Secure Branchless Banking

Ashlesh Sharma
Department of Computer Science
New York University
New York 10012
ashlesh@cs.nyu.edu

Lakshminarayanan Subramanian
Department of Computer Science
New York University
New York 10012
lakshmi@cs.nyu.edu

Dennis Shasha
Department of Computer Science
New York University
New York 10012
shasha@cs.nyu.edu

Abstract

Providing basic financial services to rural people can enhance their security by eliminating the need for them to hold cash and can offer them alternative venues for borrowing. Placing a branch in rural villages is not however cost effective. In recent years, the concept of branchless banking has emerged in which a person who has a phone and sufficient liquidity (called a shopkeeper hereafter) acts as a bank agent. Others in the village (hereafter called farmers) perform withdrawals and depositions with the shopkeeper. Because the farmers and shopkeepers may not trust one another completely and the possibilities for fraud are legion, some form of security is needed. Because the farmers are unsophisticated, the protocols must be simple and intuitive. We present such a protocol that is robust to dishonest shopkeepers, farmers, and eavesdroppers. The protocol assumes that at least the shopkeeper has a phone and that the farmer can read numbers and can converse. The protocol makes use of secret lists of numbers delivered on scratch cards. A similar protocol can be used for non-monetary transactions, e.g. to ensure that the proper drugs are delivered.

1 Introduction

Traditional banking in rural areas does not work well [9, 8], because of poor transportation services, large distances, and the resulting high cost of delivery. Branchless banking, in which a resident of a village acts as an agent for a faraway bank, provides a way of connecting rural people to the banking world. It enables a host of services including simple withdrawals and deposits. It reduces two of the biggest problems to financial access: the cost of roll-out (the cost of having a physical presence) and the cost of low value transactions [9].

There have been many branchless banking initiatives around of the world. In the Philippines, Globe GCash a mobile banking initiative uses SMS to provide basic banking facilities. Transactions cost as little as 13 cents, whereas a bank wire transfer costs around $2.50 [5, 9]. A survey conducted in Brazil shows that around 90% of those surveyed used agents to pay their bills. Also, around 78% of the financial transactions are conducted through 95,000 agents distributed over the country [12, 9]. M-Pesa in Kenya, an SMS based financial transaction scheme, transfers around 20 million Kenyan Pesos per month. WIZZIT, is a successful mobile banking provider in South Africa that has seen its user base increase over the years.

The Branchless Banking survey conducted by CGAP [9] provide some insights. First, financial providers feel that agent networks are the key to extending the market. Banks and other MFI's create partnerships with local retailers and agents to provide banking services withing a region. Second, mobile banking providers prefer ease of use over rich functionality. One open issue has been security as existing systems allow the possibility of fraud.

In this paper, we provide a design for secure rural branchless banking using cellphones and using shopkeepers as agents. Our Farmer-Shopkeeper-Bank (FSB) protocol provides secure mechanism for deposits and withdrawals using insecure airwaves and in an environment where the farmer and shopkeeper may not trust one another completely (or may not know one another). Our protocol is highly scalable and provides a simple mechanism that can be implemented in a variety of ways. In this paper we provide the technical details of the protocol and do not delve into usability and user case studies, as the system is not yet deployed and is in its nascent stage.

Finally, because there is a direct analogy between a farmer withdrawing cash from a bank and a nurse withdrawing drugs from a truck, a very similar mechanism can be used to ensure that drugs are delivered to their intended destinations. The same holds for the delivery of other goods.

The paper is organized as follows. Section 2 presents a brief introduction to branchless banking, the security problems and the solution objectives. Section 3 introduces the FSB protocol and the assurances given at each point of the protocol. Section 4 describes various threats/attacks and how the protocol provides countermeasures against them. Section 5 describes voice verification and general system considerations. The conclusion summarizes the contribution of the protocols.

