The use of smart cards to perform ATM transactions in an off-line environment (May, 2005)

A.M Rossudowski[1], H.S Venter[2]
[1]maciej@webmail.co.za, [2]hventer@cs.up.ac.za
Information and Computer Security Architectures Research Group (ICSA)
Department of Computer Science, University of Pretoria

Abstract – Automatic Teller Machines (ATMs) are a necessity in the modern world. They facilitate in the distribution and easy access to money. The clients of banks do not need to visit a bank in order to obtain money, when an ATM will do. In addition, due to the compact design of an ATM, they can easily be spread in and around a city, or even temporarily located at major people gathering events. Whilst these ATMs afford us the luxury of having money-on-the-go, bank balances permitting, they are absolutely worthless if a communication failure occurs and, thus, the ATM cannot dispense money. This paper demonstrates the role smart cards can play in eliminating this problem. It shows how adequate security measures, such as Personal Identification Number (PIN) verification, can be attained in an off-line environment. In addition, it demonstrates how synchronization, with the use of transaction time stamps, plays a vital role in maintaining the integrity of bank records.

Keywords: smart card, automatic teller machine, ATM, transactions, communications, off-line, security, synchronization.

I. INTRODUCTION

"*Money moves the world*" – this is a statement that is true no matter what field of expertise people work in; a universal constant. Money has become an integral part of society today, with people performing numerous transactions daily. While more and more transactions are becoming electronic i.e. credit card transactions, physical transitions (where the exchange of physical money, be they coins or notes) are still a certain reality. To facilitate the ever demand for cash, banks have placed numerous Automatic Teller Machines (ATMs) in and around cities to aid in the distribution of money to their clients. Thus, ATMs have allowed clients to withdraw money from their bank accounts without the need to physically visit their bank.

Although, we do not live in a perfect world and interruptions to the status quo of ATMs is always a possibility. The two main interruptions that have the largest impact on our daily lives are power failures and communication breakdowns. Both of these types of interruptions have a signification effect on the way that we perform a transaction. Most businesses need the use of computers to run the company or to perform some transaction, hence, in the event of a power failure and without any backup generators, the company ceases to function. In the case of communications failure, consider a company using a distributed database. If the network fails, no information can be retrieved or updated in the database, also ceasing the functionality of the company. Consider the scenario where a client needs to withdraw money in order to acquire some goods. Hence, he goes to an ATM to withdraw the required money only to find out that he is unable to, due to either power failure or communication breakdown or both. As a result, the client is inconvenienced by not being able to withdraw the required money, and thus, not able to perform the desired purchase transaction with some merchant. In addition, the bank loses out on the transaction by not being able to claim service fees for the withdrawal.

Power failure problems can be easily overcome with the use of Uninterrupted Power Supplies (UPSs) or electrical generators. This might be economically unviable as an ATM does not provide a critical function or service, unlike life-support machinery within a hospital. Therefore, this is beyond the scope of this paper. This paper proposes a model to show that a communication failure is no reason why a transaction cannot be fulfilled at an ATM. It presents a model showing how transactions can be performed at an ATM during communication breakdowns and how the various security concerns, such as Personal Identification Number (PIN) verification, are dealt with.

The paper delivers background information on ATMs, communication channels and smart cards in the next section. This is followed by the proposal of this paper in the third section. The fourth section deals with discussion points and various scenarios regarding the proposal. The fifth section delivers a summary and conclusion.

II. BACKGROUND

Below, information on the functionality of an ATM is discussed in the first section. The second section handles various aspects of communication channels. The third section will introduce the technology behind smart cards.

A. Automatic Teller Machine (ATM)

A standard ATM is a rather simple machine consisting of two input devices: a card reader and a keypad. Four output devices: a display screen, a speaker, a receipt printer and a cash dispenser [1]. Whilst ATMs are being developed to allow for better security features, such as the introduction of biometrics [2], their functionality needs to be optimized to allow for convenient and friendly user interaction [3], [4]. An ATM is connected to a host computer via a permanent leased-line; the host computer is then, in turn, connected to the bank's computer also on a permanent leased-line. Thus, the bank computer, host computer and ATM form a clustered node network as shown in figure 1. A clustered

node network consists of several ATMs connect to a single host computer, and several host computers connected to the bank's computing infrastructure [5].

