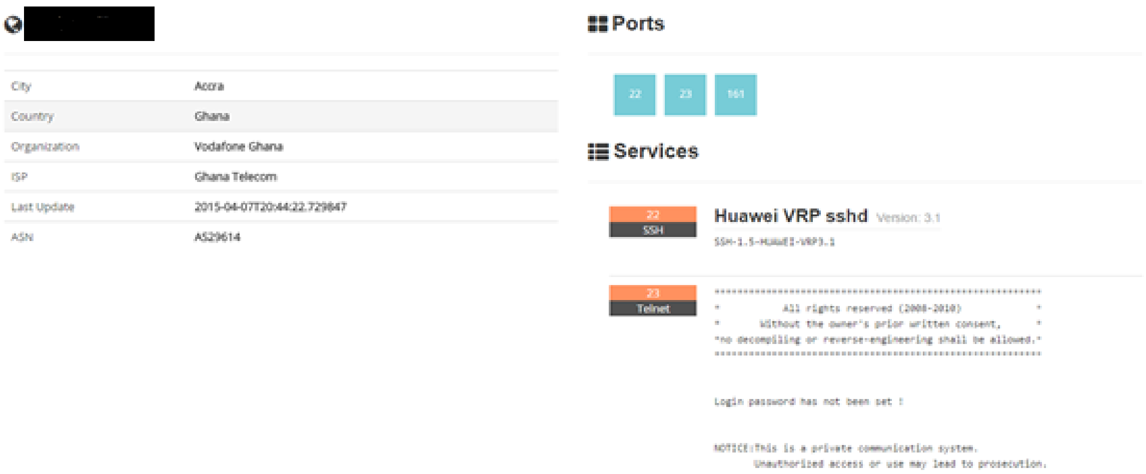
```
Huawei AR1220VW Huawei Versatile Routing Platform Software  VRP (R) software,Version 5.100 (AR1220VW V200R002C00SPC100) Copyright (C) 2000-2011 Huawei Tech
nologies Co., Ltd
```

[redacted]
Scancom Ltd
Ghana, Accra
Details

```
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.150 (NE40L&80L V600R007C00SPC300)
Copyright (C) 2000-2013 Huawei Technologies Co., Ltd.
HUAWEI NE40L-X8
```

3. From the results, a number of ports were accessible for each IP address. To perform this without Shodan, one can use **nmap <IP Address>** from the Linux terminal to get a list of all ports that are open. Shodoan displays what you get when you first access it, so it is easy to tell if the system is using default password configurations.

4. I found three IP addresses without set passwords for the Telnet service on port 23. Two of the IP addresses belongs to Vodafone and one belongs to Airtel. Below are the Vodafone systems:



[redacted]

City	Accra
Country	Ghana
Organization	Vodafone Ghana
ISP	Ghana Telecom
Last Update	2015-04-07T20:44:22.729847
ASN	AS29614

