International Journal of Engineering & Technology, 7 (2.33) (2018) 59-63

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A virtual keyboard security system for automated teller machine

V. Brindha Devi [1, 2] *, S. Sindhuja [2], S. Shanthini [2], M. Hemalatha [2]

[1] *Associate Professor*
[2] *Department of Information Technology, Sri Sairam Institute of Technology, West Tambaram, Chennai*
**Corresponding author E-mail: hodit@sairamit.edu.in*

Abstract

The Automated Teller Machines (ATM) are used for cash withdrawals. Meanwhile as ATM lacks security, thefts occurring in the ATMs are also high. Our proposed system minimizes those break-ins occurring in the ATM's by instigating a low cost standalone embedded sys-tem using Arduino Microcontroller. This system is proposed for ATM security, comprising of the components namely RGB tag, Global System for Mobile communication (GSM), Global Positioning System (GPS), Virtual Keyboard and camera. Authentication by virtual keyboard thus helps the public to protect their credentials from being captured by malicious bots, key loggers and spyware. Whenever theft occurs, Buzzer makes an alarm, DC Motor turns ON and the door of ATM is closed. The nearby police station and corre-sponding bank authorities is alerted by the GSM Modem that sends messages along with the location. This will prevent the robberies and the person in-volving in the robbery can be easily caught. In short, it discusses the methods that are used to detect the venture, initiate preemptive measures and forewarn the officials through GSM network. This system thus heightens the safety of ATM users as well as the ATM's against forthcoming attacks effectively.

Keywords: *Arduino; DC Motor; GSM; GPS; Image Processing; Shuffling Algorithm.*

1. Introduction

Obtaining information without the owner's knowledge or permis-sion is one which has been wanted throughout human history. With the increase in population that uses ATM, the attacks on the machine both hardware and software also increases. An ATM fraud includes any thoughtful 'criminal' technique which is done to obtain something of value. ATM includes two types of attacks: Physical attacks and ATM frauds. One of the most common phys-ical attacks is trying to crack open the safe or treasury box in the ATM machine. Other attacks use metallic instruments to cut through the ATM's metal case to withdraw the vault. In usual, thief tries to break the lock of ATM's safe deposit box and flees as siren goes off. Some thieves take the antiquated route and crack them right open .To avoid this type of attacks alert-based monitor-ing system is used. In this system when anyone enters the ATM room, it triggers the sensor which sends an alert to the monitoring station. In case of any unwanted activities, sensor sends alarm alert signal to monitoring station but as technology improves thieves started using skimming devices. The personal information is stolen by the hidden secret electronic items which scans the information in a magnetic strip and stores it. But still thieves need PIN number and that's where spy cameras comes in. Some ATM skimming schemes have cameras in keypads to capture PIN num-bers. Just like the card skimmers, skimming keypads are designed to mimic the keypad's design. Thus in this paper, we provide fea-sible solution for both physical attacks and frauds. Even though siren plays a major role in alerting the bank about the theft, it is not enough to protect, as thief run away before the bank authority reach the place. Hence we use Vibration detection sensor to detect the disturbance made in cash box that in turn switch on DC motor to close the shutter to avoid thief running away. It also sirens and sends message with the location to the bank authority and nearby police stations. Also, Keypad skimming can be avoided by im-plementing virtual keyboard with shuffling algorithm. The key-board shuffles its keys whenever the user clicks any key.