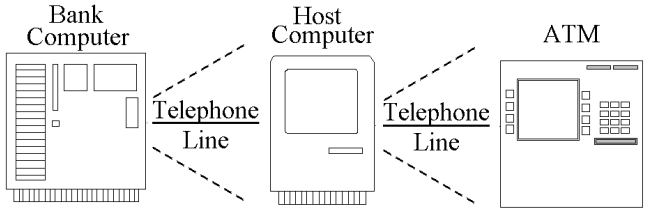

Fig. 1. An ATM cluster node network

For any type of transaction, all information is first routed to the host computer from the ATM, which then routes the information to the bank's computer. Due to the fact that these communication lines are permanent leased lines, outside intrusions are very difficult. Therefore, the PINs used for authorization purposes are always encrypted, whilst, all information sent over both channels may not necessarily be encrypted. Hence an ATM acts as a dumb terminal. No processing is done at the node itself (ATM). It is important to note that the host computer is usually controlled by some third party. In South Africa, this third party is actually an application called SASWITCH [6]. In America the host computers and ATMs are strongly privatized and can belong to a host of various companies. These third party companies allow clients to withdraw money from their bank account even if they are not using an ATM that belongs to their bank. The routing to the source bank is done by the host computer, usually for an additional surcharge.

For any ATM transaction there are two communication channels involved in connecting an ATM to a bank, either which can fail. If a communication channel between an ATM and a host computer fails, then only one ATM is affected. A more serious problem lies in the fact that if a communication channel between a host computer and a bank's computer fails, then an entire node cluster is isolated, compounding the problem several fold. Communication channels are discussed in the next section.

B. Communication Channels

Communication channels are the paths with which all information is exchanged between two or more points. Various types of communication channels exist, due to their different characteristics, such as: speed of communication, signal-to-noise ratio, cost and susceptibility to interference amongst others [7]. These different characteristics are taken into consideration whenever a new communication channel needs to be implemented, used or built Two main characteristics will be expanded on, namely: physical channels and channel bandwidth and capacity.

1) Physical Channels

Physical communication channels form the current standard in creating a communication path, such as in telephone networks. The benefit of physical channels is that they are not connected to the local electrical grid, but usually to an independent power supply (as is the case for telephone networks). Still, if these independent power supplies fail, a communication breakdown occurs.

2) Channel Bandwidth and Capacity

Channel bandwidth and capacity are two different concepts. Channel bandwidth refers to the frequency that is used to communicate information over the channel. Capacity describes the amount of information that can be processed/transmitted through a channel at any given point in time at a specific frequency (bandwidth) [7]. The capacity of a communication channel is dependent on the bandwidth used and the signal-to-noise ratio present in the channel, this is called the Shannon capacity [7]. The capacity of the different channels varies according to the purpose and application of the channel.

The next section discusses smart cards and their ability to provide processing logic.

C. Smart Cards

Smart cards typically look very similar (if not exactly) like a credit card, though, the size of the card may vary according to the application it is being used for. A smart card contains an embedded microchip to perform processing, and some form of memory to allow information to be stored on the card [8]. The most common type of smart card available today is a Subscriber Identity Module (SIM) card for cellphones. Most smart cards require some form of a PIN to be entered to allow access to the information stored on the card, and have the ability to lock themselves or to permanently cease functionality if the incorrect PIN is entered several times. The smart card market segment is growing with various current applications [9]. Application such as the use of prepaid telephone cards in the telecommunications industry, various access-control systems and the Home Affairs National Identification System (HANIS) project in South Africa [10]. Even though, the processor on the card is rather limited in its processing capability, research has shown that smart cards can play a key role in security and privacy [11].

Smart cards come in various configuration types:

- Contact type – the card contains physical contact points to interface with the card.
- Contactless type – the card has a built-in antenna to interface with the card.
- Dual type – a combination of the above two types.
- Hybrid type – come in various configurations with the most common being a smart card with a magnetic strip. These types of smart cards are typically used in conjunctions with dual level security. The magnetic strip on the card is used to allow large volumes of people through a low priority control point, such as an entrance gate to a company. The smart card is used for authentication at high priority control points, such as a critical area in a department of a company.

