The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022

Volume 21, Pages 241-247

IConTES 2022: International Conference on Technology, Engineering and Science

Threat and Vulnerability Modelling of Malicious Human Interface Devices

Mathew NICHO
Rabdan Academy

Ibrahim SABRY
Zayed University

Abstract: The threats posed by malicious Human Interface Devices (HID) have greater potential for harm owing to the inherent trust given to them by the respective Operating Systems (OS). While HIDs vary in terms of hardware and software, the OS detects them as genuine, providing access to the malicious HID to perform and execute privileged actions as if it came from a genuine user. Since the threat can bypass normal security controls, it poses a significant challenge to security managers. While the insider (both unintentional and malicious) threat level posed by the malicious HIDs is high, research in the domain of mapping HIDs to HID attack vectors and the exploited vulnerabilities is scarce, which is evident from the paucity of research outputs in a Google Scholar search. Accordingly, the objective of this research is to create a model that maps HIDs to vulnerability categories aligned to attacks. In this connection, the paper proposes an HID Threat Vulnerability model (HidTV) that identifies the malicious HID types and evaluates the nature of HID related threats and the corresponding vulnerabilities that are exploited. The resulting model can provide security managers with a visibility of critical vulnerabilities, map specific HIDs to threats and vulnerabilities and formulate security policies to defend and mitigate against these threats. From an academic perspective, the paper provides a foundation for researchers to evaluate and propose detective and mitigation strategies for specific attack paths. While there are genuine uses for HIDs, this paper focuses on the ways they can be intentionally exploited for malicious purposes.

Keywords: Human interface device (HID), Malicious HID, HID threats, HID vulnerabilities.

Introduction

The flexibility of the USB protocol and the inherent trust given by Windows, Mac and Linux operating systems to Human Interface Devices (HIDs), mainly keyboards and mice, can be maliciously leveraged to create multiple threat vectors that can directly perform malicious activities on a system as though it were performed by a logged-in user (OPSWAT, 2014). Similarly, wired HIDs as well as Bluetooth enabled devices could stealthily switch from a legitimate profile to the HID profile, emulating the behaviour of a Bluetooth keyboard and a Bluetooth mouse by injecting keystrokes, mouse movements and click events (Xu et al.,2019).

The malicious nature of HIDs can be attributed to the development of a technology based on the Universal Serial Bus (USB) HID protocol that attacks computer systems (Zhao & Wang, 2019). Since the USB-based attacks often abuse the trust-by-default nature of the ecosystem and transcend different layers within a software stack, none of the existing defences provide a complete solution (Tian et al., 2018). Of the global population of 7.11 billion, 5.07 are connected to the Internet, representing 63.5% of the population as of October 2022 (Datareportal, 2022). From a Windows Operating Systems (OS) perspective, there are 1.4 billion active devices running Windows 10 or Windows 11 monthly (Microsoft Inc, 2022), thus presenting an enormous opportunity for hackers to penetrate computer systems and smartphones using malicious HIDs.

HID, is a form of computer device used by humans to take in input and generate the required output. The primary function of an HID is to act as an electronic information system involved in the activities of data input and data output. HIDs use the USB protocol that has a default polling rate of 125 Hz with high responsiveness and lower latency, thus giving an edge for manipulation. Forming the larger part of the hardware and peripheral system of a computer setup, HIDs include headsets, USBs, webcams, speakers and mice (Karystinos et al., 2019). The fact that HIDs have the ability to provide a relational interface between computer systems and users makes them vulnerable to attack exploitation. This occurs because these devices are commonly used to access sensitive operations that require high authorisation (ibid). Thus, cyber hackers have been able to integrate malicious and anomalous HIDs whose main function is to imitate how users control their computer systems. Malicious HIDs have presented considerable challenges in the field of information security, as multiple ranges of systems have been able to neglect the security risks they pose.

Attacks using HIDs are not easily performed by external entities due to the lack of physical access to organisational networked assets, but they can be deployed as insider threat vectors (malicious), or a hacker can leverage an unsuspecting user to connect the HID to the system. In this respect, USB devices have been leveraged as a delivery mechanism for host-side exploits, where the attackers target the USB stack by embedding malicious code in device firmware to covertly request additional USB interfaces, providing unacknowledged and malicious functionality that lies outside the apparent purpose of the device (D. J. Tian, Bates, & Butler, 2015). Functionality also plays a role where the success and widespread use of the USB protocol that connects keyboards, mouse devices, printers, webcams and several other computer peripherals can be attributed to the bus characteristics, such as simplicity, ‘plug & play’ features, ‘hot plug’ support and, particularly, the possibility of supplying power to the devices (Depari et al., 2008). In this respect, current detection and prevention solutions related to HID largely tend to concentrate on specific attacks or fail to provide a comprehensive and effective solution (Nissim et al., 2017).

Academic research on the threats, vulnerabilities and attacks specifically attributed to HIDs is scarce, as is evident from the search results on Google Scholar (since 2005). Using the phrases (without quotes) ‘Human Interface Device attacks’, ‘HID attacks’, ‘HID vulnerabilities’ and ‘Human Interface Device vulnerabilities’ presented 13, 3, 2 and 6 outputs, respectively (October 2022). Hence, while multiple studies have focused on USB hardware attacks and vulnerabilities, comprehensive research on aligning the HIDs with the associated vulnerabilities that can be exploited to execute the attack is lacking in both the academic and professional fora. Accordingly, the objective of this research is to create a model that maps HIDs to vulnerability categories aligned to attacks.