2. Related work

As number of people using ATM has been widely increased, the safety to use it was decreased. The existing paper [1] describes that the vibration sensor monitors the vibration continuously and when the invader tries to break the ATM machine vibration sen-sors detects vibration as HIGH and alert the police station and bank authorities by sending messages using GSM module. This paper [2] has IR sensor which senses the presence of users and turns on Fan and Light. If ATM is meddled, then SMS is sent to two main stations via GSM. In case if thief runs with the cash box, GPS is used to track the location. But often thief gets escaped before the police arrive and needs to track him. The paper [5] [6] describes the face recognition system and biometric system where it checks for fingerprints and face recognition and makes the shut-ter close when some wrong matches occur. But those can be easily tampered. This paper [5] also uses facial recognition, If the face is not identified properly, it warns the user to adjust him/her properly to detect the face. Still if the face is not spotted, the system will lock the door of the ATM for security purpose. As soon as the door is lock, the system will automatically generate 3 digit OTP code. The OTP code will be sent to the watchman's mobile num-ber through SMS using GSM module which is connected with the raspberry Pi. Watchman enters the OTP through keypad interfaced with the Raspberry Pi Board. The OTP undergoes verification and if it matches the door will be unlocked else it will remain locked. The paper[7] deals with a security threat of wearable devices for gaining personal information while people are using the key-based security systems, a wearable device can be misused to differentiate

mm-level distances and to track the directions of the user's hand movements, which help attackers to find the trajectories of the user's hand and to recover the secret key entries. Hence, in our paper we use vibration detection sensor to detect the tampering and makes the shutter or door close using the DC motor and an alert is sent through SMS using GSM to bank authority and nearby police to take necessary actions as soon as possible. GPS is used to find the exact location the crime has occurred .But even though it provides solution for physical attacks, there should be a solution for ATM frauds too. Hence in the latter module we use virtual keyboard system to avoid those frauds by finding PIN number of the cards. Whenever the user clicks any key, the virtual keyboard provides security by shuffling its keys. Hence it is not easy to find PIN numbers of users by heat analysis rather by trajectory of hands in virtual keyboard. In addition we provide security by allowing person to be authorized by sending OTP to the registered mobile number. The card activates only if user enters correct OTP.

3. Issues

Some of the issues in ATM are described as follows:

- Physical Attacks

One of the most common physical attacks is trying to crack open the safe or treasury box in the ATM machine

- Logical Attacks
- Shoulder surfing
- PIN compromise by viewing while user enters PIN
- Transaction Reversal Fraud
- TRF involves writing an error program that makes it appear as though the cash had not been handed out
- Card Trapping
- Trapping is the process of holding the physical card itself through a device fixed to the ATM.
- Cash Trapping
- A device is used by hoaxer to physically trap the cash that is dispensed.
- Card Skimming
- Skimming refers to the stealing of the user card data, enabling the criminal to create the fake card.
- ATM "jackpotting"
- It's a sophisticated crime that forces the ATM machines to shell out huge volumes of cash by installing malicious software and/or hardware at ATMs.

Our proposed work was based on embedded technology, virtual keyboard software and vibration sensors are used to continuously monitor its environment for doubtful activities like card frauds and thefts that might put in danger the ATM and people nearby. This paper analyses the different forms of physical attacks and some PIN compromising attacks on ATM's and discusses the methods that are used to detect the attack, begin the initiative measures and warn the officials through GSM network. Thus the proposed work enhances the security of ATM's against future attacks effectively.

4. Architecture

The architecture of modules in this paper are given as User authentication module, Secured transaction module and the physical attack detection module.

The components used for the proposed system design are in the table below.

Table 1: Components or System Requirements

Components	Configuration
Hardware	• Arduino with ATmega328 microcontroller • Vibration detection sensor • DC motor • Camera • Laptop or a system • GSM • GPS
Software	• Arduino IDE • Python 3.5.2 • MATLAB

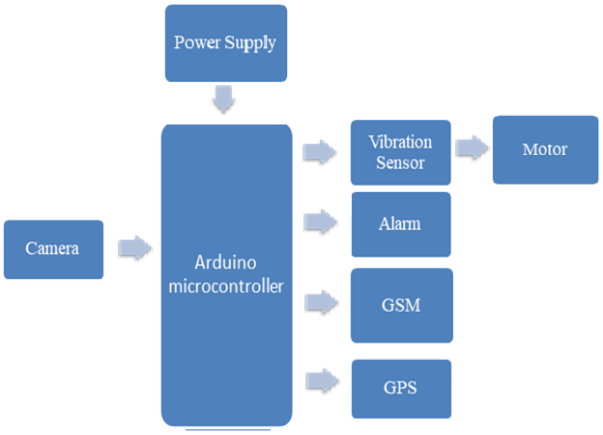

Fig. 1: The Main Architecture.

