SURVEY OF ATM PASSCODE BREAKING TECHNIQUE

ABUBAKAR MUHAMMAD
Department of Computer Science,
The Federal Polytechnic, Bauchi (Nigeria)
faqeer4sure@gmail.com

ZAINAB ALIYU MUSA
Department of Computer Science,
The Federal Polytechnic, Bauchi (Nigeria)
zynerb@gmail.com

ADONU SUNDAY EJIYIME
Department of Computer Science,
The Federal Polytechnic, Bauchi (Nigeria)
ejiyime@gmail.com

Abstract

Four digit Passcodes are used in all ATMs nationwide as access security to bank accounts for performing many transactions. Many ATM users are of the belief that these passcodes are enough access security to secure their accounts, however banks do know that passcodes are not secured and can be infiltrated by humans and machines and therefore attempts to make it secured by fixing three supply of wrong passcodes result in blocking the ATM card. This research intends to analyze whether passcodes are enough as access security to ATM users or not. The research will study the anatomy of different spywares that are capable of breaking these passcodes and get access to ATM transaction of users without the users ever knowing that. To round up this research, a spyware will be designed using Visual Pascal that will be used to demonstrate how it will infiltrate and break ATM passcodes in order to demonstrate the inefficiency of passcodes as access security to ATM transactions. The research at the end of the spyware test, recommends different access security that should be used on ATM transactions that is more reliable and proof to spyware infiltrations.

Keywords: *ATM, password, passcode, passphrase, hacking, spyware, malware.*

1. INTRODUCTION

Access control in general refers to a condition, or conditions (more than one) that must exist that specifically determines a criteria, or a set of criteria's that has to be met, before access / entrance will be granted, thus restricting free access, by enlisting a criteria. This criteria could be simple or very complicated, physical, electronic or biometric (the recording of things such as people's fingerprints or the appearance of their eye in order to identify them on an electronic system).By implication, anything from a key, to a credit card pin, to a finger print.

1.1 Access security

The aim of access security is to create a perception of sanctuary and a presence of safety, and to enforce the access criteria Access security is the selective restriction of access to a place or other resource. The aim of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier, where granting access can be electronically controlled. Typically, the access point is a door. An electronic access control door can contain several elements. At its most basic, there is a stand-alone electric lock. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision, but send a card number to an access control panel that verifies the number against an access list. To monitor the door position a magnetic door switch can be used. In concept, the door switch is not unlike those on refrigerators or car doors. Generally only entry is controlled, and exit is uncontrolled.

In cases where exit is also controlled, a second reader is used on the opposite side of the door. In cases where exit is not controlled, free exit, a device called a request-to-exit (REX) is used. Request-to-exit devices can be a push-button or a motion detector. When the button is pushed, or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.[citation needed]

1.2 Password

The Secure Shell protocol contains numerous features to avoid some of the vulnerabilities with password authentication. Passwords are sent as encrypted over the network, thus making it impossible to obtain the password by capturing network traffic. Also, passwords are never stored on the client. Empty passwords are not permitted by default (and they are strongly discouraged).

On the server side, the Secure Shell protocol relies on the operating system to provide confidentiality of the user passwords. SSH Tectia Server also supports limiting the number of password retries, thereby making brute-force and dictionary attacks difficult.

However, Secure Shell does not protect against weak passwords. If a malicious user is able to guess or obtain the password of a legitimate user, the malicious user can authenticate and pose as the legitimate user. Weak passwords can also be discovered by dictionary attacks from a remote machine.

Password authentication can also be used as a generic authentication method. This is the case with SSH Tectia Connector when all users use the same credentials. In this case only data encryption and data integrity services are provided. The responsibility for user authentication is left to the tunneled third-party application.

The following lists sum up the advantages and disadvantages of using password authentication with SSH Tectia.

Advantages

- Simple to use
- Simple to deploy—since the operating system provides the user accounts and password, almost no extra configuration is needed.
- Generic password use with SSH Tectia Connector

Disadvantages

- Security is entirely based on confidentiality and the strength of the password.
- Does not provide strong identity check (only based on password).

1.3 Passcode

A passcode is a password used to grant access. On the iPad, the passcode defaults to a simple 4-digit password similar to the passcode for an ATM bank card. However, the iPad allows for alphanumeric passwords by turning off the simple passcode and locking the iPad.

Also, a passcode identifies a person to gain access to places or things. It is often chosen by the individual and is secret. A pass code is also known as a password or a PIN (personal identification number). It can be made up of letters or numbers and is sometimes a combination of both. Because it is secret, it should not be something others can easily guess. Your pass code protects you from someone else gaining access to your things or places.

