A Biometrics-Based Solution to Combat SIM Swap Fraud

Louis Jordaan, Basie Solms

A Biometrics-based Solution to Combat SIM Swap Fraud

Louis Jordaan and Basie von Solms

University of Johannesburg, Academy for Information Technology,
Cnr Kingsway and University Road, Auckland Park, 2006 Johannesburg, Republic of South Africa
louis.jordaan@gmail.com
basievs@uj.ac.za

Abstract. Cybercriminals are constantly prowling the depths of cyberspace in search of victims to attack. The motives for their attacks vary: some cybercriminals deface government websites to make political statements; others spread malicious software to do large-scale harm; and others still are monetary motivated. In this paper we will concentrate on "cyber fraudsters". At the time of this writing, a prime hunting ground for fraudsters is online banking. Millions of people worldwide use online banking to quickly and conveniently do their regular bank-related transactions. Unfortunately, this convenience comes at a price. By doing their banking online, they are vulnerable to falling prey to fraud scams such as SIM swap fraud. This paper explains what SIM swap fraud is and how it works. We will analyze the online banking payment transaction process to discover what vulnerabilities fraudsters exploit via SIM swap fraud, and then introduce a computer-based security system which has been developed to help combat it.

Key words: Cybercriminals, Fraud, Internet Banking, Online Banking, SIM Swap Fraud, OTP, Biometrics, BIO-Swap

1 Online Banking

Let's face it, the Information Age we live in today is significantly more fast-paced and demanding than a decade or two ago. There is no longer enough time in a day for people to finish all their work, chores and obligations. Spare time is a luxury; we do not want to spend it waiting in lengthy bank queues to do our banking transactions. We would much rather prefer to do our banking from the comfort of our home, office, or whilst enjoying a beverage at our favourite coffee shop.

Enter "online banking" (also known as Internet banking). Online banking is many banks' way of harnessing the power of the Internet to provide electronic banking services to their patrons. It allows people to remotely carry out most (if not all) of their regular banking transactions, 24 hours a day, 7 days a week, from

anywhere in the world an Internet connection is available. They simply have to open their browser, navigate to their bank's online banking website, select the appropriate transaction from a menu, and then follow the instructions on screen.

The ease-of-use, speed and convenience of online banking have lead to its widespread adoption by millions of people around the world. According to the 2009 Consumer Billing and Payment Trends Survey [1], in the United States 4 out of 5 (or 69.7 million) households with Internet access make use of online banking services. In the United Kingdom more than 50% of Internet-using adults now bank online [2] while in the less developed South Africa where a mere 10.5% of the population has Internet access [3], 75% of those fortunate people make use of online banking [4].

2 Online Banking Fraud

In the brick-and-mortar world banks can use thick concrete walls, strong safe doors, state-of-the-art alarm systems and armed guards to protect their money from the likes of Jesse James [5] and Butch Cassidy [6]. In cyberspace however, bank robbers do not attempt to break into a safe, or storm into a bank pointing guns at people and order the cashiers to hand over the money. No, they are faceless criminals who do not have to step foot into a bank to nick other people's money. Thanks to power of the Internet, they can do so remotely from the safety of their hideaway.

Banks therefore have to rely on firewalls and intrusion detection systems (IDS) to protect their Internet-connected computers and databases (where their clients' financial information is stored) against unauthorized access and tampering. These security measures work well to keep intruders out of a bank's computer network infrastructure, but the protection they offer is unfortunately limited to the nodes within the infrastructure's perimeter. By providing online banking services to its clients, a bank opens a new window of opportunity for fraudsters: the people who make use of the online banking services.

The level of computer literacy and information security awareness varies between Internet users. Many people are under the impression that everything on the Internet can be trusted (e.g. an e-mail from a claimed source has to be legitimate, right?) and are therefore rather clueless when it comes to protecting their personal information in cyberspace. This makes them easy targets for cyber fraudsters who are devising ever more sophisticated and cunning scams to defraud unsuspecting victims out of their hard-earned savings.

Business is booming for cyber fraudsters as recent studies (at the time of this writing) have shown that online banking fraud is rising rapidly. According to the Fraud the Facts 2009 report [7] that was published by APACS (the UK Payments Association), the losses to online fraud scams such as phishing and

spyware during 2008 totalled a whopping £52.5 million in the UK alone — An increase of more than 130% from the previous year (See Fig. 1). Another APACS study showed that online banking fraud losses for the first semester of 2009 totalled £39 million — A 55% rise on the figure for the same period of 2008 [8].

Fig. 1. Comparison of the annual losses to online banking fraud during 2004-2008. *Percentage values in grey* show the percentage change on previous year's total. [7]

Despite these alarming statistics, many banks encourage their customers to make use of online banking by claiming that their online banking websites are safe and secure. Studies by security experts such as Professor Atul Prakash and his students show otherwise. In 2006 they examined the websites of 214 financial institutions and found that 75% of the websites had at least one design flaw which cyber criminals could exploit to gain access to people's private information and bank accounts [9].