The architecture diagram is represented as two different diagrams since the proposed system gives solution for both physical and PIN compromise attacks in ATM. These diagrams represent the working of system in detail. Fig.2 represents the system that avoids the PIN compromise attacks effectively. First, the user authentication is done by sending OTP to the user registered mobile number. Then the 4-digit PIN for transaction is entered using virtual keyboard which shuffles every time when the user clicks any key. This protects the user credentials as well as prevents logical attacks. Fig.3 represents the system that avoids the Cash-Box theft. The vibration sensor is used to continuously monitor its environment for doubtful activities like card frauds and thefts that might jeopardize the ATM and people nearby. When the vibration is HIGH, buzzer alarms, DC motor ON and the message is sent to the police as well as bank authorities along with the location using GSM and GPS module interfaced with Arduino microcontroller. This prevents physical attacks on ATM.

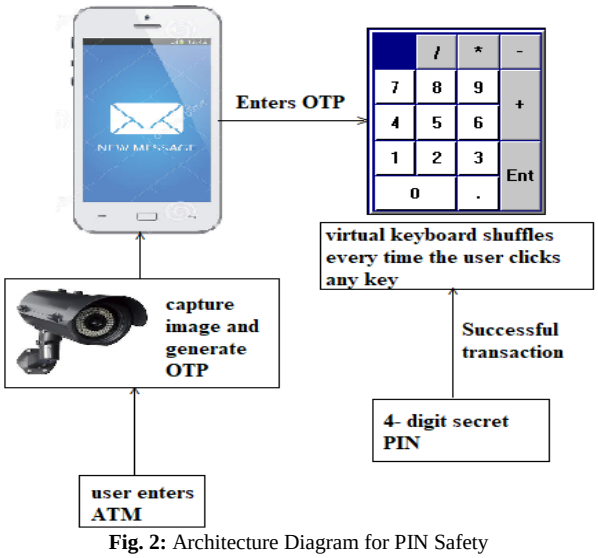

Fig. 2: Architecture Diagram for PIN Safety

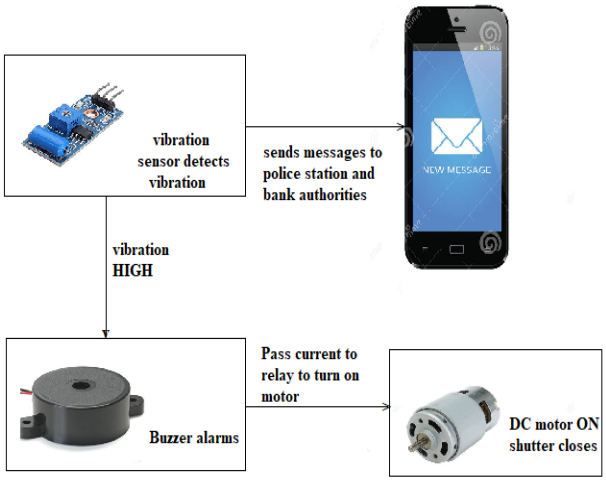

Fig. 3: Architecture Diagram for Vault Safety

a) User authentication module

This module uses image processing techniques to generate OTP. The random number is generated as OTP by processing color codes of your dresses. A Camera on top of ATM machine detects the color which is in high proportion to it and sends the OTP to the registered mobile number accordingly. Image processing happens as follows: First, image enhancement is done to achieve better resolution. Then image classification is to compare and match the color which is in high proportion. Thus random number is generated as OTP and this OTP is sent as serial data to the Arduino microcontroller. This microcontroller sends SMS to the registered mobile number. The image processing is done using MATLAB.

