Modeling Discretional Access Control in Automatic Teller Machine Using Denotational Mathematics

Rufai M. M., Adigun J. O. and Yekini N. A.
Department of Computer Technology, Yaba College of Technology

ABSTRACT
In recent time different access control methods have been proposed to secure customers account from unauthorized access. To mention but a few are Signature Authentication, PIN identity, Biometric Access control etc. Experience has shown that a singular access control techniques is not sufficient to address access control problems. Each technique, as sophisticated as they are, has flaws or weaknesses.
This paper presents the combination of Personal Identification Number (PIN) and the use of mobile phone in preventing unauthorized access to users account in an Automatic Teller Machine. A user with doubtful or suspicious access attempt is expected to additionally pass the Mobile Phone authorization test. With the mobile authorization test the security of an account is put in the hands of its owners. A review of the various security threats and abuses is done. The Discretional Access Control Techniques is explained. A model describing the combination of PIN and Mobile Phone Authorization as a discretional Access Control technique is designed using denotational mathematics.

Keywords
ATM, Access Control, Discretional Access Control, Denotational Mathematics

1. Introduction

The ATM was invented to solve the problem of long queue in banks and to improve the quality of banking services to customers. With the ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances as well as purchasing Mobile Cell Phone Prepaid credit.
Being a machine, it is important that it authenticates the user each time he applies for access to ATM services. This is usually done by the insertion of an ATM card which contains a unique card number and security information such as an expiration date. A user applies for identification by supplying the PIN number which is unique to every user. The ATM searches for the record of the user in its database and confirms or denies the existence of the record. Where the record exists, further request for service will be entertained and where the record does not exist, the user is out rightly turned down.
In this study, our contention here is the sole use of ATM card in identifying the user. Anybody can be in possession of the card and the person may have knowledge of the user's PIN number. This makes this approach vulnerable to ATM fraud. Additionally, experience reveals that the card is characterized by some inherent shortcomings.
The objective of this paper is to see to how to protect the integrity of a user's transaction using the PIN in conjunction with the use of Mobile Phone Authorisation Test. The recent spate of ATM fraud calls for an effective access control techniques that will ensure the genuine owner of an account has access to it. In the last four years of Nigeria usage of ATM, there have been complaints of penetrating of user identity codes. For example, the NDIC report published in the Punch Newspaper of 17th of October, 2011 reported that 21.29bn billion has been lost to fraud through forgeries and ATM. The challenge is how can we find solution to this problem?

2. The ATM System Architecture

The diagram below shows the architecture of the ATM system. It consist of an ATM processor, a system clock, a remote account database, and a set of peripheral devices such as the card reader, monitor, keypad, bills storage, and bills disburser.

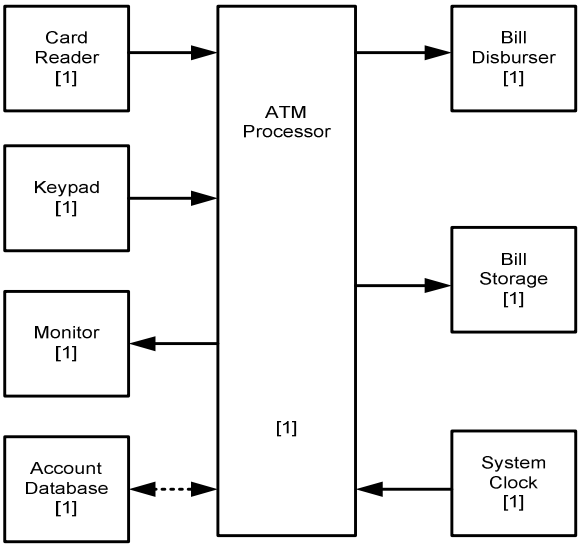

Figure 1: Conceptual Model of ATM

Manuscript received November 5, 2011
Manuscript revised November 20, 2011

2.1 The ATM System Modus Operandi

A typical ATM is online with the bank, that is, each transaction will be authorized by the bank on-demand and directly debited from the account's owner.

The ATM works as follows.