3 The Online Banking EFT Transaction Process

In an attempt to protect their clients from falling victim to online banking fraud, banks are integrating different security technologies into their online banking websites. A good example of this is two-factor authentication where banks require that a person needs to know the credentials (username and password pair) to gain access to an online bank account, as well as be able to provide a valid one-time password (OTP) when they wish to carry out certain transactions such as making a payment to a new beneficiary. An OTP is generally sent as an SMS

message to the cell phone number of the account holder. The idea is that an account holder should be the only person who knows what the username and password to their account is, and that only they will have the cell phone (to which the OTP is sent) in their possession.

Let's examine the actions that are involved in a typical online banking payment transaction; also known as an electronic funds transfer (EFT) transaction. The following points describe how an account holder and registered online banking user would carry out an EFT transaction via the online banking website of a reputable bank in the Republic of South Africa. Please note however that the details of the steps in a typical EFT transaction may differ slightly from bank to bank.

1. The account holder (say John), fires up his browser, navigates to the bank's website, and selects the online banking hyperlink.
2. The website will ask John for his bank account number and the corresponding security PIN (Personal Identification Number).
3. If a valid bank account number and PIN pair is submitted then the website will ask the John for his online banking password.
4. When the correct online banking password is submitted, the bank will send an SMS message to John's cell phone number to notify him that someone has just logged into his bank account: "Confirmation of Internet Banking logon with acc no. ending 0101. Date: 2010-02-16. Time: 22:10:59. Helpline: 08600 08600. Int no.: +2711 276 7900"
5. John can now carry out several online banking transactions, e.g. view the transaction history of his account, pay beneficiaries, etc.
6. In order to make a payment to a new beneficiary, i.e. somebody he has never transacted before, the new beneficiary must first be added to the list of payable beneficiaries.
7. To register a new beneficiary John simply needs to click on the appropriate beneficiary-related option on the website menu. As a security measure the bank will then send a OTP (sometimes referred to as a Random Verification Number or RVN) to his cell phone number: "RVN — Enter a39c0c9f sent at 22:15:33 2010-02-16, to continue with your Internet banking session. Helpline: 08600 08600. Int no.: +2711 276 7900". The online banking website will ask John to enter an OTP into an input field on the screen. Only when the correct OTP has been submitted will John be allowed to proceed to the next step in the beneficiary registration process where the beneficiary's details, i.e. name, account number etc., can be supplied.
8. Once the new beneficiary has been registered, John will be able to make payments to the beneficiary. He simply needs to start an EFT transaction by selecting the appropriate option on the website menu, then provide details for the transaction (i.e. beneficiary to pay, amount to transfer, payment date

etc.), and finally confirm that the transaction details that was submitted are correct.

At first glance the transaction process looks fairly secure. How could a cyber criminal possibly circumvent all the security barriers described above? As the following sections will explain, this is all in a day's work for an experienced fraudster.

4 Attack Vectors

From the discussion above we can identify 4 items of information that a fraudster would need to access an online banking user's account and carry out EFT transactions:

- The account number.
- The security PIN for the account number.
- The account holder's online banking password.
- The OTP which is sent to the account holder's cell phone number.

The first 3 items of information are fairly easy for a seasoned cyber fraudster to acquire — With local and remote attack vectors such as social engineering, phishing and spyware, online banking users can be duped to unwittingly divulge the secret information. Obtaining the final item of information (the OTP) however, is a whole new ball game. An OTP is randomly generated and is only valid for a single online banking session. The moment the online banking user logs out or closes their browser the OTP expires. Furthermore, the OTP is only sent to a single destination, namely the account holder's cell phone number. A fraudster will therefore have to find a way to intercept the OTP if he has any hope of successfully defrauding his target. But how would he accomplish this seemingly impossible task without the account holder's knowledge or consent? Enter "SIM swap fraud".

5 SIM Swap Fraud

"A Western Cape man was defrauded of more than R100 000 shortly before Christmas after he fell victim to a Joburg syndicate that illegally swopped his cellphone SIM card so that they could access his bank account. Barry Greyvenstein, from Grootbrak River in George, said he realised that something was amiss when he received a call from Absa Bank on the evening of Friday December 7 informing him of irregular activity on his bank account. But when he checked his phone, there was no signal - and he had become the latest victim of a new type of fraud, which earlier resulted in fraudsters plundering R90 000 from the bank account of a Cape Town NGO. This week Greyvenstein, who mainly uses internet and cellphone banking for transactions, said he was blown out of my boots' when he realised that MTN had performed a SIM card swop on his number without his knowledge or consent." [10]

5.1 What is SIM Swap Fraud?

SIM swap fraud is a cunning scam where fraudsters hijack a targeted online banking user's cell phone number in order to obtain the OTPs and security messages that the account holder's bank would send to the cell phone number during online banking transactions [11]. SIM swap fraud has in a very short period of time become a source of major concern for mobile network operators, banks and cell phone users alike. According to a report released by the e-commerce unit of the South African Police Service (SAPS) more than R80 million has been lost to SIM swap fraud in South Africa since February 2007 [12].