2 Scenario

For people in the developed world, living in a city without banking services would seem intolerably annoying. To rural people in the developing world, living in a village without banking services forces them to avoid banks. Traveling to a city to make a transaction is an enormous burden in cost and time for a poor person in a country having poor transportation infrastructure. Avoiding banks in turn implies that the rural poor must worry about the physical security of their cash (e.g. between harvest time and seed time) and may have to turn to local merchants for loans at sometimes exorbitant interest rates.

Traditional nationalized banks do not have branches in villages for lack of financial incentive. Poor people will deposit little and have poor or non-existent credit histories. Establishing a branch simply makes no economic sense.

Branchless banking has the following characteristics [9]:

1. Use of mobile phones or payment cards as a method of transaction. These are used for recording transactions and communicating with a bank. Surveys [10, 14] show that customers prefer mobile phones.
2. Use of a shopkeeper or other agent to act as a middleman who can handle physical cash, give receipts, and explain procedures.
3. Provision of at least basic banking services such as deposit and withdrawals from which more complex operations can be built.

Three features of agent based solution make it attractive for rural banking. First, shopkeepers and other retailers are already present in the market and understand it. Second, shopkeepers and agents provide a human touch to the banking process. Studies have shown that familiarity with the bankers provides additional confidence in the banking process and helps in its adoption. Third, customers need to have liquid cash. They need to be able to deposit and withdraw remotely, so a physical exchange of cash is essential and these agents and shopkeepers act as middlemen for these purposes.

A simple model of rural banking (using cellphones) primarily consists of deposit to/withdrawal from a bank account by a farmer (any person in rural area) in a remote location using the shopkeeper as the middleman. The following is the breakdown of the scenario,

1. The Bank assigns a shopkeeper in the village to be the middleman or agent who acts as a gateway for providing financial transactions.
2. The farmer must go to the Bank once to establish a bank account. After that, deposits and withdrawals can be done remotely with the help of the shopkeeper and cellphone.
3. The farmer (or any other person) goes to the shopkeeper, if he has to deposit or withdraw any amount to/from his bank account. Other services can be such as remote payments and money transfers can be built on these primitives.
4. The transaction is carried out on the cellphone of either the shopkeeper or the farmer but the shopkeeper dials.

Recently, finance and security experts have raised concerns about the lack of security in rural banking models [6]. People are not certain whether it is a safe way to conduct financial transactions [9]. Higher security might bring more users to use rural banking, but complex protocols may frustrate or confuse customers.

The highest level security goal is simply that the transactions recorded at the bank are exactly the transactions that the farmer and shopkeeper agree have occurred. This should be the case even if the farmer attempts to cheat, the shopkeeper attempts to cheat, or a third party eavesdrops on a conversation and attempts to cheat. This should also be the case even if the farmer cannot read (though we assume he or she can read numbers).

Besides these security goals, the protocol should satisfy the psycho-social goals of being intuitive and easy to verify by any intelligent person. Technically, the protocol should scale in the sense of supporting a large number of users at low cost.

3 FSB Protocol

This section presents an overview of a Farmer-Shopkeeper-Bank protocol that provides a secure approach to rural branchless banking.

3.1 Registration

Shopkeeper registration

The shopkeeper registers as an agent with the bank. The bank provides him with identity information consisting of his name and a unique number. The bank records the shopkeeper's voiceprint – whose contents consist of a unique number and his name. Also, the bank gives a sequence of random numbers $N_s = N_{s1}, N_{s2}, N_{s}3, \ldots, N_{sn}$ to the shopkeeper. N_s is a secret between the bank and the shopkeeper. This is a scratch card based check book, that is used by the shopkeeper to reveal N_{sj} in each transaction. The check book provides a carbon copy for each page. This carbon copy is kept by the shopkeeper after each transaction.