Fig. 4: User Authentication Module Flow Diagram.

b) Secured transaction module

This module uses the Fisher-Yates algorithm as a basic idea. The fisher-yates algorithm is also known as Knuth algorithm. It is an algorithm to shuffle the sequence through random permutation. Sattalo's algorithm can also be used which is based on cyclic permutations.

Following is the basic code of Fisher-Yates algorithm which is used to Shuffle an array of m elements through permutation,

For a from m-1 downto 1 do

b= random integer such that 0 <= b< = a

Exchange s[b] and t[b]

Following is the basic sattalo's algorithm which use cyclic permutation to shuffle:

From rand import range

def sattoloCycle(items):

a = len(items)

While a > 1:

a = a - 1

b = randrange (a) # 0 <= j <= i-1

Items[b], items[a] = items[a], items[b]

By using this algorithm as basic code, a program to shuffle the keys is written in Python. Thus when the user enters his/her OTP, every time he presses the key on the virtual keyboard, it gets shuffled. Hence it is difficult for the thief to guess the PIN numbers.

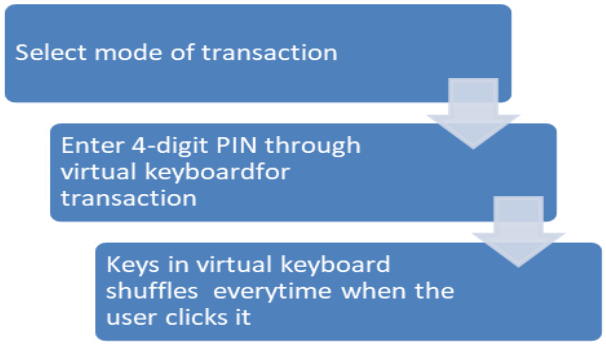

Fig. 5: Secured Transaction Module Flow Diagram.

c) Physical attack detection module

In this module, the vibration detection sensor is set for a certain range of vibration as a boundary. When someone tries to break something, vibration crosses the range. Then the Arduino microcontroller comes to act. When vibration detection sensor sends serial data, the Arduino microcontroller is programmed in embedded c as such to siren as well as to switch on DC motor to make the shutter close. The DC motor is also integrated with Arduino microcontroller. GSM module integrated with Arduino is used to send the message along with the location of ATM to the nearby police station and to bank authority. In order to locate the nearby police station as well as the bank, GPS module is used. This module provides protection over the physical attacks generally cash box theft.

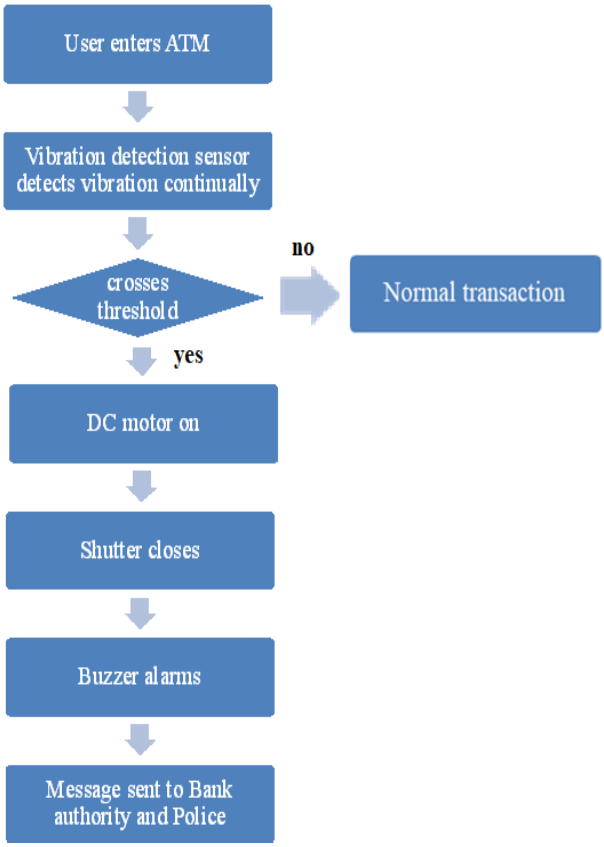

Fig. 6: Physical Attack Detection Flow Diagram.