The scam works as follows:

- **Step 1: Gathering information**
  A fraudster may select a specific person as a target, or choose to target a random group of people with the hope that he will successfully defraud a few of them. Whatever the case, the first step entails collecting personal and confidential information about his target(s). Information of interest to the fraudster includes ID numbers, contact details, residential and postal addresses, banking details such as account numbers, credit card numbers, and online banking credentials (username and password). This is rather sensitive information which people will not willingly hand over to a just anybody, let alone a complete stranger who happens to be a fraudster. The fraudster will therefore have to make use of social engineering and phishing scams to trick his target(s) into disclosing their precious personal information.

- **Step 2: Requesting a SIM swap**
  Mobile network operators like Vodacom, MTN and Cell C know how inconvenient it is for their clients to lose their cell phone numbers when their SIM card is lost or damaged, or their cell phone is stolen. For this reason they offer a SIM swap service, which allows their clients to request a SIM card swap on their cell phone number in order to replace a lost, stolen or damaged SIM card while keeping their original cell phone number. When a SIM swap is performed, the old (lost, stolen or damaged) SIM card is disabled and the client's cell phone number is linked to a new (replacement) SIM card. All that the mobile network operators ask in return is a small fee, and that the person requesting the SIM swap can prove that they are the owner of the cell phone number by providing an identity document and correctly answering a set of personal-information-related security questions.

  Fraudsters exploit this SIM swap service that mobile network operators provide, to hijack their targeted victims' cell phone numbers. By masquerading as a targeted victim, a fraudster will ask a mobile network operator to transfer the victim's cell phone number to a SIM card in his possession. The information that was collected in step 1 is used to help convince the mobile network operator that the SIM swap request is "legitimate", i.e. that the fraudster is the lawful owner of the cell phone number.

– **Step 3: Looting the victim's bank account**
When the SIM swap is complete, it is a race against the clock for the fraudster to loot his target's bank account. He must act quickly, before the victim notices that their cell phone is no longer connected to a cell phone network, and therefore unable to receive phone calls and SMS notifications. The fraudster will use the credentials that were acquired in step 1 to log into the online banking website of the bank where the victim has an account. Upon successful login, the bank will send an SMS notification to the account holder's cell phone number to inform him/her about it, but because the fraudster has hijacked his/her cell phone number, the notification will be delivered to the fraudster's cell phone instead. The fraudster will then proceed to add one or more beneficiary accounts to the victim's bank account. To authorize the addition of any new beneficiaries, the bank will request an OTP which will be delivered via an SMS notification to the hi-jacked cell phone number. At this point the fraudster will be smiling as after entering the OTP, he can proceed to transfer funds into each of the beneficiary accounts, and finally, disappear into the vastness of cyberspace.

6 Problem Analysis

From the discussion above it is clear that there are 4 parties involved in a case of SIM swap fraud, namely:

– The fraudster
– The victim
– The victim's mobile network operator
– The victim's bank

While the fraudster escapes with the money, the latter 3 parties find themselves in a situation where they point a finger of blame at one another — They do not want to accept responsibility for their contribution to the fraudster's success in the scam with which they were fooled.

Online banking users — and Internet users in general — are expected to take best efforts to protect their personal information. Banks regularly warn their clients that they will never send them an SMS or e-mail which will ask them to click on a hyperlink that will take them to a website where they must update or confirm their online banking details. In spite of these warnings, there are people who still fall into a fraudster's phishing trap because the phishing e-mail/SMS is so cleverly designed and phrased that they believe it is an authentic e-mail/SMS from their bank. The victim is therefore guilty of compromising his/her personal information and online banking credentials when he/she fell prey to the fraudster's phishing scam(s).

Is it fair though to put full blame on the victim? Surely the bank cannot be

allowed to get away scot free because it displays security notifications to its clients from time to time. The bank is after all responsible for protecting its clients' money from criminals. But the bank's online banking system failed to recognize that it was not the true account holder that was logged in (Which begs questions about the effectiveness of the bank's online banking authentication system), and that there was abnormal behaviour (i.e. transactions) on the account. Consequently the fraudulent transactions were approved and the victim is left with a big void in his/her bank account.

Finally, the mobile network operator is guilty of carrying out a fraudulent SIM swap after failing to ascertain that the person who requested the SIM swap was not who they claimed to be. A forged or stolen identity document and the correct answers to a pre-known set of security questions was all the fraudster needed to deceive the mobile network operator and hijack the victim's cell phone number. Paper-based identification documents are no longer good enough — The speed of technology has far outpaced the security of countries' identity documents [13].

7 Proposed Solution

To effectively combat SIM swap fraud, focus will have to shift from protecting online banking users' personal information, to the second and most critical link in the SIM swap fraud scam: preventing unauthorized SIM swaps. As discussed earlier, a successful SIM swap is key to a fraudster's success as it allows the fraudster to intercept the OTP messages from a victim's bank. If a good security system is put in place here, the advantages will be twofold: cell phone subscribers will enjoy the peace of mind that their cell phone numbers are safe from being hijacked, and SIM swap fraudsters will be at bigger risk of getting caught and brought to book.