Firstly, the client will insert his/her client card in the ATM and then the ATM will ask for a Personal Identification Number (PIN). The number is checked against a previously stored PIN of the user, once the correctness of the PIN is confirmed, the ATM will request the client to indicate its choice of service (e.g. Withdrawal, Balance Enquiry etc.). If the choice is withdrawal, the client is asked to supply the amount of money to be withdrawn. If the amount is available and if the client has enough money on his credit then the said amount of money will be released. Whether the amount of money is payable or not, i.e. the ATM has enough cash but could be the case the ATM has no change for that amount, will also be checked.
Once the money is offered to the client a countdown is started, i.e. the client has a determined amount of time to pick up the money. If this timeout is over, the money will be collected by the ATM and the transaction will be rolled back.

2.2 Security Threats and Abuses in ATM

Threats can be seen as potential violations of security with expected or unexpected harmful results, and exist because of vulnerability in a system. If an unauthorized user invades into a system he/she can destroy information, operating systems, and programs. They can disclose information or they can cause disruptions or interruptions (damage systems, networks, organizations, institutions).
Sources of threats can be classified as follows:

- Physical, which include natural disasters (fire, storm, water damage) and environmental conditions (dust, moister, humidity).
- Technical: This is synonymous to equipment or software failure e.g. A user apply for withdrawal in an ATM machine, the machine shows paid but the cash is not delivered.
- Human, which is the main source of communication breaches. It includes unauthorized users who wish to damage an ATM system, and authorized users who misuse the system either deliberately or accidentally. The human threats can be further categorized into internal and external: Internal human threats are disgruntled employees, hackers, former employees, system administrators, LAN and data base administrators. External human threats arise from commercial espionage, government-sanctioned espionage, vendors, manufacturers, kids looking for kicks, nosy reporters.
- Theoretical, which includes the vulnerability of the algorithms, protocols, and mathematical tools used in the methods that they are implemented in the systems.

2.3 Security Facilities in The Present ATM System

The designer of the present ATM has put in place a lot of security facilities. As good as these facilities are, it has not been able to totally solve the issue of ATM fraud. However, it is necessary we have a review of these existing security facilities. These facilities fall under different headings as follows:

Physical Security
The essence of this approach is to prevent physical attack on the ATM machine. This is achieved in two ways
1. Using dispenser mechanism that makes it difficult to retrieve money without proper authority.
2. Another approach is the use of dye markers and smoke canisters which prevent the use of the money in the machine by a thief

1.1.1
Transactional secrecy and integrity
Fraud is prevented by ensuring that personal information is encrypted. Sensitive data in ATM transactions are usually encrypted with Data Encryption Standard(DES), but transaction processors now usually require the use of Triple DES.

Customer identity integrity
There have also been a number of incidents of fraud where criminals have attached fake keypads or card readers to existing machines. These have then been used to record customers' PINs and bank card information in order to gain unauthorized access to their accounts. Various ATM manufacturers have put in place countermeasures to protect the equipment they manufacture from these threats.

1.1.2
Device operation integrity
ATMs that are exposed to the outside must be vandal and weather resistant.
Openings on the customer-side of ATMs are often covered by mechanical shutters to prevent tampering with the mechanisms when they are not in use. Alarm sensors are placed inside the ATM and in ATM servicing areas to alert their operators when doors have been opened by unauthorized personnel.

Customer security
In some areas, multiple security cameras and security guards are a common feature.