1.4 PassPhrase

A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security. Passphrases are often used to control both access to, and operation of, cryptographic programs and systems.

Passphrases differ from passwords. A password is usually short—six to ten characters. Such passwords may be adequate for various applications (if frequently changed, if chosen using an appropriate policy, if not found in dictionaries, if sufficiently random, and/or if the system prevents online guessing, etc.) such as:

Logging onto computer systems

Negotiating keys in an interactive setting (e.g. using password-authenticated key agreement)

Enabling a smart-card or PIN for an ATM card (e.g. where the password data (hopefully) cannot be extracted)

But passwords are typically not safe to use as keys for standalone security systems (e.g., encryption systems) that expose data to enable offline password guessing by an attacker.[citation needed] Passphrases are theoretically stronger, and so should make a better choice in these cases. First, they usually are (and always should be) much longer—20 to 30 characters or more is typical—making some kinds of brute force attacks entirely impractical. Second, if well chosen, they will not be found in any phrase or quote dictionary, so such dictionary attacks will be almost impossible. Third, they can be structured to be more easily memorable than passwords without being written down, reducing the risk of hardcopy theft.[citation needed] However, if a passphrase is not protected appropriately by the authenticator and the clear-text passphrase is revealed its use is no better than other passwords. For this reason it is recommended that passphrases not be reused across different or unique sites and services.

In 2012, two Cambridge University researchers analyzed passphrases from the Amazon PayPhrase system and found that a significant percentage are easy to guess due to common cultural references such as movie names and sports teams, losing much of the potential of using long passwords.

When used in cryptography, commonly the password protects a long (machine generated) key, and the key protects the data. The key is so long a brute force attack (directly on the data) is impossible. A key derivation function is used, involving many thousands of iterations (salted & hashed), to slow down password cracking attacks.

1.5 Strength of access security

Password strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.

Using strong passwords lowers overall risk of a security breach, but strong passwords do not replace the need for other effective security controls. The effectiveness of a password of a given strength is strongly determined by the design and implementation of the factors (knowledge, ownership, inherence). The first factor is the main focus in this article.

The rate at which an attacker can submit guessed passwords to the system is a key factor in determining system security. Some systems impose a time-out of several seconds after a small number (e.g. three) of failed password entry attempts. In the absence of other vulnerabilities, such systems can be effectively secured with relatively simple passwords. However the system must store information about the user passwords in some form and if that information is stolen, say by breaching system security, the user passwords can be at risk.

1.6 Spyware

Spyware is software that's installed without your informed consent, whether it be a traditional computer, an application in your web-browser, or a mobile application residing on your device. In short, spyware communicates personal, confidential information about you to an attacker. The information might be reports about your online browsing habits or purchases, but it can also be modified to record things like keystrokes on the keyboard, credit card information, passwords, or login credentials.

This software normally gets onto a computer by attaching itself to some other program that the user intentionally downloads and installs. Sometimes this is done completely discreetly, but other times the desired software will include information in the license agreement describing the spyware — without using that term — and forcing the user to agree to install it in order to install the desired program. Alternatively, spyware can get into a computer through all the avenues that other malware takes, such as when the user visits a compromised website or opens a malicious attachment in an email

Spyware can cause you two main problems. First, and perhaps most importantly, it can steal personal information that can be used for identity theft. If the malicious software has access to every piece of information on your computer, including browsing history, email accounts, saved passwords used for online banking and shopping in addition to social networks, it can harvest more than enough information to create a profile imitating your identity. In addition, if you've visited online banking sites, spyware can siphon your bank account information or credit card accounts and sell it to third-parties or use them directly.

The second, and more common, problem is the damage spyware can do to your computer. Spyware can take up an enormous amount of your computer's resources, making it run slowly, lag in between applications or while online, frequent system crashes or freezes and even overheat your computer causing permanent damage. It can also manipulate search engine results and deliver unwanted websites in your browser, which can lead to potentially harmful websites or fraudulent ones. It can also cause your home page to change and can even alter some of your computer's settings.

Spyware is something of a grey area, as there's really no copy-book definition of it. As its name suggests, however, spyware is generally loosely defined as software that's designed to gather data from a computer or other device and forward it to a third party without the consent or knowledge of the user. This often includes collecting confidential data such as passwords, PINs and credit card numbers, monitoring keyword strokes, tracking browsing habits and harvesting email addresses.

In addition to all of this, such activities also affect network performance, slowing down the system and affecting the whole business process. It is generally classified into four main categories: Trojans, adware, tracking cookies and system monitors.

