International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Mouse Jacking: A Survey

Varun Chitale[a]*, Anandita Bodas[b]

[a,b]*Department of Computer Science, MITCOE, , Paud Road, Kothrud, Pune 411038, India*
[a]*Email: varunchitale@gmail.com*
[b]*Email: anandita.bodas@gmail.com*

Abstract

In the modern era of technology, devices have become smaller, more user friendly and most importantly, wireless. Gadgets these days come with convenient wireless variants for the user. These wireless gadgets allow the user to access the host machine from a distance that varies depending upon the range of the radio signal. The latest innovation of wireless mouse has given the user freedom from the old technology of wired mouse. However, there is a serious threat that comes along with the facility of a wireless mouse. The data transmitted from the click on the mouse to the radio transceiver attached to the computer is not in an encrypted format, and is usually considered as data that is not confidential or important. Mouse Jacking is a set of vulnerabilities that is associated with wireless, non-Bluetooth mice and keyboards. Mouse Jacking allows the hacker or unauthorized user to access the target computer from 100 meters away by using an inexpensive USB dongle.

Keywords: Mouse Jacking; Spoofing Mouse; Spoofing Keyboard; Encryption in wireless devices; XOR.

1. Main text

Wireless keyboards and mice operate at the 2.4 GHz ISM Band which is devoted to the official standards that are set by the ISM. The ISM are a set of radio bands that are internationally reserved for the operations including radio frequency for industrial, scientific and medical purposes.

ISM does not permit the use of telecommunications on its bands. ISM does have a selected set of regulations but there are no strict guidelines to follow as such. In the case of wireless mice and keyboards, the connection is achieved using radio frequencies. The mice and keyboards are partnered with a USB Nano Receiver which enables easy wireless access. The transceiver is connected to the PC. The data sent from the keyboard and/or mouse is transferred to the computer via radio frequencies received by the transceiver.

---

* Corresponding author.

The data entered into the computer by typing is usually in an encrypted format[1]. This data can include confidential information, so it needs security from data theft. The data that is sent from the keyboard is usually encrypted using:

- 128 bit AES
- Exclusive-OR (XOR) operation, used commonly by Microsoft devices
- 64 bit TEA used commonly by Logitech variants

Until recent times, it was considered that this data does not hold any important information and therefore it does not require any encryption. However, it has now been noticed that the movement of the mouse and the click patterns can contain important information and thus needs to be secured.

1.1. Keyboard

1.1.1 Working of the keyboard

The wireless keyboard has a very simple working process. When the key is pressed from the user it is encrypted using one of the encryption methods. The series of pressed keys are synthesized into packets. These encrypted packets are then sent to the USB Nano Receiver that has a few functions allocated to it. The transceiver receives the packets of encrypted keys firstly and then starts the process for the decryption. This decryption is done using the decrypted key. After this process, the validity of the packet is checked. In this process, the transceiver checks whether these decrypted packets are still required, or whether there has been a timeout. If the packets are still in contention and are required by the host computer, the packets are forwarded to the computer. The computer receives the decrypted packets within its validity period and then sends an acknowledgement that the packets have been received.

1.1.2 Keyboard Encryption

Both, keyboards and wireless mice communicate with the associated PC with the USB Nano Receiver attached to the PC. Communication is carried out over radio frequencies. Keyboard data that is transmitted is encrypted (usually 128-bit AES) [2]. In a wireless keyboard, only the actual keystroke data is encrypted. This is known as USB Hid Code. One byte USB HID code is encrypted using a simple XOR mechanism with a single byte of random data generated during the association procedure. In cryptography, the simple XOR cipher is a type of additive cipher. It is mostly used in Windows devices. XOR function is a modulus 2 addition (or subtraction, which is identical). With this logic, a string of text can be encrypted by applying the bitwise XOR operator to every character using a given key. To decrypt the output, reapplying the XOR function with the key will remove the cipher.

The working of XOR function is as shown below:

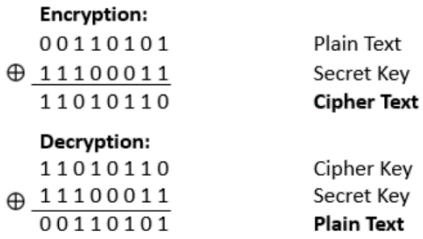

Figure1: Encryption in Keyboard

Sniffing traffic between wireless keyboards and their base stations was possible because of the weak encryption used.