Farmer registration

The farmer visits the bank and opens an account. The bank provides him an identity consisting of his name and a unique number. The bank records the farmer's voiceprint whose contents also include the unique number and his name. The bank gives the farmer three sequences of numbers (random numbers) or nonces $X = X_1, X_2, X_3, \ldots, X_n$, $Y = Y_1, Y_2, Y_3, \ldots, Y_n$ and $Z = Z_1, Z_2, Z_3, \ldots, Z_n$. These random numbers (or updates to them) can also be sent through the postal service to the farmer. These numbers remain secret between the farmer and the bank. When the farmer needs X_i, Y_i or Z_i, he will scratch a card (or a region in the card) to reveal them.

3.2 Assumptions

We assume that the farmer (respectively, the shopkeeper) keeps his nonces secret until they are used. If they are stolen, a voice-print provides a defense, but that would entail dispute resolution.

3.3 Withdrawals

We first discuss the withdrawal protocol.

1. The farmer wants to withdraw money from his bank account and goes to the shopkeeper to start the transaction. This is the *i*th transaction the farmer does with some shopkeeper.
2. The farmer gives the *i*th number from the first set, X_i to the shopkeeper. The shopkeeper calls the bank and types in X_i, the farmer's id, his id and his *j*th nonce N_{sj}.
3. The bank checks the X_i, ids, nonce and returns back Y_i as a voice response back to the farmer on shopkeeper's phone. The farmer checks the bank's response nonce Y_i against his Y_i (second set of numbers) that he already has with him. If they match, then the farmer continues with the transaction in the assurance that the shopkeeper has dialed the bank. (If they do not match, then the shopkeeper may have dialed a different number.) If shopkeeper keys in a stale (used) X_i, then the bank does not return Y_i, but returns a negative response saying X_i used and ends the transaction.
4. The farmer or the shopkeeper keys in the following information: "withdrawal", amount and Z_i. Suppose, the shopkeeper calls his accomplice (in Step 1) and provides him X_i and then disconnects the phone. This provides the shopkeeper with X_i that is unused and not given to the bank, using which the shopkeeper can initiate a new transaction. To thwart this kind of attack, the farmer keys in or provides Z_i after confirming Y_i received from the bank.
5. The bank provides voice confirmation by repeating the type of transaction, the amount, Z_i, along with the current datetime, the farmer's name, and the shopkeeper's name. (Example: "S gives T amount of dollars to F on date time", where S is the name of the shopkeeper, F is the name of the farmer)
6. After receiving the bank's voice confirmation, the shopkeeper gives the amount to the farmer.
7. The farmer speaks his voiceprint (which he registered with the bank), and type of transaction which is withdrawal, amount, current date and time, his name and shopkeeper's name into the phone. The bank compares this voiceprint with the original voiceprint of the farmer and if they are the same (if the person is the same), it confirms the transaction, else it rejects the transaction.
8. The farmer signs a receipt containing the shopkeeper's secret nonce in a check book owned by the shopkeeper saying that he has received that amount. The shopkeeper countersigns. The shopkeeper gives the receipt to the farmer. The shopkeeper keeps a carbon copy of the receipt. This receipt is the physical confirmation to the farmer and shopkeeper of the transaction. In case of a dispute, the farmer has a physical proof of the transaction and then can check with the bank by providing the secret nonce of the shopkeeper. The shopkeeper also has a physical confirmation of the transaction.

3.3.1 Protocol for withdrawals

We explain the protocol for withdrawals using the security notation.

Preliminaries

Keyin represents typing on the phone, *Voicein* represents the farmer speaking into the phone. The first part of that speech is a phrase the farmer has already recorded at the bank consisting of a name and a personal identifier. *Voiceout* represents the voice response from the the bank. *Am* represents the amount/money. We assume without loss of generality that F is doing his *i*th transaction and S is doing his *j*th transaction.