- Trojan spyware that infects computers in the form of Trojan malware.
- Adware that also serves as spyware to monitor computers and devices.
- Tracking cookie files on hard drives that track a user on the Internet if a site is aware of the tracking cookies and designed to use them.
- System monitors designed to monitor any activity on a computer and capture sensitive data such as keystrokes, sites visited, emails and more.

1.6.1 Spyware for breaking access security

Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes (also known as key logging), passwords, and other valuable data.

Spyware can also negatively affect a computer's performance by installing additional software, redirecting web browser searches, changing computer settings, reducing connection speeds, changing the homepage or even completely disrupting network connection ability. Spyware can also be used as a type of adware, where the software delivers unsolicited pop-up ads in addition to tracking user behavior.

Typically, spyware is installed when a user installs a piece of free software that they actually wanted. When the desired software is installed, the spyware will piggyback on the installation and start collecting data from the user's activities. The user can also be tricked into installing the spyware through a Trojan horse as well as it pretending to be a free piece of security software. Spyware authors have been known to pay shareware developers to bundle their spyware with the legitimate software as well as simply repackaging freeware and bundling it with their own spyware. Drive-by downloading is another method used to install spyware on an unsuspecting user's computer

1.6.2 Brute-force attack spyware

A brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data[1] (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space.

When password guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because of the time a brute-force search takes.

When key guessing for modern cryptosystems, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. A cipher with a key length of N bits can be broken in a worst-case time proportional to 2N and an average time of half that.

Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when the code has been cracked. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it.

Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one.

The term "brute-force" is not the only term to name such a type of attack. It can also be called "brute-force", "brute force" and just "brute" (that is common in names of programs that perform brute-force attacks).

1.7 Cryptanalysis

Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. This is known as breaking the cipher, cipher text, or cryptosystem.

Breaking is sometimes used interchangeably with weakening. This refers to finding a property (fault) in the design or implementation of the cipher that reduces the number of keys required in a brute force attack (that is, simply trying every possible key until the correct one is found). For example, assume that a symmetric cipher implementation uses a key length of 2^128 bits (2 to the power of 128): this means that a brute force attack would need to try up to all 2^128 possible combinations (rounds) to be certain of finding the correct key (or, on average, 2^127 possible combinations) to convert the ciphertext into plaintext, which is not possible given present and near future computing abilities. However, a cryptanalysis of the cipher reveals a technique that would allow the plaintext to be found in 2^40 rounds. While not completely broken, the cipher is now much weaker and the plaintext can be found with moderate computing resources.

There are numerous techniques for performing cryptanalysis, depending on what access the cryptanalyst has to the plaintext, ciphertext, or other aspects of the cryptosystem. Below are some of the most common types of attacks:

1.8 Ethical hacking

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

Hackers access computer system or network without authorization. At the same time they break the law. While ethical Hacker, performs most of the same activities with a hacker, but with owner's permission. Sometimes they are employed by companies to perform penetration tests.

For hacking to be deemed ethical, the hacker must obey the following rules:

- Expressed (often written) permission to probe the network and attempt to identify potential security risks.
- You respect the individual's or company's privacy.
- You close out your work, not leaving anything open for you or someone else to exploit at a later time.
- You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware, if not already known by the company.

The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerability to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.

One of the first examples of ethical hacking occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems. It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

1.9 Banks 'security against brute-force attack on ATM passcode

A Brute Force attack will take few milliseconds to crack a 4 digit PIN (10,000 possible PINs). Have you ever wondered why the PIN (Personal Identification Number) for most of the commercial ATM cards is only 4 digits ? Some banks do allow you to choose longer PINs but the minimum number of digits is mostly 4.

Despite the smaller length, PIN is still an effective way of securing the ATM card. Here are the reasons why:

1**. Two factor Authentication**

An ATM access is really a two-factor authentication. i.e, the authentication happens by
a. Something you know: your PIN
b. Something you have: Your ATM Card

Note: A three factor authentication adds 'something you are' such as your voice, finger print, hand geometry, iris, retina etc.

2. **Bank's Security Database is (supposedly) secure**

A brute force attack (a.k.a dictionary attack) generally requires a copy of the security database (or password file) to run the attack against. But Bank's security database is generally super-secure (or at least we hope so). This means an attacker needs to go through the good-old way of manually trying the 10,000 combinations of PIN in an ATM machine (or in a website).

This is where the Access control comes in to play. After three failed attempts, the ATM card gets locked down by the system. And the ATM card is useless from there.

2. RESEARCH SCOPE

This research attempts to see the possibility of using brute force embedded on software to break PIN of four digit. The attempts made in breaking the software will be taken, so as to see whether in three attempt there is any PIN that is broken; if this occur, it will be established that security system used by commercial bank is ineffective.