Enter "BIO-Swap" — Our proposed solution to address the issue of SIM swap fraud. Short for "Biometric-Swap", BIO-Swap is a biometrics- and Web-based proof-of-concept system which is designed to serve as a type of certification authority for people's identities. The idea is that BIO-Swap will vouch for registered cell phone subscriber's identity when they request a SIM swap from their mobile network operator. In layman's terms the BIO-Swap system will act as a trusted third party when SIM swaps are conducted: the mobile network operator will trust BIO-Swap to accurately verify whether a person is the legitimate owner of a given cell phone number, and the cell phone subscribers will trust BIO-Swap to protect their cell phone numbers from fraudsters.

8 The BIO-Swap System in a Nutshell

As mentioned earlier, BIO-Swap is a biometrics-based system. It uses the power of biometrics technologies to capture a person's biometrics, and to extract a set of biometric templates thereof. The acquired biometric templates are then

linked to the person's cell phone number as a hypothetical biometric lock which purpose is to protect the cell phone number against unauthorized SIM swaps.

Why did we opt for biometrics to replace traditional identification documents and security questions? Because a biometric of a person is a characteristic or trait of that person which distinguishes him/her from the other people on earth; the probability of 2 people sharing the same biometric data is virtually zero. Furthermore, biometric properties are extremely difficult to duplicate or share as they are intrinsic properties of the owner. Individuals can therefore be [uniquely] identified by their biometrics. [14]

A cell phone subscriber will need to register for the "BIO-Swap SIM Swap Service" if they wish to enjoy the protection that the BIO-Swap system has to offer. The registration process is quick and painless, and is carried out under the watchful eyes of a BIO-Swap supervisor who will assist and guide the cell phone subscriber through the process:

1. Say Mandy wishes to register for the BIO-Swap SIM Swap Service. The supervisor will first log into the BIO-Swap user interface and then proceed to ask her for a few items of personal information such as her name, surname, and a certified copy of her identity document. In addition, Mandy will have to provide cell phone-related information such as her cell phone number, contract number (if applicable) and her SIM card number.

2. Once the required information has been collected, the BIO-Swap system will connect to — and communicate with — the computer systems of Mandy's mobile network operator to verify whether the information that she provided (think contract number, SIM card number and personal details) is correct. This also serves as a notification to the mobile network operator that Mandy is attempting to register for the BIO-Swap SIM Swap Service.

3. If all the information that Mandy provided is correct and the mobile network operator has no objections to the BIO-Swap registration attempt, it will respond by sending an OTP via SMS to the cell phone number. This one-time password serves as a challenge to verify whether Mandy is the truly the owner of the cell phone number she is attempting to register for the BIO-Swap SIM Swap Service, or if she is a fraudster who has collected the information by means of a phishing scam. In other words, Mandy needs to prove that she has the cell phone number (i.e. SIM card to which the cell phone number is linked) in her "possession".

4. Say Mandy is the lawful owner and she receives the OTP from the mobile network operator. She will need to provide the OTP to the supervisor, who will then enter it in an "authorization code" input field on the user interface and submit it to the mobile network operator.

5. If the submitted authorization code is correct, the mobile network operator will approve the registration request and give the BIO-Swap system a green

light to proceed to the next step of the registration process, namely biometric enrollment. Otherwise, after 3 failed attempts to provide the correct OTP, the registration process will be terminated.

6. Say the correct OTP was submitted. The BIO-Swap system will now require Mandy's biometrics in order to complete the registration process. When the BIO-Swap biometric enrollment Java applet has finished loading into the browser, the supervisor will help Mandy to scan her biometrics with a biometrics scanner/reader. The prototype system that we have developed uses a fingerprint scanner to capture images of a random subset of a subscriber's fingerprints (Fig. 2).

7. When the required number of fingerprint images have been captured, the supervisor must authorize the captured biometrics with his password and a scan of one of his own fingerprints (which he enrolled when his supervisor user account was created). This serves as an assertion to the BIO-Swap system that he oversaw the capturing of Mandy's biometrics and that, to the best of his knowledge, there was no foul play involved.

8. The applet will then extract biometric templates from all of the acquired fingerprint images and encrypt the resulting byte arrays with the AES cipher [15], using the MD5 hash [16] of the password that the supervisor entered as a 128-bit encryption key. At this point there is no relationship between the original fingerprint images and the encrypted fingerprint template byte arrays, so the subscriber's biometric data is safe for transmission over the public Internet (I.e. there is no way to recover the fingerprint images from the encrypted biometric templates). In the event of a man-in-the-middle attack, the biometric data will be worthless to the interceptor.

9. The applet will now send the encrypted biometric data along with some meta-data to a remote BIO-Swap server. When the BIO-Swap server receives the data, it will retrieve the supervisor's password hash from a database, use it decrypt the biometric data, and then attempt to match the fingerprint template (that was captured in step 7 above) to one of the templates it has on record for the supervisor. If biometric authentication is successful (i.e. a match is found) the server will be assured that this is a legitimate enrollment request, and proceed to enroll Mandy's biometrics in a database and link it to her cell phone number. If biometric authentication fails however, the biometric data will be rejected and the enrollment process will fail.