1.	$F \rightarrow S:$	X_i, ID_F
2.	$S \rightarrow B:$	X_i, ID_S, ID_F, N_{sj}
3.	$B \rightarrow F/S:$	$Voiceout(Y_i)\vert stale(X_i))$
4.	$F \rightarrow B/S:$	$Keyin(W, Am, Z_i)$
5.	$B \rightarrow F/S:$	$Voiceout(W, Am, Z_i, datetime, Name_s, Name_f)$
6.	$S \rightarrow F:$	Am
7.	$F \rightarrow B/S:$	$Voicein(V_F(Name_f, p_f), W, Am, datetime,$
.	:	$Name_s, Name_f)$
.	$B \rightarrow F/S:$	$Accept/Reject$
8.	$S \rightarrow F:$	$Receipt(N_{sj})$

The explanation of the protocol is as follows:

1. F gives S X_i, the initiation nonce.
2. S calls up B and types in the initiation nonce X_i, his identity or account number ID_S, identity of F, ID_F and S's nonce N_{sj}. At that point, the bank knows that this transaction is from F and S.
3. B checks X_i, ID_S, ID_F, N_{si} and returns the confirmation nonce Y_i or if X_i is stale it says X_i was already used ($stale(X_i)$) as a voice response to F. F checks the authenticity of Y_i. At that point F knows that S has dialed B and not an imposter bank. S knows this already because S has done the dialing.
4. F or S keys in (types), the kind of transaction as "withdrawal" W, amount Am and nonce Z_i. Z_i ensures transaction security if S steals X_i by dialing to an accomplice in Step 1.
5. B provides a voice response which confirms to F and S that the transaction has been recorded with the correct amount, along with current datetime, farmer's name and shopkeeper's name. This enables F to be sure that S has typed in the correct information if S had done the keying and conversely if F had done the keying.
6. S gives the money Am to the farmer F as specified by W.
7. F provides his voiceprint $V_F(Name_f, p_f)$. B authenticates this V_F with the original V_F provided by F as defense against the theft of F's numbers. If they are the same, then the transaction is confirmed, else it is rejected.
8. F signs a receipt $Receipt(N_{sj})$ (containing N_{sj}) and S counter-signs it. The original $Receipt(N_{sj})$ is given to F. S keeps the carbon copy of $Receipt(N_{sj})$. Both S and

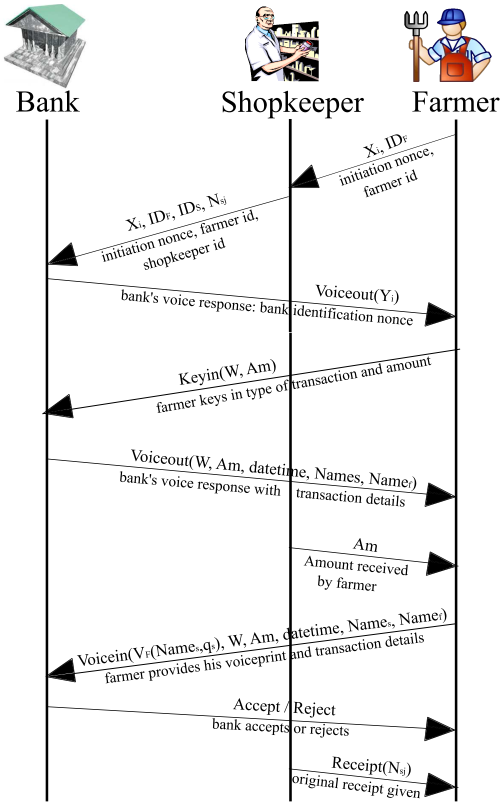
Bank
Shopkeeper
Farmer
Xi, IDF
initiation nonce, farmer id
Xi, IDF, IDS, Nsj
initiation nonce, farmer id, shopkeeper id
Voiceout(Yi)
bank's voice response: bank identification nonce
Keyin(W, Am)
farmer keys in type of transaction and amount
Voiceout(W, Am, datetime, Names, Namef)
bank's voice response with transaction details
Am
Amount received by farmer
Voicein(VF(Names,qs), W, Am, datetime, Names, Namef)
farmer provides his voiceprint and transaction details
Accept / Reject
bank accepts or rejects
Receipt(Nsj)
original receipt given

Figure 1: FSB Protocol: Withdrawals protocol

F have a physical proof of withdrawal.