Several PIN will be used during this experiment, and the spyware designed(the application) will only use brute force without making use of personal details of the owner of the card or the database of PIN. The PIN supplied is masked away from the spyware, the only way to get it is by making intelligent guesses to arrive at the correct PIN in N number of attempts.

3. PROBLEM IN FOCUS

ATM PIN are passcodes and are therefore less secure as passwords and passphrases, the only security commercial banks have on useof PIN is ability to block card on three wrong attempt to supply the PIN. This research want to find out whether this security is good enough to block spyware attempting to spy on cards' PIN. The researchers are presuming that this security is not good enough, however, an experiment is needed to find out this..

4. OBJECTIVES

The main objective behind this research work is to employ the use of a spyware using brute force to infiltrate ATM machines security and hack PIN. The number of attempt taken by the spyware will be documented to see whether it can escape the three attempts blocking security of ATM machines.

5. IMPLEMENTATION & METHODOLOGY

Visual Pascal programming language is used to design a small spyware that will be used in this experiment. The methodology the software will use in infiltrating PIN is the use of brute force.

The spyware has no knowledge of the ATM card's owner neither the ATM database, PIN supplied to the system is masked from the spyware. The spyware solely relies on brute force to make intelligent guesses on PIN having four digits.

5.1 Brute-force attack on ATM Passcode

Brute force can be used to break PIN by making guesses and forming combination of numbers then attempt to login with the combination, if the combination is wrong attempt is made with another combination until the PIN is broken. Brute force will be embedded on a software that will make attempt to login to an account by hacking the PIN.

5.2 Programming language choice

Visual Pascal will provide the needed flexibility for building a spyware employing brute force to break PIN. Apart from its rich vocabulary, GUI support and structure grammar, Visual Pascal offers easy mean of deployment of software.

5.3 Program flowchart

The flowchart of the spyware activity is shown below:

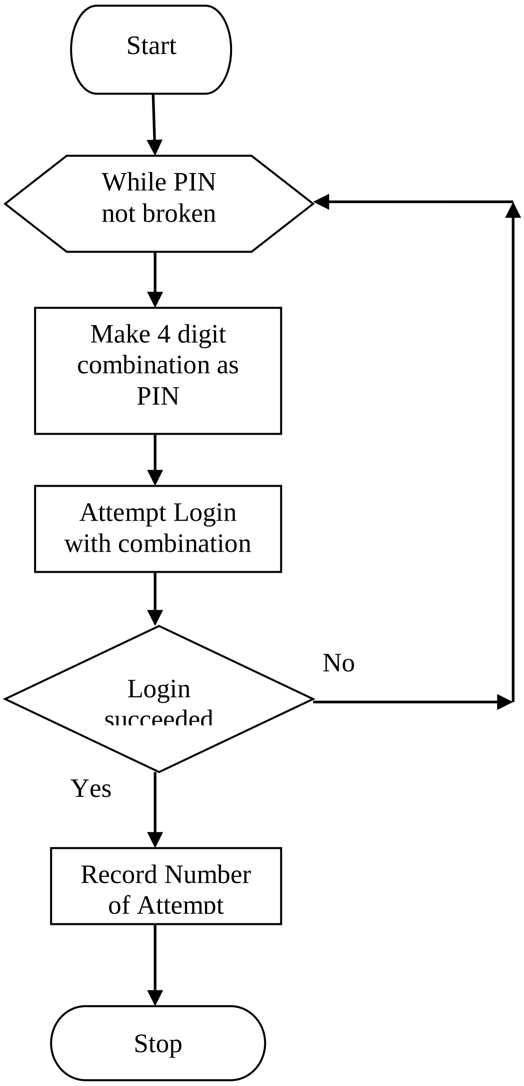


Fig. 1 Flowchart of the proposed spyware

6. TESTING

Testing of the spyware is done to find out whether the ATM security policy enforced over PIN as passcode is sufficient enough to prevent possible theft on accounts by spywares and other malware. The testing is done on clean PC with most utility software like antivirus disabled in order to have control atmosphere for successful testing.

6.1 Aim of testing

The major aim of the test is to find out whether the three-attempt blockage on Card is capable of preventing spyware illegal login to ATM after infiltrating PIN..

6.2 Testing Hypothesis

The testing hypothesis are:

- If spyware breaks PIN and login in less or equal to three attempts, then the ATM security policy imposed by commercial banks is not strong enough to prevent hacking of customers' accounts by spyware and other malware.
- If on the other hand, in all experimental attempts, the spyware is only capable of breaking PIN in more than three attempts, then the ATM security imposed by commercial banks can then say to be strong enough to prevent hacking of customers account using brute force by human or software.