5. Results

The Secured transaction module produces the output screen as follows:

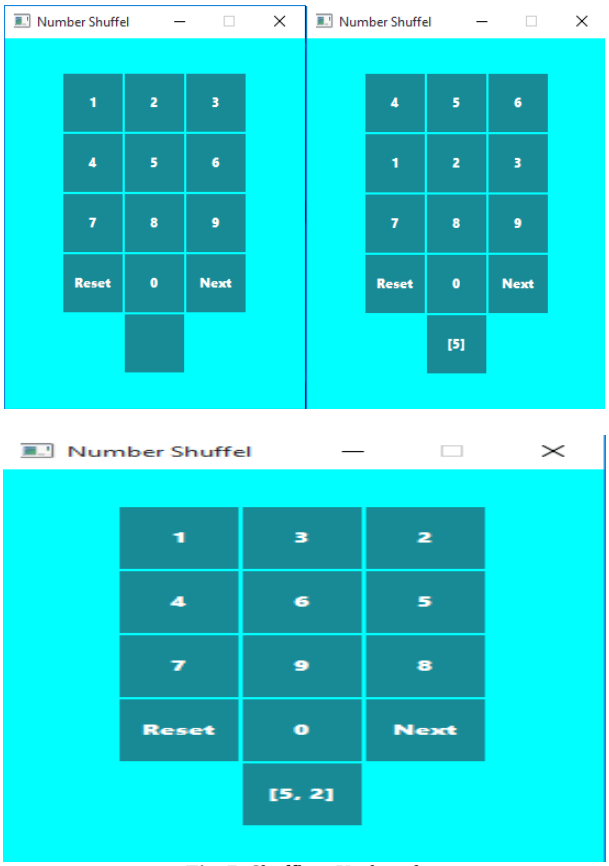

Fig. 7: Shuffling Keyboard.

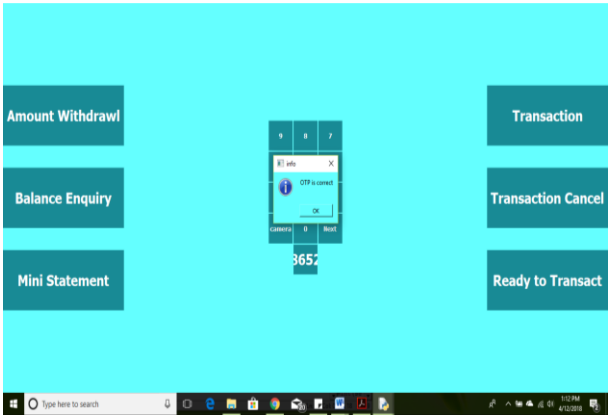

Fig. 8: Result of User Authentication Module.