That is all there is to registering for the BIO-Swap SIM Swap Service. From the moment a cell phone number has been registered, the owner can enjoy the peace of mind that BIO-Swap will use his biometrics to protect his cell phone number against unauthorized SIM swaps. When a SIM swap is requested on the cell phone number, the mobile network operator will refrain from following the standard SIM swap process, and instead entrust the task of identity verification and SIM swap authorization to the BIO-Swap system. The SIM swap requestor

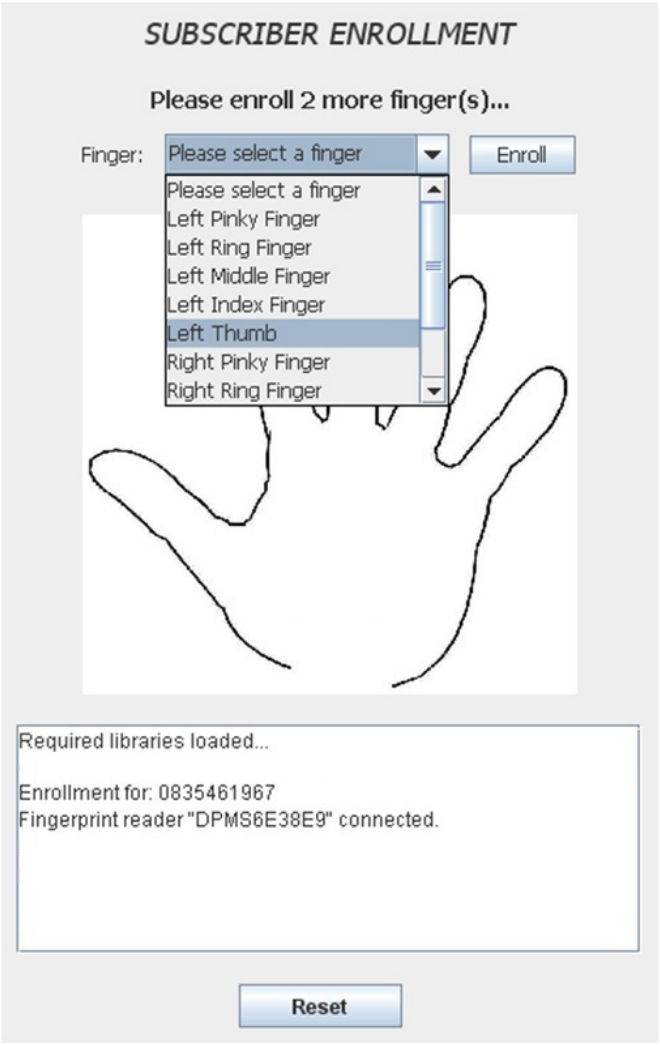

Fig. 2. The supervisor must select a finger to enroll.

will have to prove to the BIO-Swap system that he/she is the lawful owner of the cell phone number:

1. Following the use case described earlier, let's say a person who claims to be Mandy approaches her mobile network operator and requests a SIM swap on her cell phone number.

2. The BIO-Swap supervisor will search for the cell phone number or Mandy's details on the BIO-Swap system to see if the cell phone number has been registered for the BIO-Swap SIM Swap Service. If a record is found, the supervisor will select it and the BIO-Swap SIM swap Java applet will be loaded into the browser.

3. The BIO-Swap system will select a random subset of the fingers that Mandy had enrolled when she registered for the BIO-Swap SIM Swap Service. The person, who is requesting the SIM swap on her number, must now scan these fingers with the provided fingerprint scanner, under the supervision and guidance of the BIO-Swap supervisor (Fig. 3).

4. When the person has scanned all the fingers the applet asked for, the supervisor must authorize the captured biometrics with his password and a scan of one of his own fingerprints (which he enrolled when his supervisor user account was created). This serves as an assertion to the BIO-Swap system that he oversaw the capturing of the person's biometrics and that, to the best of his knowledge, there was no foul play involved.

5. As described earlier in step 8 of the registration process, the applet will create biometric templates from the acquired fingerprint images where after it will encrypt them for secure transmission over the public Internet.

6. Finally, the applet will now send the encrypted biometric data along with some meta-data to a remote BIO-Swap server. When the BIO-Swap server receives the data, it will perform biometric authentication on the supervisor's fingerprint, exactly as described earlier in step 9 of the registration process.

7. If biometric authentication of the supervisor's fingerprint is successful, the server will proceed to perform biometric authentication on the SIM swap requestor's fingerprints — It will retrieve Mandy's fingerprint templates from a database and compare it to the SIM swap requestor's fingerprint templates. If a match is found for each of the SIM swap requestor's fingerprint templates, the BIO-Swap system will accept that the person truly is Mandy, and give Mandy's mobile network operator a green light to conduct the SIM swap on her number.