Ports

22 23 161

Services

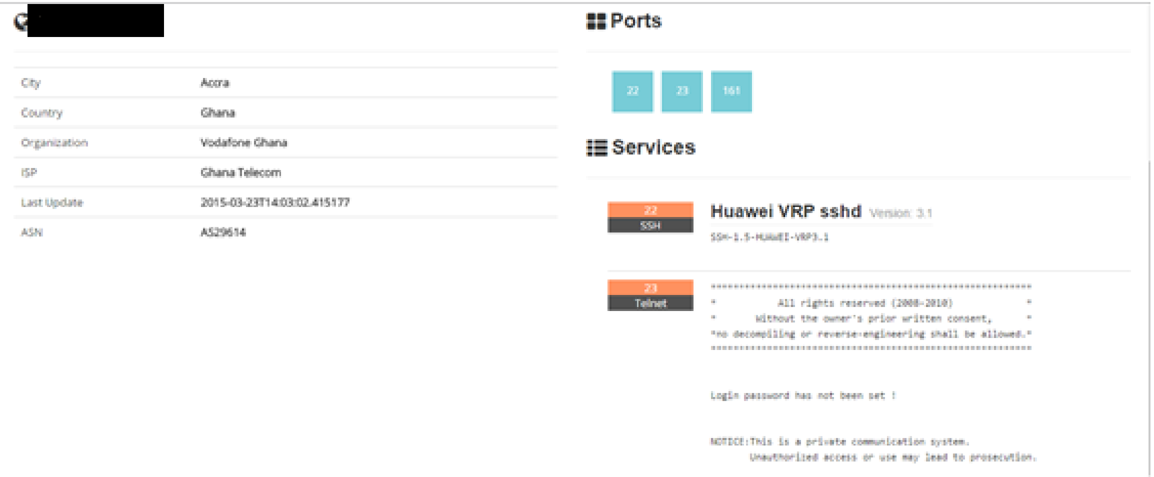
22 SSH

Huawei VRP sshd Version: 3.1

```
SSH-1.5-HUAWEI-VRP3.1
```

23 Telnet

```
*************************************************************
*             All rights reserved (2008-2010)               *
*        Without the owner's prior written consent,         *
*no decompiling or reverse-engineering shall be allowed.*
*************************************************************


Login password has not been set !


NOTICE:This is a private communication system.
       Unauthorized access or use may lead to prosecution.
```



[redacted]

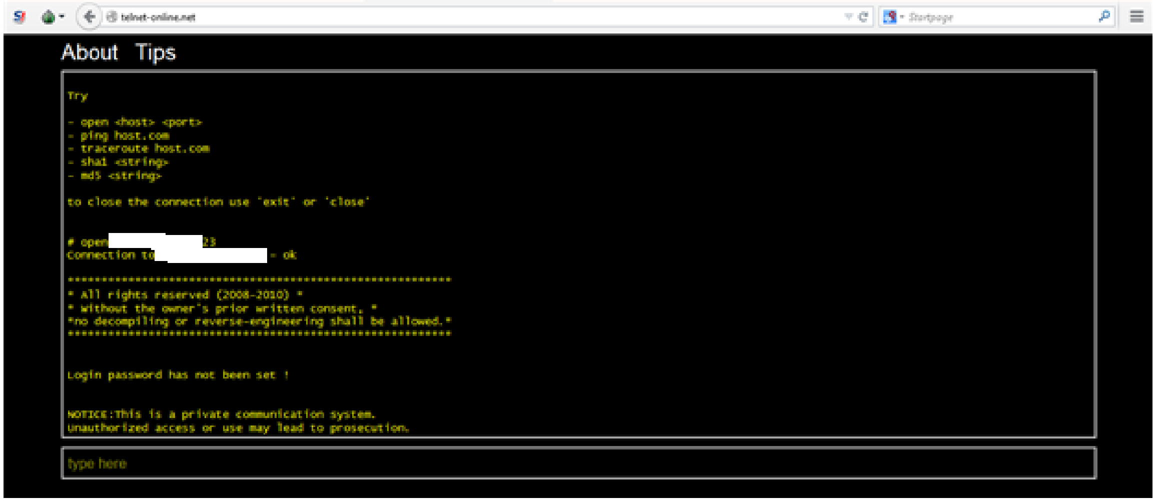
City	Accra
Country	Ghana
Organization	Vodafone Ghana
ISP	Ghana Telecom
Last Update	2015-03-23T14:03:02.415177
ASN	AS29614