The next section discusses various attack methods and associated protection mechanisms for smart cards.

1) Smart Card Security Attacks and Mechanisms

Due to the ability of smart cards to store greater quantities of information than the more widely used magnetic strip cards, the way in which this information is secured on the card, is of great importance. Smart cards have a greater protection mechanism over magnetic strip cards, due to the embedded nature and the processing ability of the chip on the smart card [12]. Due to the quantity and usually sensitive nature of the information stored on a smart card, the security

and protection requirements for a smart card are greater than that of a magnetic strip card. The most widely used form of security mechanism on smart cards, as discussed earlier, is in the entering on a PIN to access the information on the card.

Though, even with this type of protection mechanism, smart cards are neither impervious nor infallible to various attack methods. The various attack methods that can be used, range for simple attacks, such as, replay and duplication/cloning attacks and offline dictionary attacks [13], to more complicated and sophisticated attacks which are represented under two categories: Invasive and Non-invasive attacks [14]. Invasive attacks are attacks that perform reverse engineering on the card, whereby the card is disassembled and picoprobes are attached to the various buses on the chip. This is done to determine the design of the chip, and to monitor the various signals processed by the card. The design of the chip can also be determined through a legal dispute, known as "litigation attacks", challenging the intelligent property right of the chip to obtain a more details design of the chip [15]. Non-invasive attacks, also called side channel attacks, have the added benefit of being performed relatively quickly and with no evidence of tamping to the card. Power Consumption Analysis using multi-bit attacks [14], Differential Power Analysis, Data Dependent Timing and Electromagnetic Analysis [15] can all be used to determine the structure of the chip by studying the electronic signature of the card to determine the design of the chip, and hence, determine possible security weaknesses. Once the design of the chip on the card is known, it is then possible to by-pass certain security features, such as restricted access to memory [15]. The countermeasures to these attacks are handled by their respective references.

Additional steps in securing the information on the cards, is by digitally signing the information into a tamper-resistant and trustworthy smart card [16].

III. A MODEL FOR OFF-LINE ATM TRANSACTIONS

The problem that was presented earlier, states that when the communication channel breaks down between an ATM and a bank, the ATM is not able to perform any transaction.

We propose a system that employs the use of smart card technology and demonstrate a model that allows ATMs to still process transactions, to a limited extent, when the communication channel to the bank is broken. In the rest of the paper a smart card will refer to an ATM card with an Integrated Circuit Chip (ICC) on it. The proposed model shows how the various security situations are handled. This is not the first time that smart cards have been proposed to be used in the ATM/banking environment. It has previously been concerned mainly with the prevention of fraud [17].

In the event of a communication breakdown, the smart card will contain the necessary information for a transaction to occur at an ATM. As shown in figure 2, the proposed model consists of three components involved in an ATM transaction: a smart card, the ATM and the bank computer. However, due to the communication breakdown, the bank computer is temporarily removed from the model.

Currently, for a withdrawal transaction to occur at an ATM, there are several pieces of critical information that are required by the ATM in order for this transaction to take place, such as: the account number, the verification of the PIN, the current balance within the account, the daily withdrawal limit on the account, and whether any money has been withdrawn already within the present day (withdrawal time stamp).

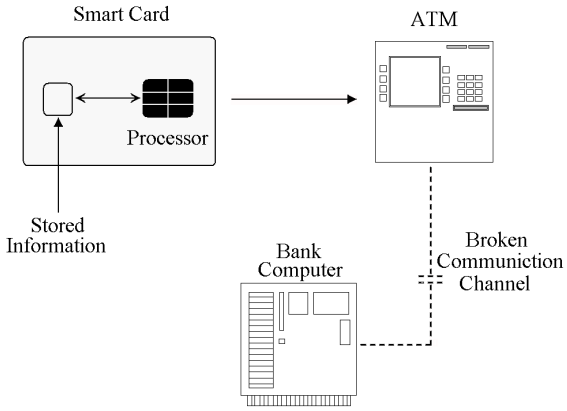

Fig. 2. An ATM transaction with a smart card

The critical information mentioned above, consisting of: the account number, verification of the PIN, the current account balance, the withdrawal limit and the withdrawal time stamp, are required in the proposed model, along with one new requirement, a transaction time stamp.