3 ATM Card Frauds

ATM card fraud has been on the loose in recent time. Fraudsters use various methods in perpetrating this crime. They exploit the weakness in the existing ATM system to their advantage. An insight into how these fraud are done will lead us to solution to these problems. Some of the methods used by fraudster are described below:
The easiest of all these method is to simply steal a customer's card. A later variant of this approach is to trap the card inside of the ATM's card reader with a device often referred to as a Lebanese loop. When the customer gets frustrated by not getting the card back and walks away from the machine, the criminal is able to remove the card and withdraw cash from the customer's account.
Other cases are using the internet to cajole user to have access to their ids and pin number by sending a phishing mail to the card owner and requesting him to supply identity information.
Another simple form of fraud involves attempting to get the customer's bank to issue a new card and stealing it from their mail. The concept and various methods of copying the contents of an ATM card's magnetic stripe on to a duplicate card to access other people's financial information was well known in the hacking communities by late 1990.
A sophisticated method of card fraud involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera to observe the user's PIN. Card data is then cloned onto a second card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity wireless cameras and card readers has made it a relatively simple form of fraud, with comparatively low risk to the fraudsters.
From the aforementioned, one can observe all card fraud techniques has the user ATM card as target because it is seen as the user's sole identity. The need for a user to have multiple identities becomes incumbent which is the focus of this paper.

4. Discretionary Access Control

Access control refers to exerting control over who can interact with a resource. Discretionary access control (DAC) is an access control policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have. There are two important concepts relevant to Discretionary Access Control. These are:

File and data ownership: Every object in the system has an owner. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.
The application of the Discretionary Access Control Policy to ATM can be summarized as: Every Access to a user account either through ATM or any other method(e.g. bank counter) must get the approval of the account owner wherever he may be.
The procedure is as follows:

- Users insert ATM
- The user supplies PIN, seeking access
- PIN is verified
- If verification fails the user has the right to retry 2 more times.
- If at the third time PIN is confirmed wrong then transaction is cancelled, Card ejected and ATM is returned to welcome state.
- If PIN is correct then, the user selects withdrawal transaction.
- An authorization request is sent to the account owner's phone for transaction approval
- If approval is denied then the card is ejected and the ATM is returned to welcome state
- If approval is given, withdrawal amount is requested
- The machine verifies if amount requested is less than available account balance
- It also verifies if there is sufficient bills in the ATM
- Disburse bills, eject card and return to welcome state.

5. A Discretional Access Control Model for ATM Using Denotational Mathematics

The composition of an ATM using mobile phone as additional access control can be formally described using Denotational Mathematics such as Real Time Process Algebra(RTPA). According to RTPA methodology for system modelling and refinement, a software system can be specified as a set of architectural and operational components as well as their interactions. The architectural component is modeled by Unified Data Models (UDMs, also known as the component logical model (CLM)) (Wang, 2008b), which is an abstract model of system hardware interfaces, an internal logic model of hardware, and/or an internal control structure of the system. The operational component is modelled by static and dynamic processes using the Unified Process Models (UPMs) (Wang, 2007,2008b;). In this paper our focus is to model architectural component of an ATM with discretional access control.

The formal model of the Discretional Access Controlled ATM as a Finite State Machine DATMST is defined as a Five tupple relationship

$$DATMST \mid\mid (S, \Sigma, s, F, \delta) \qquad (1)$$

Where

- S is a set of valid states that forms the domain of the ATM, S = {s0, s1, …, s8} where the states are:

s0 –System,
s1 – Welcome,
s2 - Check PIN,
s3 – Input withdraw amount,
s4 – Seek Approval,
s5 - Verify balance,
s6 - Verify bills availability,
s7 - Disburse bills, and
s8 - Eject card, respectively;

Σ is a set of events that the ATM may accept and process, Σ = {e0, e1, …, e12} where:
e0 - Start,
e1- Insert card,
e2 - Correct PIN,
e3 - Incorrect PIN,
e4 – Request ≤ max,
e5 – Request > max,
e6 - Cancel transaction,
e7 -Sufficient funds,
e8 - Insufficient funds,
e9 - Sufficient bills in ATM,
e10 - Insufficient bills in ATM,
e11 – Approval granted,
e12 – Approval denied;

- s is the start state of the ATM, s = s1 (Welcome);
- F is a set of ending states, F = {s1};
- δ is the transition function of the ATM that determines the next state of the FSM, si+1, on the basis of the current state si and a specific incoming event ei, i.e., si+1 = δ (si, ei), where δ = f: S × Σ → S (2).