In the protocol the notation $F \to B/S$ means that S is also the recipient of the message, as it is S's phone that is used for the transaction.

3.4 Deposits

This section presents the deposit protocol.

Preliminaries

The Deposit protocol is similar to Withdrawal protocol until step **5.**, although in steps **4.** and **5.**, the kind of transaction is marked as a deposit instead of a withdrawal. *Voicein* here represents the shopkeeper speaking into the phone. The first part of that speech is a phrase the shopkeeper has already recorded at the bank consisting of a name and a personal identifier.

1. $F \to S:$ X_i, ID_F

2. $S \to B:$ X_i, ID_S, ID_F, N_{sj}

3. $B \to F/S:$ $Voiceout(Y_i | stale(X_i))$

4. $F \to B/S:$ $Keyin(D, Am, Z_i)$

5. $B \to F/S:$ $Voiceout(D, Am, Z_i, datetime, Name_s, Name_f)$

6. $F \to S:$ Am

7. $S \to B/F:$ $Voicein(V_S(Name_s, q_s), D, Am, datetime,$

. $:$ $Name_s, Name_f)$

. $B \to S/F:$ $Accept/Reject$

8. $S \to F:$ $Receipt(N_{sj})$

The guarantees of the protocol concerning authentication and amount of transaction up to step **5.** are as before. From step **6.**, we proceed as follows:

6. The Am is given by F to S, since this is a deposit.
7. S speaks on the phone and provides the voiceprint $V_S(Name_s, q_s)$ as well as the fact that the transaction is a deposit, the current date and time, and the farmer's name and his name. Because this is a deposit, we do not need V_F. V_S is required to protect S as a second level of defense. Otherwise an imposter who had stolen S's nonces could create phantom deposits for which S would then be liable.
8. S signs a receipt $Receipt(N_{sj})$ (containing N_{sj}) and gives the original to F. S keeps the carbon copy of $Receipt(N_{sj})$. F and S have proof of the deposit. F need not counter-sign, as F has the $Receipt(N_{sj})$ signed by S as a proof of the deposit.

4 Security guarantees

This section provides a security analysis of the FSB protocol in three different ways: (a) a two stage analysis of of the FSB protocol where, (i) the Bank is trusted, (ii) the Bank is not trusted; and for two different forms of threats: (b) internal threats where one of the three parties (bank, shopkeeper or farmer) acts in a malicious manner; (c) external threats where an external attacker can launch different types of attacks to disrupt the FSB protocol. Using this analysis we show that the FSB protocol is secure in a variety of ways.

4.1 Analysis with respect to Bank

We have provided a detailed analysis of the FSB protocol in Section3. In this section, assuming the nonces X_i, Y_i and Z_i are secure, we provide an analysis of FSB protocol with or without trusting the Bank.

Trusted Bank

If the bank is trusted, then all the steps in the protocol remain the same except for saving the voiceprint in Step 7 ($F \to B/S$: $Voicein(V_F(Name_f, p_f), W, Am, datetime, Name_s, Name_f)$. The bank receives X_i and Z_i which ensure that the transaction is performed by the farmer, and Y_i received by the farmer ensures that it is indeed the bank. So, the voiceprint is not necessary in the protocol if the bank is trusted, as a secure channel is already established between the farmer and the bank using the nonces.