The first component of the proposed model, i.e. the smart card, is that all the critical information mentioned above be stored on the smart card itself. These critical pieces of information are discussed under the following headings.

A. Account Number

The account number of the client is stored under this heading.

B. Current Balance

The current balance of the account is stored on the card and updated (reduced) every time a withdrawal is made.

C. Withdrawal Limit

A withdrawal limit is a figure that represents the maximum amount of money that a client can withdraw from his bank account, as cash, within a set time limit.

D. Withdrawal Time Stamp

The withdrawal time stamp is a time stamp that is placed on the card so that the client cannot overdraw his daily limit. This is done as follows. The withdrawal time stamp is needed to verify whether or not a day has passed since the last transaction. If a day has past since that last transaction then the withdrawal limit is reset and a new time stamp recorded under the withdrawal time stamp variable. If a day has not passed then the current withdrawal limit and withdrawal time stamp are used. However, the issue of resetting the withdrawal limit according to the withdrawal time stamp depends largely on the bank's definition of a day. There could be two different definitions

- The first definition could be a 24-hour period from midnight to midnight the next day.
- The second definition could be a 24-hour period from an initial withdrawal.

Under the first definition, a 24-hour period from midnight to midnight, if the withdrawal time stamp stored on the card is from a previous day, then the withdrawal limit is reset and the current time is stored under the withdrawal time stamp variable. Whilst, if the second definition is used, a 24-hour period from an initial withdrawal, the withdrawal limit and new time stamp, recorded under the withdrawal time stamp variable, are recorded only if the current time is greater than one day's time increment from the current time stamp stored in the withdrawal time stamp variable on the card.

E. Transaction Time Stamp

This transaction time stamp refers to the last time the card was used to perform a successful transaction. The transaction time stamp and the withdrawal time stamp both store a time stamp value, but these time stamp values are for different purposes and are not to be confused with each other. The transaction time stamp is very important for maintaining synchronization, which is discussed later.

F. PIN

ATMs send the PIN encrypted back to the bank for verification when a communication channel exists. Therefore, the PIN needs to be stored on the card to perform a transaction with an ATM when a communication breakdown occurs. Thus the PIN should be stored on the card in some kind of an encrypted format.

One type of encryption format that can be used to actually store the PIN on the card is by utilizing an MD5 hash. MD5 is a one-way hashing algorithm that takes an arbitrary length message and produces a 16-byte message digest, also called a hash [18]. The hash value of the clients PIN is stored on the card. When the client is prompted to enter his PIN at the ATM, the PIN that he enters is hashed using the MD5 algorithm and this hash value is checked according to the hash value stored on the card. Verification is positive that the correct PIN has been entered, if the two hash values are the same. The MD5 hashing algorithm requires little processing power, ideally suited for a smart card, and can be reproduced at a hardware level [19]. However, large online databases exist containing the results of numerous MD5 hashes, reducing the secure ness of an MD5 hash [20].

A different technique that can be used to indirectly store the PIN on the card, is the verification step used in the Kerberos architecture [21]. In the Kerberos architecture, the information on the card, namely, the account number, the current balance, the withdrawal limit, withdrawal time stamp and the transaction time stamp are encrypted with the PIN. Therefore, verification that the correct PIN has been entered when prompted by the ATM is performed if the information on the card is correctly decrypted. This form of verification of the PIN is useful, as a PIN value is never directly stored on the card. The Kerberos architecture is computationally more expensive than an MD5 hash, due to the amount of information that needs to be encrypted and decrypted.

The second component of the proposed model, i.e. the ATM, requires two changes to the ATM itself. The first obvious change is that the ATM need to be able to interface with the smart card and be able to read the information stored on the card. The processor on the card will handle the updating of the information stored on the card. The second change that is required is a date storage element within the ATM itself; a non-volatile cache. This cache will store all the required details of the transaction during a communication failure. When the communication channel is restored, all the details of the transactions that occurred during the communication failure will be transmitted to the bank's computer in batch format, allowing the bank's computer to update their records and reflect these ATM transactions. At that stage, the bank records will be synchronized with the information stored on the card.