6.3 Screen Capture

The screen captures of the spyware during some of the testing are shown below:

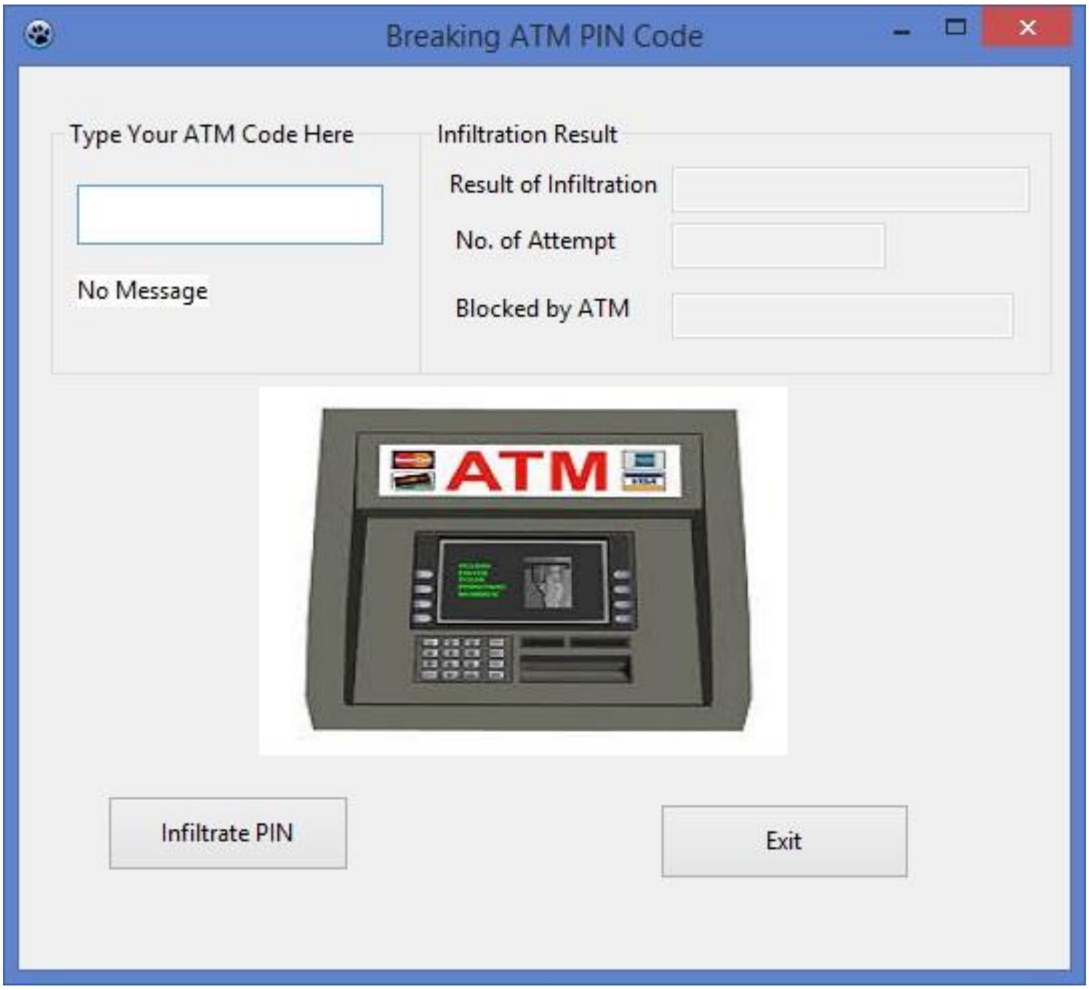
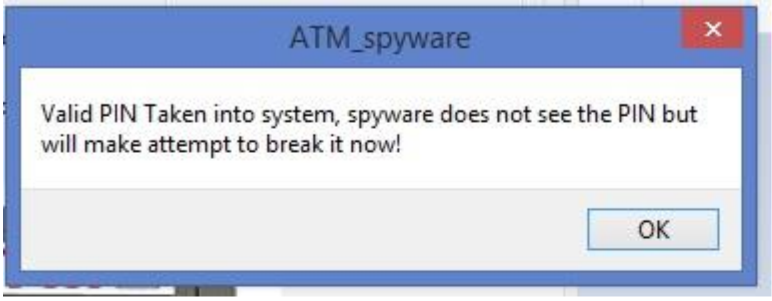