The transition table showing the transition from one state to the next state upon an even is shown below

S_i	e_i	$Si+1=\delta(s_i,e_i)$
s_0	e0	s1
s_1	e1	s2
s_2	e2	s3
s2	e3	s2
s2	e6	s7
s3	e4	s4
s3	e5	s3
s3	e6	s7
s4	e7	s5
s4	e8	s7
s5	e9	s6
s5	e10	s7
s6		s7
s7		s1

The transition diagram derived from Table 1 is shown in Fig. 2 and Fig. 3..

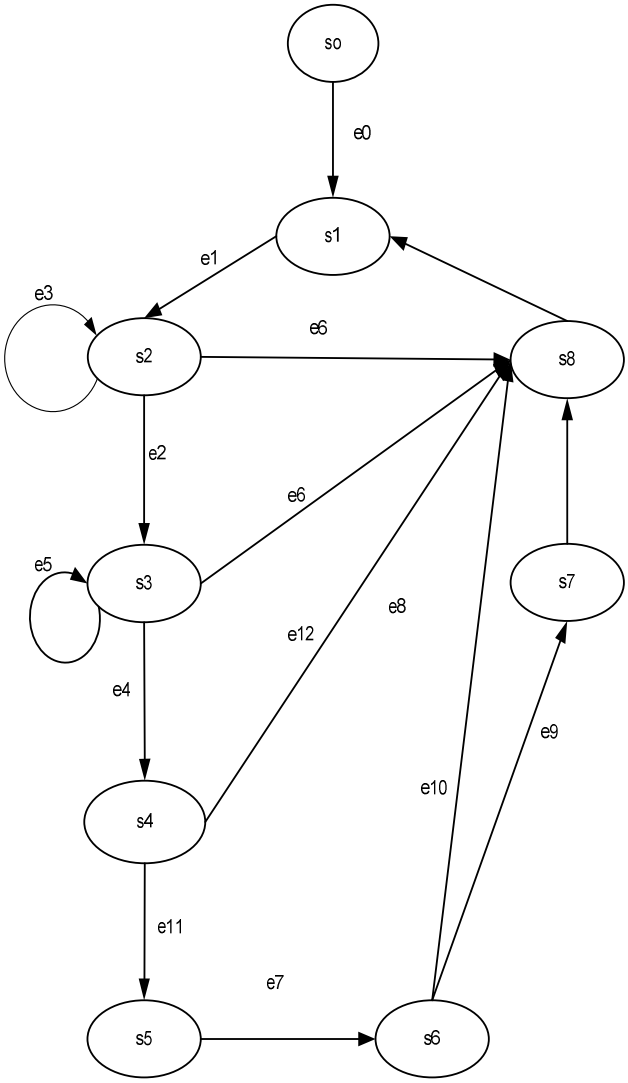

Figure 2: The Abstract Transition Model of The ATM Behaviors

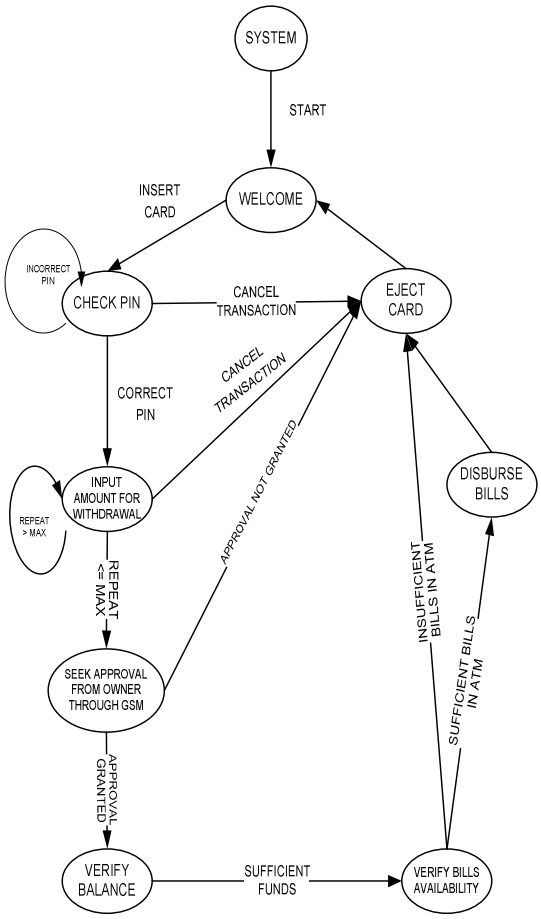

Figure 3: The Transition Model of the ATM Behaviours

5.1 The Architectural Framework of The Modelled Discretional Access Control ATM System(DAC_ATM)

The top level framework of the DAC_ATM system can be modeled by a set of architecture, static behaviors, and dynamic behaviors using RTPA (Wang, 2002, 2008a) as follows:

§(DAC_ATM) ≙ DAC_ATM§.ArchitectureST
|| DAC_ATM§.StaticBehaviorsPC
|| DAC_ATM§.DynamicBeh aviorsPC

Fig 4: The Top Level Model of DAC_ATM

where || indicates that these three subsystems related in parallel, and §, ST, and PC are type suffixes of system, system structure, and process, respectively.

The Architectural framework is derived from the conceptual model and the behavioural model as shown in Figs. 1 to 3. The high-level specification of the architecture of DAC_ATM i.e. DAC_ATM§.ArchitectureST, is described using the RTPA format in Fig. 4. DAC_ATM§.ArchitectureST encompasses parallel structures of a set of UDMs such as the ATMProcessorST, CardReaderST, KeypadST, MonitorST, BillStorageST, BillsDisburserST, AccountDatabaseST, and SysClockST, as well as a set of system events @EventsS and a set of statuses ⓈStatusBL. The numbers in the angel brackets indicate the configuration of how many data objects that share the same UDM.

DAC_ATM§.ArchitectureST <ATMProcessor : ST | [1]>|| <CardReader : ST | [1]>|| <Keypad : ST | [1]>
|| <Monitor : ST | [1]>
|| <BillStorage : ST | [1]>
|| <BillsDisburser : ST | [1]>
|| <SysClock : ST | [1]