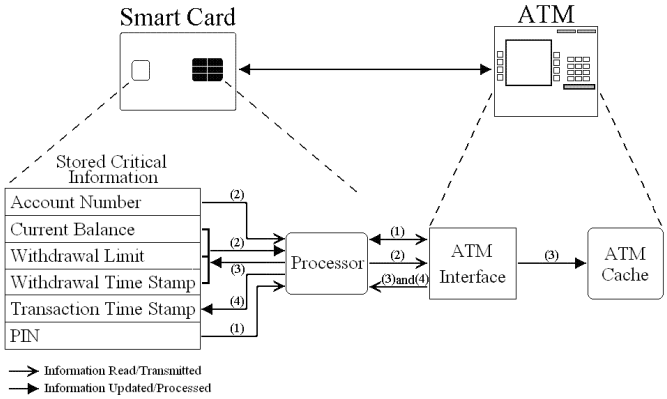

Fig. 3 Smart Card and ATM interaction process

Figure 3 demonstrates the interaction process that the smart card and ATM undergo during a communication breakdown. Step 1 of the interaction is the verification of the PIN. The PIN value stored on the card, if MD5 is used, is an MD5 hash of the PIN. If the Kerberos architecture is used, then the PIN value stored on the card is the encrypted format of the critical information. The PIN value is retrieved off the card, the processor then verifies the correctness of the entered PIN and informs the ATM of the result. If verification was successful, step 2 of the interaction, is that the card determines the amount of money the client is able to withdraw. This is determined using the current balance, withdraw limit and the withdraw time stamp. This information and the bank account number stored on the card are then sent to the ATM. If a withdrawal takes place, step 3 of the interaction, the ATM records the necessary information regarding the transaction into its cache. Then, the ATM responds to the smart card that the transaction was successful. The card in turn updates the current balance, the withdrawal limit and, if necessary, the withdrawal time stamp. In step 4 of the interaction, the smart card obtains a time stamp from the ATM, and updates the transaction time stamp with this value.

Due to the fact that the ATM transactions are stored in two places i.e. on the card and in the ATM's cache. This model shows remarkable robustness in that if two transactions occur at different ATMs, and should either or both ATMs have a communication failure, the second ATM will be able to recognise that an earlier transaction has taken place by the information residing on the card. In the event that the second ATM is off-line as well, then the information on the card contains accurate information about the client's current bank balance. In the event that the second ATM is online, whilst the first ATM is off-line, and therefore, has not updated the bank's records regarding the first

withdrawal. The second ATM will regard the information on the card as being accurate, due to the fact that the transaction time stamp stored on the card is newer than the one stored in the bank's records.

IV. Critical Evaluation of the Model

There are several issues that are raised by the proposed model. These issues discussed below are: information storage on the smart card, the synchronization process regarding the smart card, the ATM and the banks and how overall ATM networks load can be minimized using the proposed model.

A. Information Storage

The information on the card needs to be updated whenever a transaction occurs at an ATM. This updating process needs to occur whether or not a communication channel to the bank is present. This updating process is fundamental for the card to be in sync with the bank's records. Synchronization will be handled in more details under its own section below.

The updating of the information on the card is handled by the card itself. Hence, the functionality of the ATM remains unchanged, expect for the storage of transaction details in a cache, in the event of a communication breakdown. The card will collect the necessary information from the ATM to fulfil the updating of the information correctly. The necessary information from the ATM would include the following:

- Whether the withdrawal transaction was successful.
- How much money has been withdrawn.
- The current time.

The account balance value on the card will be reduced by the amount withdrawn. The withdrawal limit value will also be altered with this amount. The withdrawal time stamp on the card is compared to the current time retrieved from the ATM, and depending the client's bank's definition of a day, as discussed earlier, is updated accordingly. The transaction time stamp is updated with the current time. And finally if the Kerberos method is used for PIN verification, the PIN, which was stored earlier when it was entered so as to perform the decryption, is now used to encrypt the information. After which, the now encrypted information is stored on the card.