Untrusted Bank

If the bank is untrusted, then the saved voiceprint is necessary as the transaction details can be contested by the farmer or the shopkeeper. The bank can process the voiceprint in two ways. One, it can identify the voice of the farmer (V_F) or shopkeeper (V_S) in real time using automated voice identification software. This ensures the bank that it is indeed the farmer or the shopkeeper and also provides for easy voice identification if the transaction is contested later by the farmer/shopkeeper. The FSB protocol given in Section3, we assume that the bank is untrusted, as we use *Voicein* in Step 7 of the protocol.

Second, the bank can simply store the voiceprint as a proof of the transaction, and only when a transaction is contested by the farmer/shopkeeper, it can use use a group of people to identify the saved V_F/V_S with the original voice of the farmer or the shopkeeper.

4.2 Internal Threats

The first question is: how do the three parties authenticate themselves to the other two parties? In both Withdrawals and Deposits, the farmer, shopkeeper and bank have to be sure that they are communicating with each other and not with any imposter.

Shopkeeper and Bank

The shopkeeper is responsible for calling the bank and hence implicitly knows that he is contacting the bank. The bank verifies the identity of the shopkeeper by validating that the nonce N_{sj} is associated with the shopkeeper and hasn't been used before.

Farmer and Bank

The bank verifies the identity of the farmer by verifying that X_i is associated with the farmer and hasn't been used before. The farmer knows that the shopkeeper has indeed dialed the bank, as soon as the bank provides the confirmation nonce Y_i with a voice response.

Shopkeeper and Farmer

The shopkeeper can verify the identity of the farmer and vice versa because the bank announces the identities of the farmers and shopkeepers in its *Voiceout* message.

Other forms of internal threats with respect to the shopkeeper, the farmer and the bank are:

Shopkeeper faking a withdrawal

The shopkeeper cannot initiate the withdrawal without the farmer X_i's nonce. The shopkeeper cannot key in an incorrect amount of the withdrawal because of the bank's *Voiceout* message.

Farmer faking a deposit

The farmer cannot initiate a deposit without the shopkeeper N_{sj} nonce. The shopkeeper types in the amount and dials the bank.

Shopkeeper and Farmer collude

The shopkeeper or farmer cannot collude to game the system since any transaction is a zero sum game with respect to the bank (this is equivalent to two parties simply exchanging cash without the bank being in the loop). For every transaction in the FSB protocol, the recipient of the amount has to record his/her voice as proof to the bank and this voice is verified by the bank before transaction completion. Hence, the recipient cannot later claim that he/she did not get the amount.

Bank faking the details

The bank cannot fake a transaction (Withdrawal or Deposit) entirely because they must keep the *Voicein* report of the transaction. Further, the receipts $Receipt(N_{sj})$, provide physical evidence of the transaction. In addition, the Shopkeeper and Farmer can record the conversation (with the bank's message and telephone logs) to prove the authenticity of the transaction from their end. However, these protections will require dispute resolution to be effective. The bank has little incentive to be dishonest as they have a reputation to maintain.

4.3 External threats

We discuss various external threats and under the initial assumption that the nonces are secure, except for the last threat (Stolen nonces).

Eavesdropping

GSM standard uses A5/1 or A5/2 stream cipher [1] for encryption of over-the-air waves. Both A5/1 and A5/2 can be decrypted at considerable effort and expense [4, 7]. For each transaction in the FSB protocol, F's nonces X_i, Y_i and S's nonce N_{si} are keyed in. Even if an eavesdropper decrypts these nonces, they cannot be used for replay attacks as the bank or the farmer would detect the reuse of a nonce.

Spoofing

Spoofing cellphone and SIM

SIM card information and the IMSI (International Mobile Subscriber Identity) number of the cellphone can be spoofed [18] as this information is sent in plain text in most cases [4, 7]. Even with this information however, the attacker cannot initiate a transaction as he still needs nonces X_i, Y_i and N_{si}. Our protocol does not rely on a specific cellphone or SIM.

Spoofing the bank

An attacker may act as the bank by spoofing a nearby GSM cell tower. If the shopkeeper sends X_i to a fake base station b_s, b_s has to respond with Y_i. Provided Y_i is secure, spoofing the bank is not possible.