   Otherwise, if single one of the SIM swap requestor's biometric templates does not pass biometric authentication, the BIO-Swap system will consider him/her a threat and a potential fraudster who is attempting to hijack Mandy's cell phone number. The SIM swap process will be terminated and

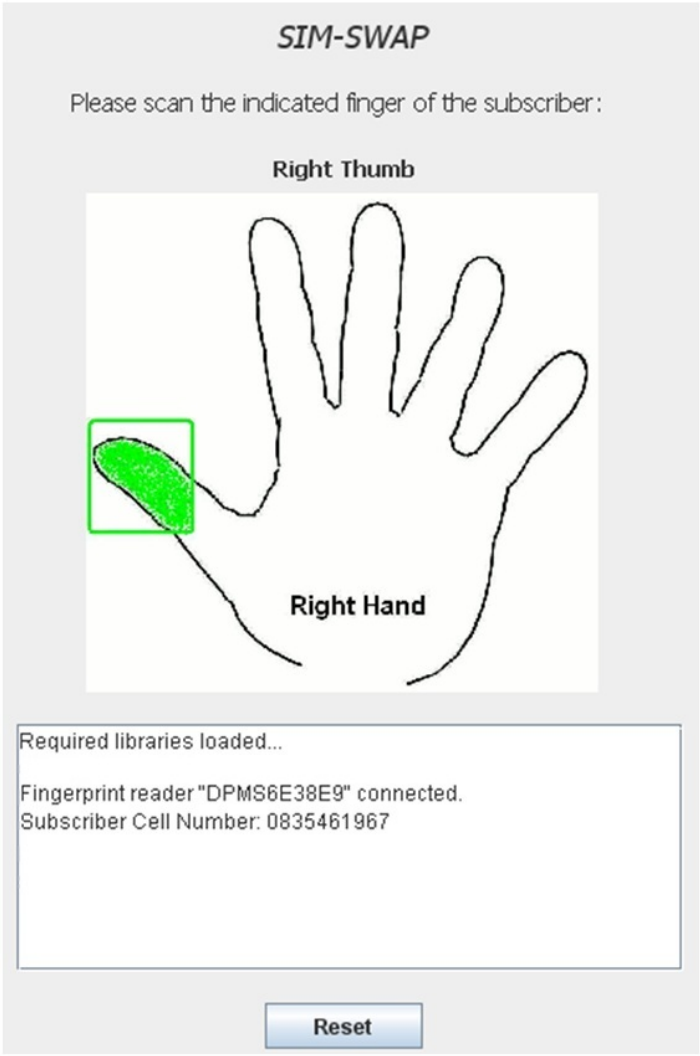

Fig. 3. The supervisor must scan the indicated fingers of the person who is requesting the SIM swap.

the SIM swap will consequently be denied. In addition, if BIO-Swap has been integrated with the computer systems of law enforcement agencies such as the FBI [17], the person's biometric templates could be compared against databases of biometrics of known criminals and fraudsters. If any matches are found authorities can be alerted.

This concludes the high-level overview of the BIO-Swap system. The next section will lift the hood of the BIO-Swap system to reveal what its main building blocks are, and how they work together to achieve its ambitious goal of combating SIM swap fraud.

9 The BIO-Swap System Architecture

The authors put a lot of effort, thought and consideration into the design and implementation of the BIO-Swap system. Factors like security [most importantly], efficiency, usability, robustness, availability and maintainability were high on the agenda. We visualized BIO-Swap from each of its end-users' perspective to identify what they would expect from it, and how it could win their trust. Furthermore, some of the latest (at the time of this writing) software frameworks were used to develop the system.

The result of the above was a prototype of a multi-part Web-based system which consists of 5 main components, each of which can function independently from the others. None of them are able to combat SIM swap fraud on their own though. Only when they work together as a unit, do they become a serious threat to SIM swap fraudsters. The 5 main building blocks[1] of the BIO-Swap system are:

- **The BIO-Swap Web application:** A Microsoft ASP.NET 3.5 Web application. It is the main graphical user interface (front-end) which authorized BIO-Swap users can use to interact with the BIO-Swap system and to access the functionality it has to offer. Depicted as "A" in Fig. 4.
- **The BIO-Swap Java applet:** A Java applet that gets embedded in some of the Web pages of the BIO-Swap Web application. It runs inside a client's browser, and its main functions are client-side biometrics acquisition and biometric templates extraction. In addition, the applet consumes the BIO-Swap Web service (discussed below) and calls upon its services when biometric data needs to be sent to the BIO-Swap Web server for processing (i.e. biometric verification during SIM swap requests) or storage in the database (i.e. biometric enrollment during subscriber registration). Depicted as "B" in Fig. 4.

[1] BIO-Swap is a fairly large and complex system. A detailed and technical discussion of its 5 main components was not possible in this paper due to the constraint on the allowed number of pages. Please contact the authors for more information.

- **The BIO-Swap Web service:** A Microsoft .NET Framework 3.5 Web service that serves as an interface between the BIO-Swap Web server and the client-side Java applet (discussed above). It exposes services to enroll the biometric templates of new subscribers into the BIO-Swap database, and to verify the biometrics of existing subscribers. Depicted as "C" in Fig. 4.
- **The mobile network operator Web service:** A Microsoft .NET Framework 3.5 Web service which provides a means for the BIO-Swap system to exchange information with a mobile network operator. It exposes services to validate the information of cell phone subscribers, and to send notifications to the computer systems of a mobile network operator. Any mobile network operator can integrate with BIO-Swap system by simply hosting a Web service which implements a common BIO-Swap-defined interface. Depicted as "D" in Fig. 4.
- **The BIO-Swap database:** A Microsoft SQL Server 2005 database in which BIO-Swap stores all its data, e.g. subscriber- and employee information, biometric templates, etc. Depicted as "E" in Fig. 4.