The updating of the information on the card is performed after all transactions are completed, and just prior to the ejection of the card. Memory clean-up is performed on any temporary variables used, such as the PIN storage value used in the Kerberos method, just prior to the ejection of the card.

B. Synchronization

Synchronization of the card and the bank's records are very important to maintain security and stability of the proposed method. The transaction time stamp stored on the card will be vital in the synchronization process. Synchronization of the card will occur every time the client visits their bank to perform any transaction or goes to an ATM that is online with the bank. The proposed model requires that the client present their smart card when performing any transaction at the bank. The account balance and transaction time stamp on the card and at the bank are compared to determine if synchronization needs to take place. If, any of these values are different, then synchronization needs to occur somewhere, either on the card or at the bank. This will be illustrated in a number of scenarios as follows.

1) Scenario 1

Suppose a client has a bank balance of R500. The client goes to an ATM that is currently off-line and performs a withdrawal of R200. This withdrawal information is stored in the ATM's cache and the information on the card is updated, the card now contains a balance of R300. Due to the ATM being off-line the bank's record have now become out of sync. If the same client goes to another ATM, which is online though, and wishes to perform another withdrawal, of R200, which account balance should be used? The one on the card or the one from the banks records? This is solved by the fact that the transaction time stamp on the card has a newer time stamp than the last transaction time stamp stored in the bank records, hence, the card's values will be used. After the second transaction, when the bank's records are updated, they will only reflect the withdrawal performed at the online (second) ATM. When the off-line (first) ATM eventually comes back online, it will update the bank's records with the transactions that it performed whilst off-line. After this occurs, the bank's records will be synchronized again.

2) Scenario 2

Suppose a client has a bank balance of R500 and that the bank charges some kind of service fees on the account, amounting to R20. The information on the card will now be out of sync. Though, as soon as the card is used in an ATM that is online, the information from the bank's records will be used, as it contains the newer time stamp, and the new information is then stored on the card once the transaction is completed.

Assume however, now that the client goes to an ATM that is off-line before the service fee of R20 is updated on the card, hence, the card still has a balance of R500. If banks wish to protect themselves from client overdrawing their bank account, they could limit the amount of money that the client can withdraw from an ATM which is currently off-line. Therefore, even though the client has R500 is his bank account, as stored on the card, he will only have a withdraw able balance of R400, as the ATM is currently off-line and cannot verify the balances.

3) Scenario 3

Suppose a client has a bank balance of R500. The client performs a deposit of R200 at an ATM. No information on the card or at the bank is updated, until the deposit is confirmed by an operator, as is the current standard procedure with ATM deposits. Once an operator confirms the validity of the deposit, the bank's records are updated to reflect the deposit of R200 and show a balance of R700. The card is synchronized the next time the client visits the bank or an ATM that is online.

As shown in the above examples, the card will never try to update the bank's records with its information. The card will always synchronize its information with that of the bank records, as long as the bank records contain a newer transaction time stamp than the card.

The whole synchronization process needs to be handled very carefully so that complications do not arise.

C. Minimizing ATM Network Load

ATM networks form large clustered node networks, with the ATMs representing the nodes. These nodes have the ability to start communicating with a central node (the host computer) at any point in time. ATM networks, therefore, may require a large amount of bandwidth, especially as more and more ATMs joins the ATM networks.

The proposed model can be extended to ATM cluster networks in the way that the nodes communicate, by allowing the nodes very specific time periods in which to communicate. In other words, our model could be applied in such an ATM network where ATMs may be off-line most of the time and only connects periodically to the bank's network, at which time, transactions will be communicated to the bank in batch form. This technique, therefore, would reduce the bandwidth required by these networks. This will be handled in future work in conjunction with synchronization.

V. Conclusion

The core of the problem that was presented was how could an ATM perform transactions whilst a communication failure with the bank had occurred? This paper proposed a model that shows how this problem can be over come, by employing smart cards. In addition, the paper showed that relatively few variables are required to necessitate a transaction at an ATM whilst its communication is off-line. The model proposed two new methods, the first is the storage of the PIN directly or indirectly on the smart card. The second method being synchronization through the use of transaction time stamps.