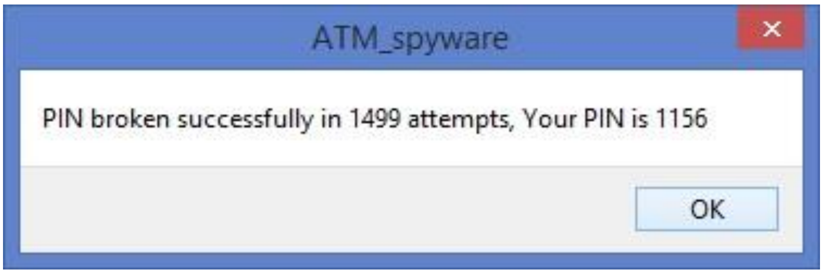
Fig. 2 Spyware Main Page



ATM_spyware

Valid PIN Taken into system, spyware does not see the PIN but will make attempt to break it now!

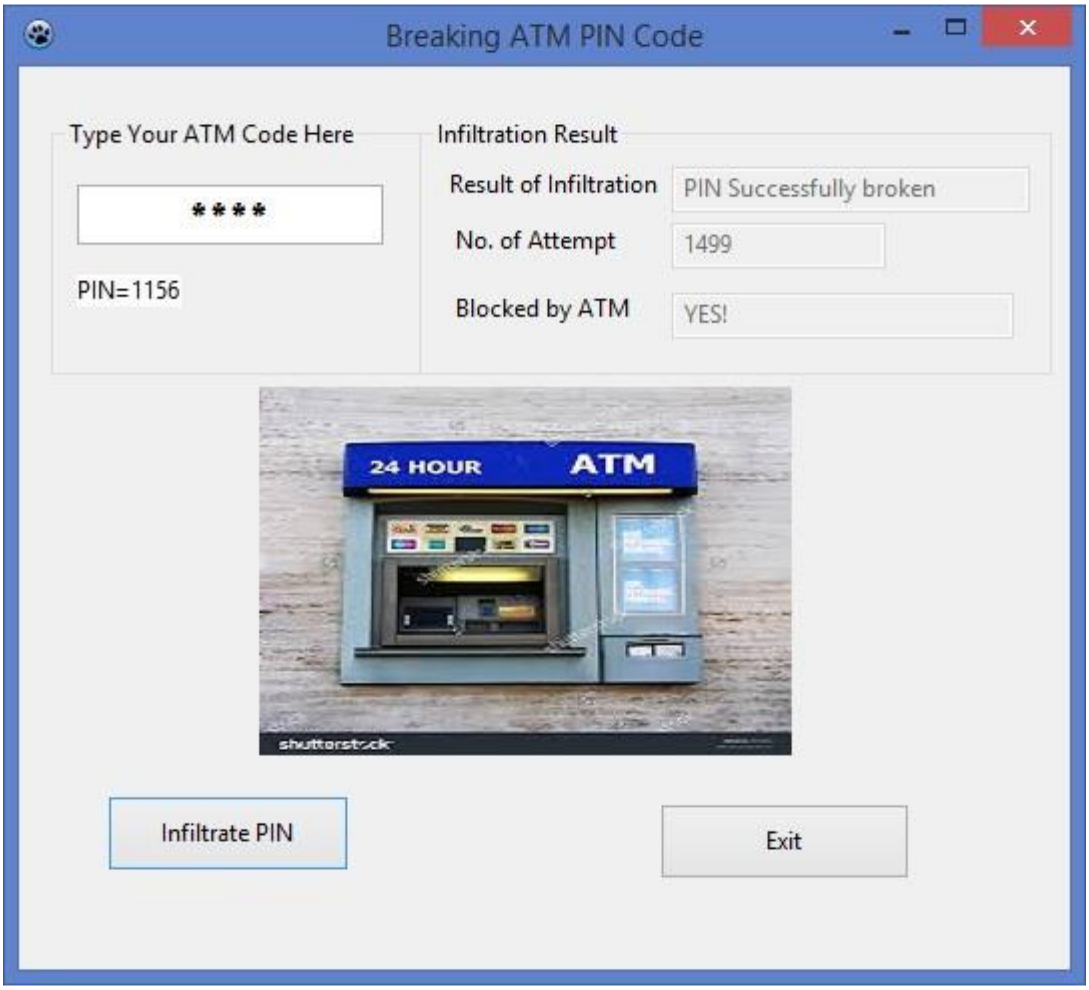
Fig. 3 PIN supplied to the system.



ATM_spyware

PIN broken successfully in 1499 attempts, Your PIN is 1156

Fig. 4 PIN successfully hacked



Breaking ATM PIN Code

Type Your ATM Code Here

****

PIN=1156

Infiltration Result

Result of Infiltration: PIN Successfully broken

No. of Attempt: 1499

Blocked by ATM: YES!