Inserting packets

Data packets can be inserted in real time over-the-air by decrypting the encryption scheme (A5/1 or A5/2) [3]. Decrypting the voice traffic and inserting fake or malicious information (like inserting fake amount) is time consuming and has not be done in realtime [4]. Instead, random rogue data packets can be inserted to the voice traffic. But, this can be easily detected at the receiving end at the bank which can then deny the transaction.

Stolen nonces

So far, we have assumed the nonces cannot be stolen. If they are, then there remain two lines of defense: the voiceprints V_F, V_S and the receipt. These are "soft" lines of defense in the sense that dispute resolution may be required, but they are effective nevertheless.

1. If X_i and Y_i are stolen, then the imposter cannot complete the transaction (Withdrawal), as his voiceprint will not match V_F in *Voicein*. Also there will be no signatures on receipts.
2. If N_{si} is stolen, then the imposter cannot complete the transaction (Deposit), as his voiceprint will not match V_S in *Voicein*. Also there will be no signatures on receipts.

5 Speech interface

The FSB protocol uses the speech interface for two purposes:

1. Authenticate F using voiceprint V_F in step **7.** of the Withdrawals protocol and authenticate S using voiceprint V_S in step **7.** of the Deposits protocol. Authentication means identifying the speaker only, not the content.

2. Record *Voicein* for the purpose of transaction verification in case of a dispute.

5.1 System

The FSB protocol uses lists of nonces, cellphones and voice calls for transactions. To achieve robust functionality, *B* uses the Asterisk based Interactive Voice Response(IVR) system [2]. Asterisk is an open source multiplatform PBX solution that provides features both for traditional telephony services like call waiting, call hold, etc. and modern features for VOIP. Voice is recorded using the *Call Record* feature. The IVR prompts for the voiceprint and *F* speaks his voiceprint which is also recorded and sent for processing via the Asterisk Gateway Interface. The voiceprint is then processed and based on the result, the IVR responds whether the voiceprint was genuine or not.

5.1.1 Voiceprint Authentication

Voice based authentication is easy to use, non-intrusive and is widely accepted by users [11, 16]. Voice-based authentication systems are being used by various companies [16] as part of their user authentication process.

In FSB, we want to verify whether the candidate waveform matches the original waveform of voice verification in the possible presence of noise. It is a text-dependent voice identification process and this type of system is being deployed in Turkey by Vodafone Turkey called VocalPassword [17, 15]. In an ideal environment, the identification is accurate, but in developing region where the environment is quite noisy and far from ideal, the accuracy of voice identification might not be accurate. To improve this text-dependent voice identification, when the farmer and shopkeeper register with the bank, they can repeat their voiceprints or vocal passwords under different settings, which would help in voice identification at a later stage. The verification of the voiceprint is performed by computing the correlation of the waveform of the voiceprints in the frequency domain. As noise does not affect all frequencies equally, an approximate search is possible. Details will follow in the full paper.

6 Existing solutions

We compare the existing solutions in branchless banking or more generally in mobile banking with our FSB protocol. The two successful mobile banking initiatives are M-PESA and GCash. We compare these systems with our protocol under three categories: i) Functionality, ii) Security, and ii) Ease of use

Functionality

M-PESA and GCash provide person-to-person money transfers, deposit/withdrawal, payment of utility bills and similar functionality. They are currently operated by regional mobile service providers and do not directly interact with the regional or national banks. Recently, GCash has tied up with Bank of the Phillipine Islands (BPI) [13] to provide mobile banking facility, for which the it requires users to have smartcards issued by BPI. M-PESA is largely used for person-to-person transfer money and paying utility bills. If a user wants to convert his mobile money (virtual money) to cash, then he has to approach a nearby M-PESA agent to convert his virtual money to cash.