1.1.3 Meta Keys

A Meta key [3] is a modifier key on certain keyboards. It is a special key on a computer keyboard that temporarily modifies the normal action of another key when pressed together. Shift, Ctrl and Alt are examples of Meta keys. By themselves, modifier keys usually do nothing; that is, pressing any of the Shift, Alt, or Ctrl keys alone does not (generally) trigger any action from the computer. The key point is that the Meta-Keys are not obfuscated or encrypted, so hackers would be able to exploit this.

1.2. Encryption in Mouse

Wireless mouse too uses Radio Frequency (RF) for communication. A standard 27 MHz band is generally used. It consists of a receiver and transmitter. Its working is as follows:

The transmitter in the mouse sends a radio signal to the USB Nano Receiver. The USB Nano Receiver encodes the information about the mouse's movements and the buttons you click. The receiver which is connected to the computer (it may be a separate device like a card that goes into a slot, or a built-in component), accepts the signal, decodes it and passes it on to the mouse driver software and computer's operating system.

The transmitter and receiver must operate on the same frequency in order to communicate and pair with each other. Some may have a common encryption key or a pass-phrase for added security.

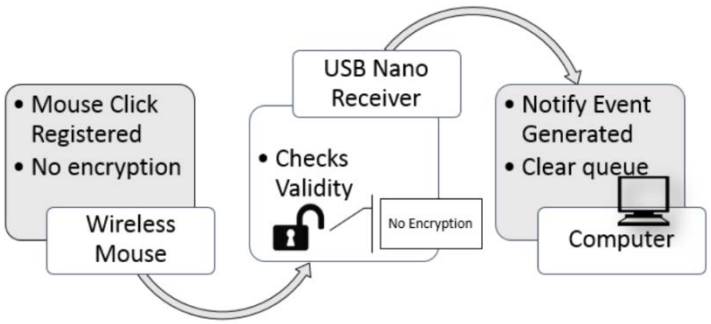

Figure2: Working of a typical electronic mouse

1.2.1 Introduction to Mouse-Jacking

Since the radio communication between mouse and USB Nano Receiver is unencrypted, it will accept any seemingly valid command. A hacker can intercept the signal within 100 m of range. The hacker can then send packets that generate keystrokes instead of mouse clicks, allowing him to carry out malicious activities. This is known as Mouse Jacking.

"Since the displacements of a mouse would not give any useful information to a hacker, the mouse reports are not encrypted." -Logitech 2009 White Paper [4].

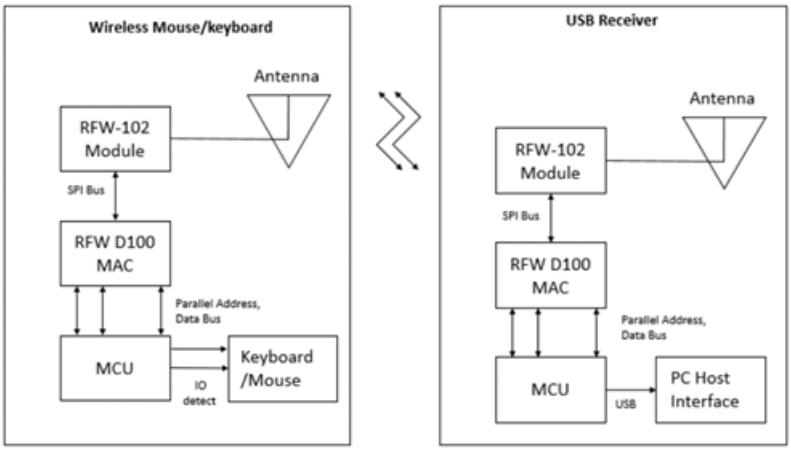

Figure3: Internal Working of an electronic wireless mouse

1.2.2 Vulnerabilities

- Keystroke Injection, spoofing a mouse:

Since communication takes place with the help of RF packets, some dongles do not verify that the type of packet received matches the type of device that transmitted it. This is done in order to reduce the time lag experienced during the verification process. A higher and faster response rate is achieved when the packets are processed without verification, but at the cost of security.

Normally, a mouse is identified by the movement or clicks that the user inputs whereas a typical keyboard, by its key-presses. If the dongle does not verify that the packet type and transmitting device type match, it is possible for an attacker to pretend to be a mouse, but transmit a key-press packet. The dongle does not expect packets coming from a mouse to be encrypted, so it accepts the key-press packet, allowing the attacker to type arbitrary commands on the victim's computer, which is fooled into accepting the commands [5].

- Keystroke Injection, Spoofing a keyboard:

Most keyboards, especially ones released after 2010 encrypt data before transmitting, in order to ensure apt security. Most of them, which are dated, follow the XOR protection mechanism, explained in section 1.1.2.