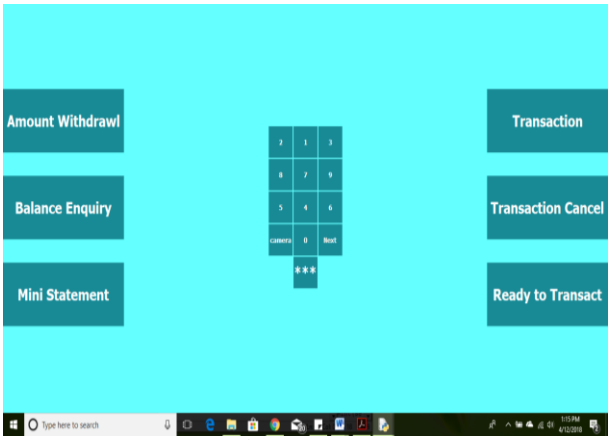

Fig. 9: Result of Secured Transaction Module

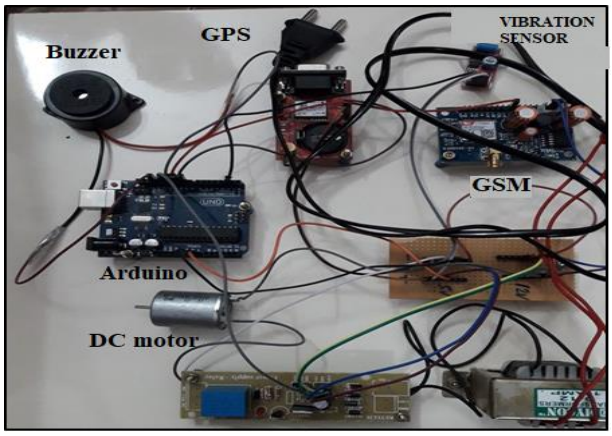

Fig. 10: Result of Physical Attack Detection Module.

Table 2: Test Cases

Test Steps	Expected Results	Actual Results	Status Pass/Fail
OTP Generation	Webcam must recognize the colour and sent the OTP to the registered mobile number.	Webcam had recognized the colour and delivered the OTP to the registered mobile number.	Pass
Virtual Keyboard	The keys in the virtual Keyboard should shuffle each time when the user presses the key.	The keys in the virtual Keyboard had shuffled each time when the user presses the key.	Pass
OTP authentication	When wrong OTP is entered it should report an error.	Reported an error When wrong OTP is entered.	Pass
Pin Authentication	When wrong Pin number is entered it should report an error.	Reported an error When wrong Pin number is entered	Pass
High vibration detection	When high vibration occurs it should sent an alert message , turn on the DC Motor and ring the alarm	Alert message is sent	Pass
		DC motor ON	Pass
		Buzzer rings	Pass

6. Summary and outlook

In this paper, the first part of the work describes the way to avoid physical attacks such as cash box theft. The latter part describes the way to help users to safeguard their credentials from being saved by malicious bots, spyware, and key loggers. The first part consists of Vibration detection sensor and once the vibration exceeds the threshold, it makes the DC motor ON to close the shutter and sends SMS to bank authority as well as to the nearby police station by using GSM and GPS modules integrated with Arduino microcontroller. The latter part describes OTP generation with respect to color codes and the entry of OTP and secret pin with the help of virtual keyboard. The virtual keyboard shuffles (Fisher-Yates algorithm) every time when the user clicks it

7. Conclusion

The results indicate that the major threats such as the recent attack ATM “jackpotting”—a crime that spits out huge volumes of cash. This can be avoided by the above techniques. Hence this embedded technology provides safety and security measures to prevent such attacks in future. The proposed system hence increases the security of ATM's against risky attacks effectively. But still, there may be some software attacks possible. It would be desirable if security is provided to avoid those software hacks.

Acknowledgement

We would like to show our gratitude to Dr.V. Brindha devi, Head of the Information Technology Department, Sri Sairam Institute of Technology for sharing their pearls of wisdom with us during the course of this research and for comments that greatly improved the manuscript.

References

[1] M. Ajaykumar, N. Bharath Kumar, "Anti-Theft ATM Machine Using Vibration Detection Sensor", B.Tech-CSE Department & JNTU Hyderabad India. International Journal of Advanced Research in Computer science and software, vol. 3, no. 12, December 2013.

[2] Bharati M Nelligani, N V Uma Reddy, Nithin Awasti,"Smart ATM security system using FPR, GSM, GPS", Invenive Computation Technologies (ICICT) , International Conference , January 2016.