10 Pros and Cons

The positive and negative aspects of a computer system are often weighed against each other to assess how well it solves the problem that it was designed for. Let's compare the pros and cons of the BIO-Swap system to see how it fares.

10.1 Pros

On the positive side, BIO-Swap offers the following advantages to its users:

- It is safe and anonymous in the sense that no biometric images are ever stored on a hard-drive or transmitted over the public Internet — Only biometric templates are stored and transmitted.
- It is completely flexible with regards to biometric technologies because it is biometric template driven. Other forms of biometrics such as facial recognition, hand-, iris-, and retina biometrics are supported and can be easily integrated.
- It is completely Web-based. This allows for the effortless and centralized distribution of Web pages and necessary client-side software (e.g. the BIO-Swap Java applet) to remote computers.
- Biometric enrollment and SIM card swaps are carried out in a protected and controlled environment, under the watchful eyes of a trained supervisor. Successful biometric identification and verification within this controlled environment is a prerequisite of a SIM swap on a cell phone number that has been registered for the BIO-Swap SIM Swap Service.

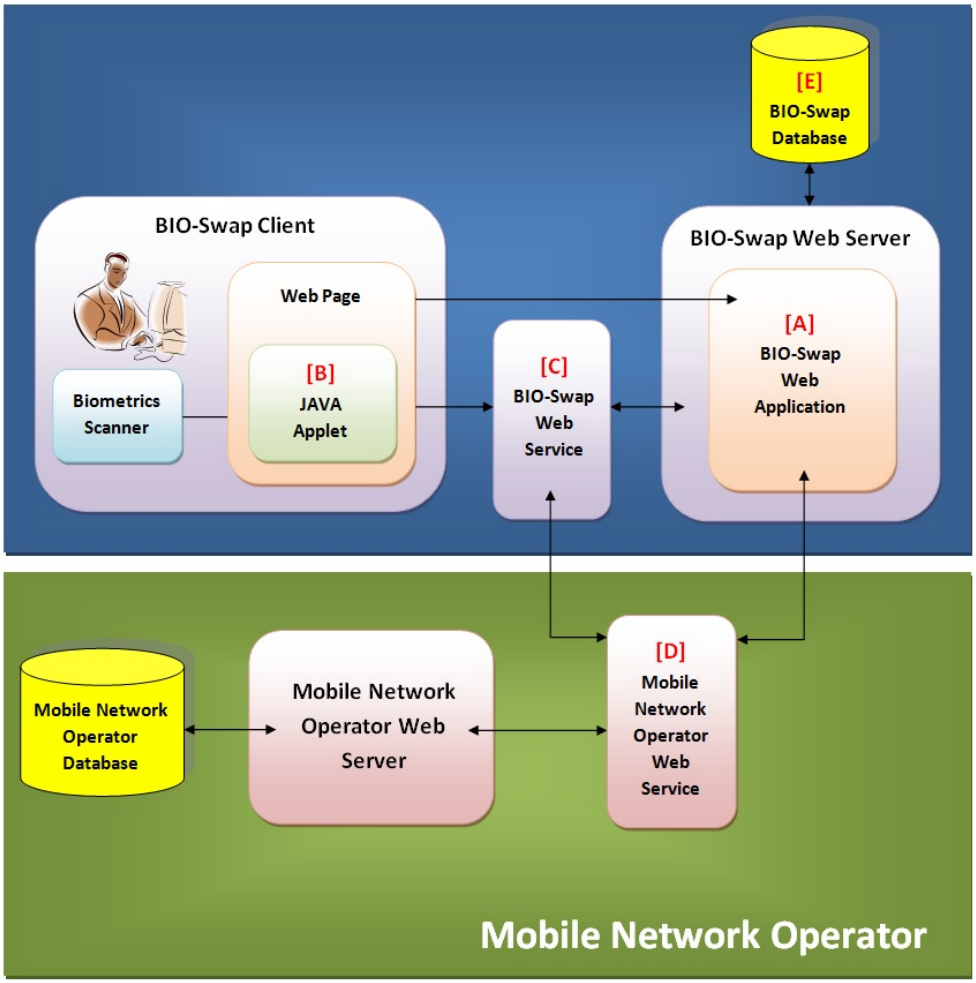

Fig. 4. The BIO-Swap architecture.The *arrows* indicate in what directions data flows between the components.

– It relieves mobile network operators of the difficult task of verifying whether a person is the legitimate owner of a cell phone number when a SIM swap is requested, and will accept accountability if fraudster manages to carry out an unauthorized SIM swap on a registered cell phone.

10.2 Cons

There is unfortunately no such thing as a 100% perfect and secure computer or software system [18]. The BIO-Swap system is no exception. Like every other man-made creation, it is not flawless:

– It is dependent on stable Internet connections because it is a Web-based system. Any network problems will therefore render the system non-functional, which could be a problem when an emergency SIM swap needs to be carried out.