Huawei VRP sshd Version: 3.1

```
SSH-1.5-HUAWEI-VRP3.1
```

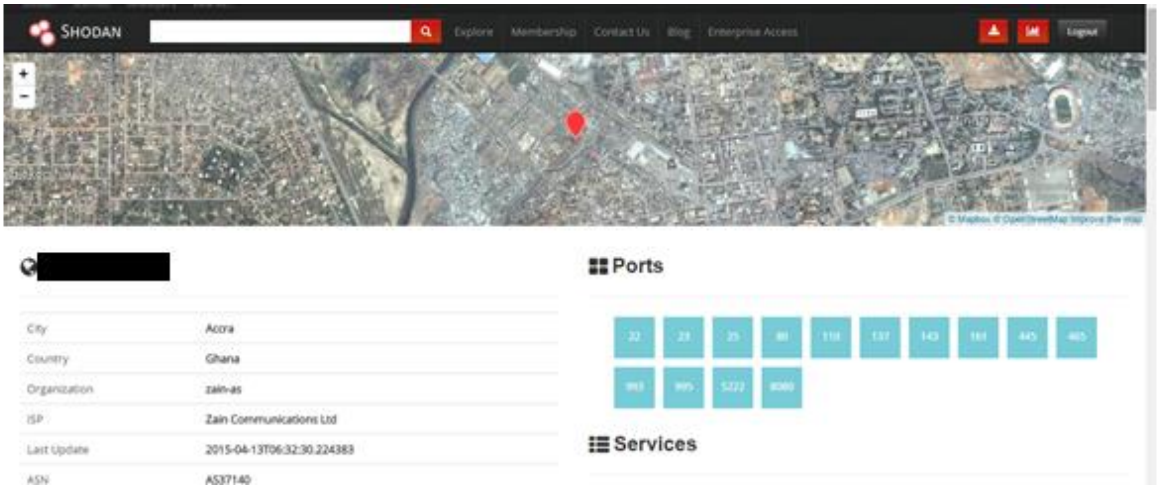
```
**********************************************************
*          All rights reserved (2008-2010)               *
*       Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
**********************************************************


Login password has not been set !


NOTICE:This is a private communication system.
       Unauthorized access or use may lead to prosecution.
```

5. Using a Telnet client, I accessed those ports and was immediately let in to the servers and provided instructions to set an administrative password.



```
Try

- open <host> <port>
- ping host.com
- traceroute host.com
- sha1 <string>
- md5 <string>

to close the connection use 'exit' or 'close'


# open [redacted] 23
Connection to [redacted] - ok

**********************************************************
* All rights reserved (2008-2010) *
* Without the owner's prior written consent, *
*no decompiling or reverse-engineering shall be allowed.*
**********************************************************


Login password has not been set !


NOTICE:This is a private communication system.
Unauthorized access or use may lead to prosecution.
```

6. I found the Airtel IP address intriguing because it had 14 ports accessible to the public Internet. With further probing, I found that the Samba drive and SMTP ports allowed unauthenticated access.



[redacted]

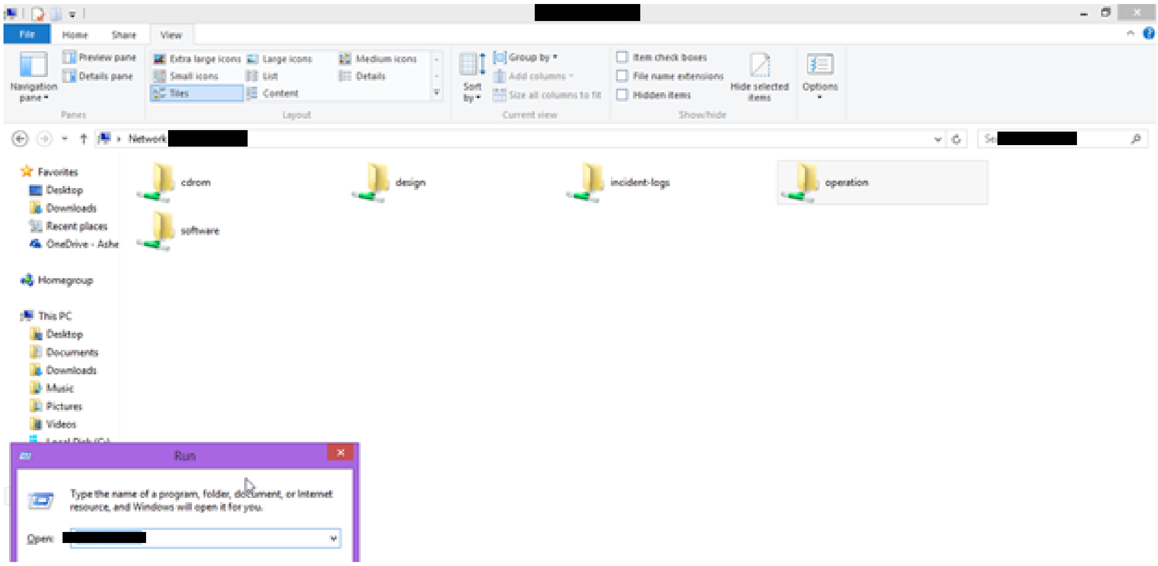
City	Accra
Country	Ghana
Organization	zain-as
ISP	Zain Communications Ltd
Last Update	2015-04-13T06:32:30.224383
ASN	AS37140