[3] Ulrich Burgbacher , Klaus Hinrichs "Synthetic Word Gesture Generation for Stroke-Based Virtual Keyboards" Department of Computer Science, University of Münster, Münster, Germany IEEE Transactions on Human-Machine Systems (Volume: 47,issue: 2, April 2017).

[4] Mrs.S.P.Balwir,Ms.K.R.Katole,Mr.R.D.Thakare,Mr.N.S.Panchbudhe,Mr.P.K.Balwir. "Secured ATM Transaction System Using Micro-Controller" International Journal of Scientific Engineering Research Volume 4, Issue 4, April 2014.

[5] Dhiraj Sunehra, "Fingerprint based biometric ATM authentication system", Department of Electronics & Communication Engineering Jawaharlal Nehru Technological University Hyderabad India. International Journal of Engineering Inventions, vol. 3, no. 11, June 2014.

[6] Jignesh J. Patoliya ,"Face Detection based ATM Security System using Embedded Linux Platform"2017 second International Conference for Convergence in Technology (I2CT).

[7] C. Wang, X. Guo, Y. Chen, Y. Wang and B. Liu, "Personal PIN Leakage from Wearable Devices," in IEEE Transactions on Mobile Computing, vol. 17, no. 3, pp. 646-660, March 1 2018.

[8] K. Kadir, M. Kamaruddin, H. Nasir & S. Safie, "4th International-Conference on Engineering Technology and Technopreneuship (ICE2T)", 2014, p. 335.

[9] S. Monk, first Ed., Raspberry Pi Cookbook, O'REILLY, 2013.

[10] Open CV Website. [Online]. Available: http://www.opencv.org.

[11] Homepage on Open CV: Face Detection using Haar Cascades.[Online].Available.http://docs.opencv.org/master/d7/d8b/tutorial_py_face_detection.html#gsc.tab=0.

[12] L. Zhuang, F. Zhou, and J.D. Tygar, "Keyboard Acoustic Emanations Revisited," ACM Trans. Information and System Security, vol. 13, article 3, 2009.

[13] F. Maggi, A. Volpatto, S. Gasparini, G. Boracchi, and S. Zanero, "AFast Eavesdropping Attack against Touchscreens," Proc. Seventh Int'l Conf. Information Assurance and Security (IAS), 2011.

[14] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp)iPhone:Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers," Proc. ACM Conf. Computer and Comm.Security, 2011.

[15] D. Balzarotti, M. Cova, and G. Vigna, "ClearShot: Eavesdropping on Keyboard Input from Video," Proc. IEEE Symp. Security and Privacy, 2008.

[16] All about skimmers. http://krebsonsecurity.com/all-about-skimmers/.

[17] P.A. Viola and M.J. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," Proc. IEEE CS Conf. Computer Vision and Pattern Recognition, 2001.

[18] K. Jung, K.I. Kim, and A.K. Jain, "Text Information Extraction in Images and Video: A Survey," Pattern Recognition, vol. 37, no. 5, pp. 977-997, 2004.

[19] H. Grabner, M. Grabner, and H. Bischof, "Real-Time Tracking via On-Line Boosting," Proc. British Machine Vision Conf., vol. 1, pp. 47-56, 2006.

[20] P.A. Viola and M.J. Jones, "Robust Real-Time Face Detection," Int'l J. Computer Vision, vol. 57, no. 2, pp. 137-154, 2004.

[21] How strong is your password? https://www.msecure.com/blog/howstrong-is-your-password/.

[22] S. Stalder, H. Grabner, and L.V. Gool, "Beyond Semi-Supervised Tracking: Tracking Should Be as Simple as Detection, but Not Simpler Than Recognition," Proc. Workshop On-Line Learning for Computer Vision, pp. 1409-1416, Sept. 2009.

[23] Android sensor event. http://developer.android.com/reference/androidHardware/SensorEvent.html.