In FSB protocol, the users (farmer and shopkeeper) interact directly with the bank, and provide basic functionality of deposit and withdrawal of money. In our protocol, the farmer need not have a cellphone and he can completely depend on the shopkeeper for his banking needs. The shopkeeper acts as an agent between the shopkeeper and the bank. The concept of agent is similar to M-PESA or GCash, where the agent provides the money to the user.

Security

M-PESA and GCash use SMS (Short Message Service) as the underlying communication channel to send messages and transfer money. As discussed in Section 4.3, SMS might be subjected to various types of attacks, which would jeopardize the virtual money transfer. A detailed security analysis of M-PESA or GCash would provide much needed respite against this argument.

In FSB protocol, we use the cellphone voice channel as the communication medium between the users and the bank. Voice channel is secure against various types of attacks and provides better security than SMS [4].

Ease of use

M-PESA and GCash use cellphone and SMS to transfer money, and the user studies show that they have significant user base in both Kenya and Philippines. The simple menu based system, to transfer money through SMS is easily adopted by users. Also, it would be fairly easy to use the system after some amount of practice.

In FSB protocol, the users use voice and key in numbers, which is similar to SMS in terms of usability. We do not have detailed user studies, as the FSB protocol is still under development and we plan to test and deploy it in the near future.

7 Conclusion

We have presented a simple cellphone-based protocol for secure branchless banking in rural villages that assumes only that a farmer (or other unskilled worker) can read numbers and understand voice recordings. The protocol supports withdrawal and deposit, the two basic operations upon which other operations (e.g. transfers, pre-payment) can be built. The same protocol can be used to do remote confirmation of the delivery of non-financial goods (e.g. drugs, building supplies, food).

8 References

[1] GSM Security Algorithms. http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm.

[2] Asterisk. http://www.asterisk.org.

[3] Valer Bocan and Vladimir Cretu. Threats and Countermeasures in GSM Networks. *Journal of Networks*, 1(6):18–27, 2006.

[4] The Hacker's Choice. http://wiki.thc.org/gsm.

[5] Globe GCash. http://gcash.globe.com.ph/.

[6] Globe GCash. http://www.234next.com/csp/cms/sites/Next/Home/5413169-146/Branchless_banking:_Uncertainties_emerge.csp.

[7] David Hulton. Intercepting GSM traffic. In *BlackHat Briefings*, March 2008.

[8] Gautham Ivatury. Using technology to build inclusive financial systems. In *CGAP Focus Note 32*, Washington D.C., 2006.

[9] Gautham Ivatury and Ignacio Mas. Early experiences with branchless banking. In *CGAP Focus Note 46*, Washington D.C., 2008.

[10] Gautham Ivatury and Mark Pickens. Mobile phone banking and low-income customers. *Vodafone Group Foundation and United Nations Foundations in collaboration with FinMark Trust*.

[11] S. Liu and M. Silverman. A practical guide to biometric security technology. *IT Professional*, 3(1):27–32, Jan/Feb 2001.

[12] CGAP 2006: Survey of branchless banking in Pernambuco, Brazil. http://cgap.org/portal/site/
Technology/research/technology/agents/.

[13] Bank of the Philippine Islands. http://www.bpiexpressonline.com/.

[14] Tapan S. Parikh, Paul Javid, K. Sasikumar, Kaushik Ghosh, and Kentaro Toyama. Mobile phones and paper documents: evaluating a new approach for capturing microfinance data in rural india. In *CHI*, pages 551–560, 2006.

[15] PerSay. http://paysay.com/vocalpassword.asp.

[16] TradeHarbor$^{\text{TM}}$ The Voice Signature Company. http://www.tradeharbor.com/.

[17] Vodafone Turkey rolls out Voice Identification Service. http://wirelessfederation.com/news/16761-vodafone-turkey-rolls-out-voice-identification-service/.

[18] Turbo SIM. http://en.wikipedia.org/wiki/Turbo_SIM.