|| <SysDatabase : ST | [1]>
|| <@EventsS>
|| <StatusBL>

Fig. 4: Architectural Framework of the DAC_ATM Model

The set of events of DAC_ATM are predefined global control variables of the system, as given in Fig. 4, which represent an external stimulus to a system or the occurring of an internal change of status such as an action of users, an updating of the environment, and a change of the value of a control variable. Types of general events, @EventS, that may trigger a behavior in a system can be classified into operational (@eS), time (@tTM), and interrupt (@int ⊙) events where @ is the event prefix, and S, TM, and ⊙ the type suffixes of string, time, and interrupt, respectively, i.e.:

DAC_ATM§.ArchitectureST.EventsST≙
@SysInitialS| @tTM = §thh:mm:ss
| @SysClock100msInt⊙

Fig. 5: Events UDM

In RTPA, a status denoted by ⓈsBL is an abstract model of system state in Boolean type with a status prefix Ⓢ, such as an operation result and an internal condition. The DAC_ATM statuses as a set of predefined global control variables are as follows:

DAC_ATM§.Archite ctureST.StatusST ≙ ⓢ
CardReadStatusBL
| ⓢMonitorStatusBL
| ⓢKeypadStatusBL
| ⓢBillStorageStatusBL
| ⓢBillsDisburserStatusBL
| ⓢBillsDisburseEngineStatusBL
| ⓢBillsAvailableBL
| ⓢBillsDisbursedBL
| ⓢCardInsertedBL
| ⓢCardEjecte dBL
|ⓢCancellKeyPr essedBL
| ⓢEnterKeyPressedBL
| ⓢDataEnteredBL
| ⓢTimeOutBL
| ⓢServiceCompletedBL
| ⓢServiceCancelledBL
| ⓢSystemFailureBL
| ⓢSysShutDownBL
| ⓢValidAmountBL
| ⓢValidBalanceBL
| ⓢValidCardBL
| ⓢValidPINBL
| ⓢApprovalGrantedBL

Fig. 6: Status UDM

5.2 MERITS OF THE MODEL

Multiple Access Control: The model proposes the control access from multiple access. The first source is the use of the card by supplying the correct PIN while the second source is the request for authority from the user through its phone number, when the use of the card is suspected. These two sources must authorize the transaction before it can be processed.