Fig. 5 Final result of PIN hacking process

6.4 Result of Test

The result of successful hacking of different PIN by the software is shown on a table below:

Table 1. Some of the result obtained during testing

S/n	PIN	Hacking Result	Number of Attempts before success
1.	**0401**	**PIN Hacked Successfully**	**13,507**
2.	**5892**	**PIN Hacked Successfully**	**12,158**
3.	**7744**	**PIN Hacked Successfully**	**760**
4.	**6325**	**PIN Hacked Successfully**	**28,660**
5.	**6325**	**PIN Hacked Successfully**	**27,219**
6.	**0000**	**PIN Hacked Successfully**	**17,558**
7.	**1111**	**PIN Hacked Successfully**	**796**
8.	**5911**	**PIN Hacked Successfully**	**11,259**
9.	**1041**	**PIN Hacked Successfully**	**3,928**
10.	**4680**	**PIN Hacked Successfully**	**17,501**
11.	**0077**	**PIN Hacked Successfully**	**16,577**
12.	**2190**	**PIN Hacked Successfully**	**32,244**
13.	**9306**	**PIN Hacked Successfully**	**1,428**
14.	**2507**	**PIN Hacked Successfully**	**8,050**
15.	**7112**	**PIN Hacked Successfully**	**5,140**
16.	**0123**	**PIN Hacked Successfully**	**11,389**
17.	**1974**	**PIN Hacked Successfully**	**17,926**
18.	**9003**	**PIN Hacked Successfully**	**196**
19.	**4190**	**PIN Hacked Successfully**	**14,656**
20.	**8127**	**PIN Hacked Successfully**	**2953**

After 100 PIN were hacked by the freeware, the result shows no PIN was hacked in a maximum of three attempts and therefore all the hacking attempts on 100 PIN will not be successful on ATM machines as all the cards will be blocked by the system. This result indicate the security measure of blocking card after wrong PIN is inputted for more than three times is strong enough to prevent a spyware or human using brute force to hack an account. This result has contradicted what the researchers initially presumed that it will be possible to by-pass the ATM security with a spyware using brute-force.

However, the spyware used in this experiment can repeat guess, this resulted in attempts going beyond 10,000. There are 10,000 combinations of PIN at all times and only one is correct. It may be possible, if the same spyware is modified not to repeat guess, may be it can bypass the ATM system

7. CONCLUSION

The aim of this research has been achieved and the research has shown the strength of ATM security policy is capable of thwarting brute force (with repetition) from hacking into accounts, even though PIN is a weak method of access authentication.

8. RECOMMENDATION

We hereby recommend the continue usage of three PIN attempts in all ATM machines by commercial banks and further recommend the integration of other security measures to increase the security of the system, options like biometric authentications can be added to ATM. We likewise recommend subsequent researches on the same area using more intelligent spyware, so that loopholes can be detected easily before villains use such methods on the system.

10. ACKNOWLEDGEMENTS

All consulted materials are duly acknowledged.

11. REFERENCES

'The purpose and Process of Security Access Control', retrieved from https://bookstrategic.wordpress.com/2011/12/05/the-purpose-and-process-of-security-access-control/

Computer Hope, (2016), 'Ethical Hacking' retrieved from http://www.computerhope.com/jargon/e/ethihack.htm

Kaspersky Lab, (2016), 'What is Spyware?-Definition' retrieved from http://usa.kaspersky.com/internet-security-center/threats/spyware#.Vwn96TvKuIV

Linkedin Corporation, (2016), 'Presentation on ethical hacking', retrieved from http://www.slideshare.net/giridhar_sadasivuni/hacking-ppt?next_slideshow=1

PC Tools, (2016),'What is spyware and what does it do', retrieved from http://www.pctools.com/security-news/what-is-spyware/

Tech Target, (2016), 'Ethical Hacker', retrieved from http://searchsecurity.techtarget.com/definition/ethical-hacker

Tech. Target, (2016), 'cryptanalysis', retrieved from http://searchsecurity.techtarget.com/definition/cryptanalysis

Wikimedia team, (2016), 'Brute-force attack', retrieved from https://en.wikipedia.org/wiki/Brute-force_attack

Wikimedia team, (2016), 'Passphrase', retrieved from https://en.wikipedia.org/wiki/Passphrase