– By using biometric technology, BIO-Swap inevitably inherits all the cons associated with it. This includes:
  - False acceptance rate (FAR). I.e. on rare occasions, the system may make a positive match between a scan of one person's fingerprint and another person's biometric template in its database.
  - False rejection rates (FRR). I.e. the system may occasionally fail to find a positive match between a scan of a person's fingerprint and their biometric template in its database.
  - On rare occasions the system may fail to enrol a person's biometrics because it is of very poor quality or badly damaged. Think of construction workers who have little or no fingerprints because the hand labour they do has worn it away.

From the points discussed above it is clear that the positive aspects of the BIO-Swap system far outweigh its negative aspects. The issues that are inherited from biometric technology will become less of a problem as the technology (i.e. biometric scanners, algorithms, etc.) improves over time. As for the dependency on stable Internet connections: Internet downtime is out of the control of the BIO-Swap system, but when it does occur it is usually resolved quickly because it is equally critical to the operation of many other organisations and computer systems. It is therefore fair to say that BIO-Swap has the potential to effectively reduce — maybe even eliminate — SIM swap fraud.

11 Summary and Conclusion

This paper started off with a discussion of online banking: the Internet-based service which evermore people across the world are adopting because it allows them to quickly and conveniently do their bank transactions from just about

anywhere in the world. As we saw from a few statistics however, this ease-of-use and convenience comes at a price. Online banking users are vulnerable to sophisticated online banking fraud scams that are master-minded and executed by cyber fraudsters. We saw that total annual losses to online banking fraud in the UK alone exceeded £50 million in 2008.

To determine what attack vectors a cyber fraudster could possibly use to defraud a victim, the online banking EFT transaction process was examined for vulnerabilities. We discovered that the mechanisms that banks have put in place to secure online banking transactions (at the time of this writing), can be circumvented via SIM swap fraud — A cunning scam where fraudsters hijack targeted victims' cell phone numbers in order to intercept the OTP messages that are required to authorize fund transfers to new beneficiaries. An analysis of what SIM swap fraud entails revealed that fraudsters are able to carry out illegal SIM swaps because mobile network operators rely on a set of security questions and identification documents to verify a subscriber's identity.

The paper then introduced a biometrics-based security system called "BIO-Swap" which the authors have developed to combat SIM swap fraud. We saw that BIO-Swap is designed to act as a certification authority for cell phone subscribers' identities, with the goal to prevent unauthorized SIM swaps. A brief run-through of the BIO-Swap registration- and SIM swap process was given to explain how BIO-Swap works, followed by a high-level overview of its main components. Finally, the positive and negative aspects of the BIO-Swap system were discussed.

To conclude: nothing is impossible for determined cyber criminals, but with the right tools and well-designed security systems we can make their lives extremely difficult. So much so that whatever they have to gain from their nefarious deeds will not be worth the effort and risk of getting caught.

References

1. Fiserv Survey Shows Online Banking Growing, Now Used by Four of Five Online Households, http://investors.fiserv.com/releasedetail.cfm?ReleaseID=396336
2. Half of UK net users bank online, http://www.finextra.com/news/fullstory.aspx?newsitemid=20938
3. South Africa Internet Usage and Marketing Report, http://www.internetworldstats.com/af/za.htm
4. Social networking in South Africa, http://mybroadband.co.za/news/Internet/11238.html
5. Jesse James Biography, http://www.biographybase.com/biography/James_Jesse.html
6. History of Butch Cassidy, LeRoy Parker, http://www.utah.com/oldwest/butch_cassidy.htm

7. Fraud the Facts 2009: The Definitive Overview of Payment Industry Fraud and Measures to Prevent it. APACS, London (2009)
8. Financial Fraud Action UK announces latest fraud figures, http://www.banksafeonline.org.uk/documents/2009H1FraudPressRelease.pdf
9. Security flaws in online banking sites found to be widespread, http://www.ns.umich.edu/htdocs/releases/story.php?id=6652
10. Beware SIM card swop scam, http://www.security.co.za/fullStory.asp?NewsId=5907
11. Protect yourself from fraud, http://www.standardbank.mu/portal/site/mauritius/menuitem.cb169d81ccc6cb0e7b6965103367804c/?vgnextoid=c3876ddd47d51210VgnVCM10000050ddb60aRCRD
12. Police probe SIM swap fraud, http://www.mydigitallife.co.za/index.php?option=com_content&task=view&id=1036940&Itemid=38
13. Fake IDs, Fake Passports Easy To Make or Buy, http://realtysecurity.com/blog/2009/03/16/fake-ids-fake-passports-easy-to-make-or-buy/
14. Biometric systems offer many important benefits, http://www.biometricnewsportal.com/biometrics_benefits.asp
15. The AES-CBC Cipher Algorithm and Its Use with IPsec, http://w3.antd.nist.gov/iip_pubs/rfc3602.txt
16. The MD5 Message-Digest Algorithm, http://www.ietf.org/rfc/rfc1321.txt
17. Federal Bureau of Investigation, http://www.fbi.gov/
18. Eugene Kaspersky: "no such thing as 100% secure software", http://www.pcadvisor.co.uk/blogs/index.cfm?entryid=104702&blogid=4