www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 20108-20111
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.45

A Literature Survey on Password Extraction via Reconstructed Wireless Mouse Trajectory

Divya S, Anju J Prakash
M.Tech CSE
Sree Buddha College of Engineering Elavumthitta, Kerala 689625
Assistant Professor of CSE
Sree Buddha College of Engineering Elavumthitta, Kerala 689625

Abstract
Since the mouse movement data are not encrypted secret information such as password can be leaked through the displacement of mouse.Two attacks are proposed here, the prediction attack and replay attack, which can rebuild the on-screen cursor trajectories by sniffing mouse movement data. Two inference strategies are used to discover pass-words from cursor trajectories.This work is the survey to demonstrate the different techniques and tools in privacy leakage from raw mouse data.

I. Introduction

The mouse movement data can be used by the attacker to sniff secret information such as user's profile,passwordsetc.Theinformations are leaked by the reconstruction of onscreen mouse cursor trajectory.

The raw Bluetooth mouse data semantics are checked and analysedvarious mouse cursor acceleration algorithms.The Bluetooth human interface device (HID) [5] profile needs authentication and encryption support for keyboards and other HIDs.Device files are created bythe mousedev driver and user space application API are created by the evdev generic input event driver in the kernel space.TheXserver improves the mouse cursor acceleration by increasing the mouse movement in userspace.

Mouse acceleration is the mapping between the physical mouse movement and onscreen cursor motion.Since it is unable to get the source code of the Windows and Mac mouse acceleration algorithms, the replay attack is recommended to reconstruct the on-screen cursor trajectory without knowing the mouse acceleration algorithm.

The cursor positions are calculated using acceleration algo-rithm from the raw mouse movement data.Mouse Acceleration Algorithms are of into two types: (i) lightweight accelera-tion algorithm and (ii) complex acceleration algorithm.The Lightweight acceleration algorithm does not consider the packet arrival time where asThe Complex Acceleration Al-gorithm considers the packet arrival time

Lightweight Acceleration Algorithm

In Lightweight Acceleration Algorithm cursor movement is calculated from raw mouse movement coordinates and thresh-old value T.

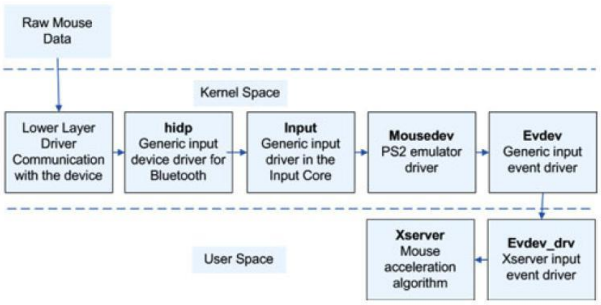

Fig. 1. Linux input device driver stack.

Complex Acceleration Algorithm

When a new mouse event arrives, a mouse event is created for the mouse packet. Next, the system first computes the velocity of the mouse movement and then computes the acceleration based on the derived velocity. Based on the raw movement information in the mouse packet and the derived acceleration, the system determines the cursor movement on screen.

If the mouse acceleration algorithm is not familiar the replay attack is the solution.In the replay attack, an attacker sniffs raw Bluetooth mouse data between a Bluetooth mouse and a victim computer using the sniffer FTS4BT[3]. Then to derive the onscreen cursor trajectory, the attacker uses a computer as the attack computer, and replays the sniffed mouse data to an impersonating computer, which is installed with the same operating system as the victim computer. The cursor trajectory on the impersonating computer is the approximate on-screen cursor trajectory on the victim computer.

II. Literature survey

A. Bluetooth Technology:

Bluetooth[16]works at 2.4 GHz frequency and it is an open specification for a short range radiotechnology for wireless communication of voice and data. Bluetooth frequency hop-

ping uses a maximum of 79 different Baseband frequencies to avoid channels that suffer from interference.A Bluetooth unit leaves the Standby or the Connection state periodically to do Inquiry or Inquiry Scan.

Inquiry procedures[13]allow a unit to discover which units are in range, and their device addresses and clocks.Bluetooth communication[19]is easierthan the traditional cable-based communicationbutit alsomakes eavesdropping much easier.Bluetooth devices have a pattern of frequencies that they transmit on set by their MAC address and clock signal. If two devices wish to communicate they must be synchronised in their hopping and, as Bluetooth is a one-to-many protocol[20], they must be able to address the packets for the intended recipient. This is done through the inquiry process which takes place at the start of communications to establish hopping patterns, identifiers and encryption keys.

B. Bluetooth Security:

Security measures of Bluetooth are necessary since there are a lot of vulnerabilities[10].Bluetooth works insecurity modes. In Security Mode 1,there is no security enforcement, meaning that the device is effectively taking no steps to protect itself. Security Mode 2 provides service level security enforcement.In this mode, a particular application is safe but no additional device protection. Security Mode 3 is the highest level of security,employing link level enforced security mechanisms. Security Mode 3 secures the device from certain intrusions and, therefore, all services and applications .