Appendix A
Source Code

```
unit Main;

{$mode objfpc}{$H+}

interface

uses
  Classes, SysUtils, FileUtil, Forms, Controls, Graphics, Dialogs,
StdCtrls,
  ExtCtrls;

type

  { TForm1 }

  TForm1 = class(TForm)
    Button1: TButton;
    Button2: TButton;
    EdtResult: TEdit;
    EdtPIN: TEdit;
    EdtResult1: TEdit;
    EdtResult2: TEdit;
    GroupBox1: TGroupBox;
    GroupBox2: TGroupBox;
    Image1: TImage;
    Image2: TImage;
    Img3: TImage;
    Img2: TImage;
    Img1: TImage;
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    LblMsg: TLabel;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
    procedure EdtPINChange(Sender: TObject);
  private
    { private declarations }
  public
    { public declarations }
    PIN:Integer;
  end;

var
  Form1: TForm1;

implementation

{$R *.lfm}

{ TForm1 }
```

```
procedure TForm1.EdtPINChange(Sender: TObject);
var
  tempPIN:Integer;
begin
   {tempPIN:=strtoInt(EdtPIN.Text);}

end;

procedure TForm1.Button2Click(Sender: TObject);
begin
  halt;
end;
function  IsNumeric(Value:  string;  const  AllowFloat:  Boolean):
Boolean;
var
  ValueInt: Integer;
  ValueFloat: Extended;
  ErrCode: Integer;
begin
// Check for integer: Val only accepts integers when passed integer
param
Value := SysUtils.Trim(Value);
Val(Value, ValueInt, ErrCode);
Result := ErrCode = 0;      // Val sets error code 0 if OK
if not Result and AllowFloat then
    begin
    // Check for float: Val accepts floats when passed float param
    Val(Value, ValueFloat, ErrCode);
    Result := ErrCode = 0;    // Val sets error code 0 if OK
    end;
end;
procedure TForm1.Button1Click(Sender: TObject);
var
  IntFlag, broken:boolean;
  guess, attempt:Integer;
begin

  if(EdtPIN.GetTextLen <>4) then
  begin
    showmessage('Length of PIN should be Four!');
  end
  else
 begin
    IntFlag:=IsNumeric(EdtPIN.Text,false);
    if(IntFlag=false) then
     begin
       showmessage('PIN can only be integer!');
     end
     else
     begin
        showmessage('Valid  PIN  Taken  into  system,  spyware  does  not
see the PIN but will make attempt to break it now!');
        PIN:=strtoint(EdtPIN.Text);
        randomize;
        broken:=false;
        attempt:=0;
        while(broken=false) do
         begin
            guess:=random(9999);
            attempt:=attempt+1;
            if(guess=PIN) then broken:=true;
          end;
         showmessage('PIN        broken        successfully        in
'+inttostr(attempt)+' attempts, Your PIN is '+inttostr(guess));
         EdtResult.Text:='PIN Successfully broken';
         EdtResult1.Text:= inttostr(attempt);
         LblMsg.Caption:='PIN='+inttostr(guess);
         if (Attempt<=3) then
          begin
            EdtResult2.Text:='NO!';
            img3.Visible:=false;
            img1.Visible:=false;
            img2.Visible:=true;
          end
         else
          begin
            EdtResult2.Text:='YES!';
            img1.Visible:=false;
            img3.Visible:=true;
            img2.Visible:=false;
          end;
     end;
 end;


end;

end.
```

Authors

Abubakar Muhammad

He instructed Computer Science courses in Professor Iya Abubakar Community Resource Centre, Bauchi as Consultant Instructor and later as Permanent Instructor.

He also instructed different Computer related courses in Institute of Computer & Management Studies, Bauchi and is a CEO of Gwani Software limited, an ICT Solutions Provider Company based in Bauchi town. He had his Bachelor of Technology Degree in Computer Science and Post Graduate Diploma from Abubakar Tafawa Balewa University, Bauchi. Currently he is pursuing his Masters degree in Computer Science from the same university. He is currently a staff of The Federal Polytechnic, Bauchi in Department of Computer Science. His research focus is designing software applications and Artificial Intelligence theories and practices.

Zainab Aliyu Musa

She first worked in the ICT unit of Bauchi State Board of Inland Revenue Service as Data Processing officer. She had her Bachelor of Science Degree in Information Systems from American University of Nigeria (AUN), and Post Graduate Diploma in Education from NTI. She is currently a staff of The Federal Polytechnic, Bauchi in Department of Computer Science. Her research focus is on use of software applications in information systems and system analysis & design.

Adonu Sunday Ejiyime

He has been teaching computer courses in Department of Computer Science, The Federal Polytechnic Bauchi for over a decade. He has a Bachelor of Engineering (B. Eng) degree in Computer Science and Engineering obtained from Enugu State University of Science and Technology and a Master of Science (M.Sc) in Electronic and Communication Engineering from University of Huddersfield, UK. His research interest is on machine intelligence and computer applications to automation.