Microsoft keyboards followed a standard XOR mechanism. 128 bit AES has also been implemented in select models, typically the higher costing ones. The attacker has to pretend as a keyboard, and transmit unencrypted keyboard packets. This bypasses the encryption normally used by the keyboard, and allows an attacker to type arbitrary commands on the victim's computer, and carry out the intended malicious activities.

- Forced Pairing:

Before a typical wireless keyboard or mouse leaves the factory, it is paired with a dongle. A wireless mouse or a keyboard thus, can communicate with only the parent USB Nano Receiver. To prevent unauthorized access, the dongle will only accept new devices in pairing mode, each defined by the company manufacturing the devices. Pairing mode typically lasts for about 30-60 seconds. It is possible to bypass this pairing mode and pair a new device without any user interaction. With keystroke injection by spoofing a keyboard, an attacker can pair a fake keyboard with the dongle, and use it to type arbitrary commands on the victim's computer.

1.2.3 Tests conducted

During experimentation, researchers found that they were able to generate a word rate of about 1000 words/min transferable over an unencrypted wireless mouse connection to the affected host. This ensures installation of a malicious Rootkit, possibly within 10 seconds of interaction. Furthermore, any seasoned hacker could pry on the system and consider installing a backdoor Meterpreter Listener and thus, exploit the system completely.

1.2.4 Affected Devices

Security researchers have discovered this new vulnerability hitting multiple leading brands of wireless mice and keyboards. Listing out the manufacturers whose non-Bluetooth wireless devices are affected by the lack of encryption could be difficult. As put forth by the Bastille group working towards setting up a defense mechanism for this vulnerability, manufacturers like Logitech, Dell, HP, Lenovo, Microsoft, Gigabyte, AmazonBasics, have taken the top place.

1.2.5 Limitations and Countermeasures

In analyzing the scenario, Mouse-Jacking is feasible only if certain criteria are fulfilled. Firstly, the target should use an electronic wireless mouse. Secondly, certain companies have included encryption in the interactions with the mouse. Mouse-Jacking is not possible in such a scenario. Lastly, if the mouse input is fulfilled, this ensuring security, prevents an attack. The vulnerability, though minor is ubiquitous. Furthermore, by being aware of the typical approach used by attackers as well as their goals, you can be more effective when applying countermeasures. Firmware upgrades (like the one by Dell and Logitech) provide an efficient way to be up to date with the latest encryption patterns. Another simple, yet effective way is to lock your device when not in use. Since these wireless devices are being used in close proximity to the machine, it is advisable to reduce the range of operation. Force pre-pairing of the device at manufacturer level or the use of Bluetooth keyboards and mice, both have their benefits to fight the attacker. The most efficient way to secure one's machine is to use a wired mouse or touchpads in unsafe locations.

1.3. Conclusion

As hackers are becoming increasingly skilled in their targeting, mouse jacking could be used to steal data and files from a remote machine. Mouse jacking can have an effective range of 100 meters. The hacker can copy and delete programs at will. Mouse jacking can also cause network vulnerabilities by opening a command window in the network administrators' machine[6]. The attacker can install a root kit using the administrator privileges in barely 30 seconds to result in a complete network compromise. At that point, the attacker can enter into the network as a mouse jack attacker and gain complete access to all resources on the network. These are a few examples of the harm that Mouse jacking can cause to vulnerable computer and their networks.

Acknowledgements

The authors would like to thank the professors at MITCOE institute, Pune for their constant and insightful support.

References

[1] Godspeed Travis, "Promiscuity is the nRF24L01+'s Duty." Internet:

http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html. Feb 7, 2011 [Mar 04, 2016].

[2] William Stalling, "Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice" , 6th edition, vol. 1, Ed. New York, Pearson, 2014, 66-231.

[3] Wikipedia: The Free Encyclopedia. Wikimedia Foundation Inc., "Meta key", Internet:

https://en.wikipedia.org/wiki/Meta_key, Feb. 6, 2016 [Mar. 05, 2016]

[4] Logitech, "Logitech Advanced 2.4 GHz Technology", Internet:

http://www.logitech.com/images/pdf/roem/Logitech_Adv_24_Ghz_Whitepaper_BPG2009.pdf, Mar. 2, 2009 [Mar. 3, 2016]

[5] Andy Greenberg. "Flaws in Wireless Mice and Keyboards Let Hackers Type on Your PC." Internet:

https://www.wired.com/2016/02/flaws-in-wireless-mice-and-keyboards-let-hackers-type-on-your-pc/, Feb. 23, 2016 [Mar. 03, 2016]

[6] Newlin, Marc, "Hacking Wireless Mice with an NES Controller", ToorCon 17, San Diego, CA, Oct 24, 2015, [Mar 05, 2016].