C. Types of Attacks:

Bluebugging,bluebumping,bluedumping,bluejacking, bluesmacking, bluesnarfing, bluespooofing [sic], bluestabbing,bluetoothing, and car whisperer[9] are some Bluetooth attacks.

D. Bluetooth Architecture:

Blootooth is an adhoc network which provides easy connection establishment between devices in the same physical area. A Bluetooth client is a device with a Bluetooth radio.The functions of hosts are to provide higher layer protocols, such as Logical Link Control and Adaptation Protocol (L2CAP) and Service Discovery Protocol (SDP).

The controller is responsible for the lower layers. The controller options are done by an integratedBluetooth adapter. The host and controller send information to each other using standardized communications over the Host Controller Interface (HCI). This allows hosts and controllers from different product vendors to interoperate.

E. Bluetooth Security features:

The main security services of Bluetooth are:

Authentication: verifying the identity of communicating devices based on their Bluetooth device address.

Confidentiality: preventing unauthorized devices from accessing and viewing transmitted data.

Authorization: It ensures that a device is authorized to use a service before permitting it to do so.

F. Pairing and Link Key Generation:

Link key generation is the generation of secret key.Bluetooth BR/EDR[14] performs pairing or link key generation in one of two ways. Security Modes 2 and 3 initiate link key establishment through a method called Personal Identification Number (PIN) Pairing (i.e., Legacy or Classic Pairing), while Security Mode 4 uses SSP. Both methods are described below.

G. Computer Mouse:

The Computer mouse[11] is the physical device which fits correcttly in the curve of the user's hand and enables the user, through very limited movements of the hand and fingers to give point and click instructions to the computer. A rolling ball on the underside of the mouse gives directions on where to move to the cursor on the monitor or screen, and one to three buttonsallow the user to say yes by clicking the buttons on the right instruction for the computer's next operation.

H. Logitech Advanced 2.4 GHz Technology8:

Logitech offers a variety of wireless mice, keyboards and mice + keyboard combinations which come standard with Advanced 2.4 GHz technology[2]. This technology includes:

i) Secure 128-bit (AES) encryption between device and receiver

ii) Up to 3-years battery life

iii) Range of up to 10 meters or 33 feet

With Logitech's Advanced 2.4 GHz,all the benefits of wireless are available. Logitech's wireless mice and keyboards are easy to use since no software installation or pairing are required.

I. Encryption:

Encryption is used only to the wireless link between the keyboard and the receiver. Encryption is totally transparent to the software which receives clear data from the receiver over the USB. This means that the advanced 2.4 GHz encryption is susceptible to hackers who can get physical access to the PC, or who can remotely install spy software on the PC.

Encryption Algorithm

The encryption method consists of hiding the wireless messages with a cryptogram. The encryption algorithm used is the AES 128-bit cipher, which has been adopted as an encryption standard by the US government.

Generation of Encryption Keys

When a device that requires encryption is paired to a receiver, the pairing process includes the128-bit encryption keys generation. The same unique key is constructed both in the keyboard and in the receiver based on random values exchanged during the pairing procedure.

J. An Efficient User Reauthentication and Verification System via Mouse movements:

Modeling mouse-movement[17] behavior of a user a on a machine b requires capturing both the cursor movement and the mouse events.To study a user's behavior on a mouse device,2D screen coordinates of a cursor are captured each time that detect that the mouse has moved.Then check whether the mouse has moved every 100msec.Mouse dynamics[6], with their unique

patterns of mouse movements, is a behavioral biometric.The predictable pointer acceleration code[7] is an

e Piconet to ensure that no data is being missed.

* Single Connection (Air Basic)

This is the standard Air Sniffer using the Bluetooth Com-Probe (USB dongle) as the hardware interface to Bluetooth air traffic.

Three buttons appear at the bottom of the dialog; Run, Cancel, and Help. When the dialog first opens, Cancel and Help are active, and the Run button is inactive (grayed out).starts FTS using the selected protocol stack.

N. Data Collection and Feature Extraction:

To extract features from the mouse movement[17] data set, it is necessary to compute the distance, angle, and speed between pairs of data points. These pairs can either be consecutive or they can be separated by k data points. Let the parameter k be the frequency. After getting raw features, calculate their mean, standard deviation and the third moment values over a window of N data points.In addition to the cursor movement data, collect all mouse generated events to obtain the mouse event data. Record the time of each event. To extract features from the event sequence data, group each user's event sequence data into a hierarchical structure that contains all data points at the top level. At the next level split the event data into mouse wheel movements, clicks and nonclient (NC) area mouse movements.Finally group the click data into single and double click data. There is a strong

.

two approaches for password inference: a basic inferring approach to enumerate all candidate passwords from a clicking topology and enhanced inferring approach that uses the statistical distribution of human clicking patterns to reduce the number of candidate passwords corresponding to a clicking topology. For future work,this attack can be extended to graphical passwords such as the picture password in Windows 8.For example,PassBYOP[15] is a new graphical password scheme for public terminals in which static digital images in graphical passwords are replaced by personalized tokens in the form of digital picture in private mobile phones.

detection signal for each category of this hierarchical structure that can be used to distinguish users.