Withdrawal Alert System: This proposal has created a withdrawal alert system that keeps the account holder inform each time the integrity of his account is violated. He approves or denies this violation
It is another way of keeping log of transaction of the customer account. For example the date and time the account is accessed is preserved in the text message on the user's mobile phone.
It reduces ATM fraud to the barest minimum if not completely because each access to the account get the consent of the owner wherever he may be.

6. CONCLUSION

In this paper we presented a conceptual framework for the use of Mobile Phone as additional access control mechanism in Automatic Teller Machine (ATM) and a model using denotational mathematics. The model is designed in a way that will facilitate physical design showing the DAC_ATM Architectural structure.
The proliferation of ATM fraud justifies the need for an effective access control mechanism that will guarantee the protection of users transaction. This approach introduces multiple access control thereby making it difficult for fraudsters. The fact that a user is synonymous to his mobile phone i.e. he can be reached at anytime shows the potency of the approach. Future work may see to the implementation of the proposed concept in an Automatic Teller Machine.
Apart from the fact that it takes us to another level in ATM access control interface, it is economical and easy to use, it should be adopted by financial institutions.

References

[1] "ATM Fraud And Security White Paper"PDF (126 KiB) a Diebold report via Credit Union National Association
[2] "Text of the ATM Safety Act" State of New York Banking Department
[3] Commission of the European Communities (1993) "Glossary of Information Systems Security "Contract 52001, Definitions within information systems security,.
[4] Furnell, S.M., Morrissey, J.P., Sanders, P.W., Stockel C.T. (1996). "Applications of keystroke analysis for improved login security and continues user authentication" Proceedings of Information Systems Security (edited by S. Katsikas, D. Gritzalis), pp.283--294.
[5] Hamilton D.J., Whelan, J, McLaren, A. ,MacIntyre, I., Tizzard A (1995). " Low cost dynamic signature verification system" IEE Conference Publication n 408, England , p. 202-206.
[6] Simonds, F (1996) "Network Security, Data and Voice Communications" McGraw-Hill, N.Y.
[7] The Punch Newspaper, October 17, 2011
[8] Wang, Y. (2007a). Formal description of the cognitive process of memorization. In Proceedings of the Sixth International Conference on Cognitive Informatics (ICCI'07) (pp. 284-293). Lake Tahoe, CA: IEEE CS Press.
[9] Wang, Y. (2008a). Deductive semantics of RTPA. The International Journal of Cognitive Informatics and Natural Intelligence, 2(2), 95-121.
[10] Wood, H.M. "The use of passwords for controlled access to computer resources" National Bureau of Standards Special Publication 500-9, US Dept. of Commerce/NBS

Rufai Mohammed Mutiu obtained his B.Sc degree from Ogun State University (Presently Olabisi Onabanjo University), Ago Iwoye, Ogun State, Nigeria. He got his Masters in Computer Science from University of Lagos, Akoka, Lagos, Nigeria. He is a member of Nigeria Computer Society and presently lectures at Yaba College of Technology, Lagos, Nigeria. His research area is Information Systems Design and Modelling.

Adigun Johnson Oyeranmi is a specialists in computer software, security and knowledge management. He obtained his first degree (B.Sc Computer Science) from University of Ibadan, Oyo State, Nigeria and his Masters(M.Sc. Computer Science) from University of Lagos. He is a member of Nigeria Computer Society of Nigeria and Computer Professionals Council of Nigeria. He is the current Dean of The School of Technology, Yaba College of Technology, Yaba, Lagos.

Yekini Nureni Asafe majors in Data Communication and Networking. He obtained his B.Sc. degree in computer engineering from Lagos State University and Master Degree in Computer Science from University of Lagos, Nigeria. He is a member of Nigeria Society of Engineers. He currently lectures Data Communication and Networking in Yaba College of Technology, Lagos, Nigeria.