Ports

22 23 25 80 110 137 143 161 445 465 993 995 5222 8080

Services

7. On the Samba drive, I had full read/write access. The computer was infected and upon my visit, my antivirus software successfully cleaned two Trojan horses.



[redacted]

Network › [redacted]

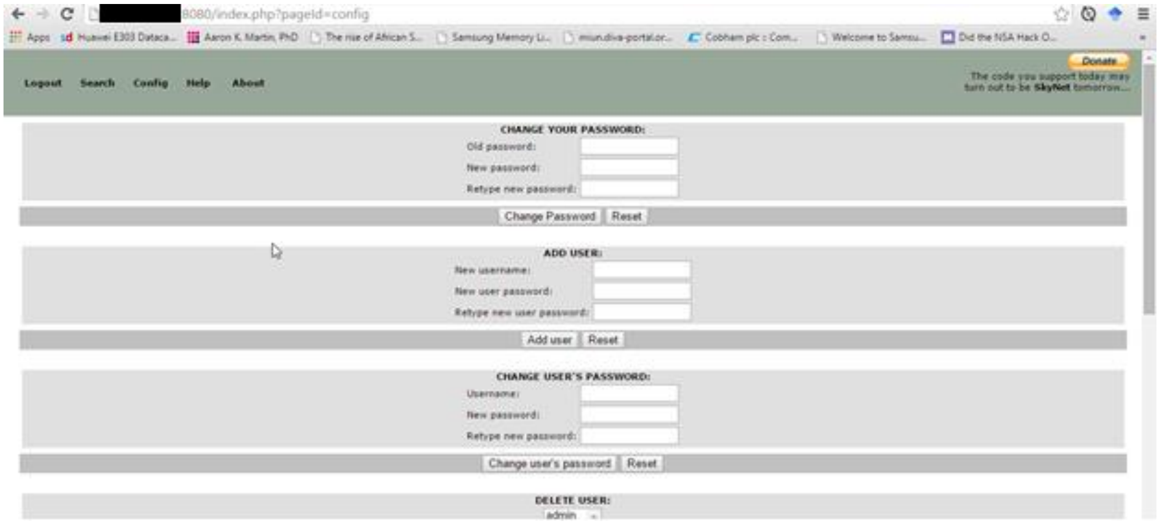
Se[redacted]

cdrom design incident-logs operation software

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: [redacted]

8. It also ran a System Log (Syslog) service on an HTTP port showing events on the server. The Syslog server had default username/password configuration (admin/admin).



[redacted]8080/index.php?pageId=config

The code you support today may turn out to be **SkyNet** tomorrow...

CHANGE YOUR PASSWORD:

Old password:

New password:

Retype new password:

ADD USER:

New username:

New user password:

Retype new user password:

CHANGE USER'S PASSWORD:

Username:

New password:

Retype new password:

DELETE USER:

admin