Secure host data provenance verification:

Data-provenance defines integrity as the security property stating that the source where a piece of data is generated cannot be spoofed or tampered with.In order to achieve data provenance a cryptographic protocol is developed using onchip Trusted Computing Platform[21].

III. Conclusion

This Survey represents a study of password extraction Methods[1] for different Indian scripts .This paper helps researchers and developers to understand history of the wireless mouse data leakage research work for Indian scripts. This survey will be helpful for researchers in this field.In this paper, an analysis of privacy leakage from unencrypted Bluetooth mouse traffic is carried out. The Bluetooth mouse packet semantics are examined to develop two attacks, the prediction attack and the replay attack which are used to reconstruct on-screen cursor trajectories based on sniffed raw mouse movement data when a lightweight or complex mouse acceleration algorithm is used. An investigation of how packet losses and variations of packet arrival timing may affect the accuracy of reconstructed cursor trajectories. Finally, an extensive evaluation of Bluetooth mouse sniffing is performed on the inference of passwords that a user enters through an onscreen software keyboard. We proposed

References

[1] Xian Pan, Zhen Ling, AniketPingley,Wei Yu, Member, IEEE, Nan Zhang, Member, IEEE, KuiRen, Senior Member, IEEE, and Xinwen Fu, Member, IEEE. Password Extraction via Reconstructed Wireless Mouse Trajectory. IEEE Transactions on Dependable and Secure Computing, Vol. 13, NO. 4, July/August 2016.

[2] Logitech advanced 2.4 GHz technology, revision 1.1h http: [Online] *//www.logitech.com/images/pdf/roem/* . (2009, Mar.).

[3] Frontline test system FTS4BT user manual . [Online] Available:http://fte.com/docs/FTS4BT. (2010).

[4] FTS4BT Bluetooth protocol analyzer and packet sniffer . [Online] Available: http://www.fte.com/products/fts4bt.aspx. (2012).

[5] Bluetooth human interface device profile. [Online] Available: http://www.bluetooth.com. (2015).

[6] N. Zheng, A. Paloski, and H. Wang. An efficient user verification system via mouse movements. in Proc. 18th ACM Conf.CCS, Oct. 2011, pp. 139âAS150¸.at the Black Hat US, Las Vegas, NV, USA, Aug. 2008.

[7] Pointer Acceleration [Online]. [Online]. Available: http://www.x.org/wiki/Development/Documentation/PointerAcceleration. (2013).

[8] A. A. E. Ahmed and L. Traore. A new biometric technology based on mouse dynamics. IEEE Trans. Dependable Secure Comput., vol. 4, no. 3, pp. 165âAS179,¸ Jul.âASSep¸. 2007.
[9] A. Becker. Bluetooth security and hacks [Online].Available: http: //gsyc.es/ anto/ubicuos2/ . (2007, Aug.)
[10] K. Haataja Security threats and countermeasures in bluetoothenabled systems. PhD thesis, University of Kuopio, 2009.
[11] T. Engdahl. PC mouse information [Online]. Available:http://www.epanorama.net/documents/pc/mouse.html. (2014).
[12] M. Ettus. USRP products [Online]. Available: http://www.ettus.com/. (2015).
[13] Y. Gelzayd An alternate connection establishment scheme in the Bluetooth system. MasterâAZs thesis, Polytechnic Univ., 2002.
[14] Y. Shaked and A. Wool Cracking the Bluetooth PIN. in Proc. 3rd Int. Conf. Mobile Syst., Appl., Services, Jun. 2005, pp. 39âAS50¸.
[15] National Institute of Standards and Technology (NIST). Available: http*://csrc.nist.gov/publications/drafts/*800 − 121*r*1/ Draft-SP800-121-Rev1.pdf. (2011,Sep.).
[16] M. Ossmann Bluetooth keyboards: Who owns your keystrokes [Online]. Available: http://ossmann.com/shmoo-2010/. (2012).
[17] M. Pusara and C. E. Brodley. User re-authentication via mouse movements. in Proc. ACM Workshop Vis. Data Mining Comput.Secur., Oct. 2004, pp. 1âAS8¸.
[18] T. Schroeder and M. Moser. Keykeriki-Universal wireless keyboard sniffing for the masses. DeepSec Security Conference,2009.
[19] T. Schroeder and M. Moser. Practical exploitation of modern wireless devices. CanSecWest, 2010.
[20] D. Spill Final report: Implementation of the Bluetooth stack for software defined radio, with a view to sniffing and injecting packets [Online]. Available: www.cs.ucl.ac.uk/staff/a.bittau/dom.pdf. (2007, May)
[21] K. Xu, H. Xiong, C. Wu, D. Stefan, and D. Yao. Data-provenance verification for secure hosts. IEEE Trans. Dependable Secure Comput.,vol. 9, no. 2, pp. 173âAS183,¸ Mar./Apr. 2012