The model showed that the synchronization of the information stored on the card and in the bank's records, can be effective with the use of time. Though the exact details of the implementation of transaction time stamps in the synchronization process will be handled in future work.

VI. Acknowledgement

This material is based upon work supported by the National Research Foundation under grant number 2054024. Any opinion, findings and conclusions or recommendations expressed in this material are those of the authors and therefore the NRF does not accept any liability thereto.

VII. Reference

[1] How Stuff works, May 6 2005, http://money.howstuffworks.com/atm.htm.

[2] Korean banking sector backs biometrics in ATMs, January 2003, Biometric Technology Today, 11(1):12.

[3] German saving banks reject biometrics at ATMs, April 2002, Biometric Technology Today, 10(4):6-7.

[4] R. Colonia-Willner, March 2004, Self-service systems: new methodology reveals customer real-time actions during merger, Computers in Human Behaviour 20(2):243-267.

[5] M. Aron, P. Druschel, W. Zwaenepoel, 2000, Cluster reserves: a mechanism for resource management in cluster-based network servers, SIGMETRICS '00: Proceedings of the 2000 ACM SIGMETRICS International Conference on Measurement and Modelling of Computer Systems, ACM Press, 90-101.

[6] L. Fild, 1998, Paying through the nose for your own cash, Sunday Time: Business Times, Available: http://www.btimes.co.za/98/0125/btmoney/money2.htm

[7] B. A. Forouzan Data Communication and Networking: 2nd edition, McGraw Hill, pg 216-218.

[8] A. Abrail, J. Bouvier, M. Renaudinv, P. Senn, P.vivet, July 2001, A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller, IEEE Journal of Solid-state Circuits, 36(7):1101-1107.

[9] Out of Africa, October 2004, Card Technology Today, 16(10):9.

[10] New smart ID for South Africans, October 2004, Biometric Technology Today, 12(9):5.

[11] H. Huang, C. Chang, 2004, A new design of efficient partially blind signature scheme, The Journal of Systems and Software 73:397-403.

[12] Sofia Gleni, Panagiotis Petratos, 2004, DNA Smart Card for Financial Transactions, http://info.acm.org/crossroads/xrds11-1/dnasmartcard.html.

[13] Chun-I Fan, Yung-Cheng Chan and Zhi-Kai Zhang, May 2005, Robust remote authentication scheme with smart cards, Computers & Security.

[14] Thomas S. Messerges Ezzat A. Dabbish, Robert H. Sloan, 2002, Examining Smart-Card Security under the Threat of Power Analysis Attacks, IEEE Transactions on Computers 51(5);541-552.

[15] Simone Moore, Ross Anderson, Paul Cunningham, Robert Mullins, George Taylor, 2002, Improving Smart Card Security using Self-timed Circuits, Computer Laboratory, University of Cambridge.

[16] Roger Kilian-Kehr, Joachim Posegga, 2002, Smart Cards in Interaction: Towards Trustworthy Digital Signatures, Cardis, pg 11-18.

[17] Nigel Walsh, February 2005, ATM fraud prompts card rethink, Card Technology Today, 17(2):10.

[18] T. Hsieh, Y. Yeh, C. Lin and S. Tuan, September 1999, One-way hash functions with changeable parameters, Information Sciences 118(1-4): 223-239.

[19] B. Robatmili, N. Yazdani and M. Nourani, February 2005, Optimizing SMT processors for IP-packet processing, Microprocessors and Microsystems.

[20] H. Dobbertin, 1996, The status of MD5 after a recent attack, CyptoBytes 2(2). Available: http://www.rsasecurity.com/rsalabs/node.asp?id=2149.

[21] E. English, June 1995, Use of Kerberos authentication, Computer Fraud & Security Bulletin, 6:16-18.

VIII. Bibliography

Alexander M. Rossudowski, obtain his B.Sc. Information Technology (IT) from the Rand Afrikaans University in 2003, a B.S. (Hons.) Computer Science from the Rand Afrikaans University in 2004. He is currently studying his M.Sc. in Computer Security at the University of Pretoria in the ISCA research group.