Review of Malicious HIDs

Malicious HIDs are categorised into three types in relation to their primal technique. They are wireless communication malicious HIDs, HID interface composite devices and pure HIDs. Wireless communication malicious HIDs work under the functionality that the corrupted HIDs operate through wireless communication signals (Zhao & Wang, 2019). Normally, the wireless signals are transmitted through a short-range radio using medium waves. Some of the wireless communications include Wi-Fi and Bluetooth communication. The devices that will use the wireless communication include Bluetooth and Wi-Fi mice and Bluetooth and Wi-Fi keyboards. On the other hand, composite interface malicious HIDs are devices that have been partially corrupted. In essence, they refer to original HIDs that are corrupted with manipulative files, such as malicious payloads. Finally, pure HIDs are common everyday devices that are used to interact with systems, such as mice, keyboards and audio headsets (Zhao & Wang, 2019).

Leveraging Malicious HIDs

Maliciously crafted HIDs include the Programmable HID USB Keystroke Dongle (PHUKD), USB ninja, Wi-Fi HID injector (WHID), the rubber ducky, the BadUSB and the skimmers. The PHUKD, a small hardware device that uses the Teensy microcontroller development board, allows the device to mimic keystrokes and mouse macros, thus bypassing security controls. The device can execute itself when the device is plugged into the target system or can be programmed to execute after a set time or when certain environmental conditions are met. Since the PHUKD acts like mice and keyboards, it does not require administrative privileges to be installed and function, thereby enabling the hacker to leverage it for malicious activities (Crenshaw, 2011). However, the USB ninja, a penetration and information security tool that is used for vulnerability analysis and penetration testing (VAPT), can also be leveraged for malicious methods. It works like a regular USB cable for the pairing

functions of data and power but alters its normal functionality whenever the choice of an attack payload is triggered by a wireless remote controller to the victim's computer system (Pescatore, 2019). The attack pattern involved with the deployment of the USB ninja is triggered by a concealed Bluetooth device within the cable. Whenever the device receives the command, the cable transitions from a normal USB cable to a malicious attacker by emulating a USB mouse or keyboard. The payload with the use of USB ninja devices is customisable, where Arduino IDEs can be employed in payload creation (ibid). The need for affordable and dedicated hardware gave rise to the WHID, after which it could be remotely controlled to perform its primal attacks as a malicious HID attacker. The core of the device constitutes an ESP-12s that is capable of offering Wi-Fi access (Hong, Kim, & Kim, 2019). The attack pattern involved with the deployment of the WHID is based on the creation of new payloads that could be stored locally on mobile devices, thus eliminating the need for memory injection through uploading onto the WHID. In addition, this technique of storing the payload locally makes it more strategic for the attacker, as it becomes harder for forensic analysis to trace the attack (Golushko & Zhukov, 2020).

The rubber ducky is an HID that physically imitates a USB flash drive. When plugged into a computer's serial interface, the computer configures it as a USB keyboard and accepts the input of electronic signals as keystroke commands as with the functions of a normal keyboard (Arora et al., 2021). The rubber ducky has been used by attackers in cyber adversary activities, such as webserver attacks and user login credential harvesting. The method of attack a rubber ducky uses is to incorporate keystroke technology through various injection methods so that anomalous and malicious code is executed seamlessly and rapidly on a device (Arora et al., 2021). The rubber ducky uses the ducky script as its default programming language for the execution of its payload, which is usually stored on the SD card. The BadUSB exploit that was first demonstrated at the 2014 Black Hat conference (Nohl et al., 2014) exploits USB firmware vulnerability by re-programming the USB device to imitate an HID. BadUSBs are a cyber-security threat that involves the use of malicious USB devices that are corrupted with an anomalous software. The attacker re-programs the microprocessor (Ex. Intel 8051 microcontroller) and alters its main function of a data storage device to a malicious manipulative tool (Zhao & Wang, 2019). Using Internet of Things (IoT) devices such as Raspberry Pi Pico and Intel 8051, the micro controller's logic circuit programming is altered, and the primal functioning as a simple IoT device is transformed to be used in cyber-attacks. Furthermore, HID methodology is also used for card skimming, a process where the data and information found in magnetic stripes on debit or credit cards are copied and duplicated using skimmer devices (Scaife et al., 2018). The method of attack of skimmer devices is to duplicate the data and information stored in the magnetic stripe at the Point of Sales (POS) terminals. In this respect, Proxmark3 (PM3) is a standard RFID diagnostic, testing and programming tool that allows users to read, emulate, fuzz and brute force the majority of RFID protocols. The PM3 has a USB interface to the computer where it uses the default HID USB protocol (Lorenzo et al.,2019). Skimming has allowed attackers to acquire sensitive digital information of card users, especially related to their bank and financial credentials.

Vulnerabilities Exploited by HIDs

Attacks by malicious HIDs have created various weaknesses on systems, such as on operating systems and software applications, where the attacker can find weaknesses that can be exploited to satisfy their cyber needs, such as data collection. The use of malicious HIDs has exposed the field of security, where gaps in a network system such as an OS are uncovered (Zhao & Wang, 2019). Critical vulnerabilities that can be exploited include poor encryption, data misplacement, system misconfiguration, unpatched and outdated software and weak authorisation credentials. Since HIDs are not inherently malicious devices, most USB device firmware is not typically scanned by computer systems. In addition, most common antivirus software is not able to detect or defend against these types of attacks. As such, we can infer that HIDs are more susceptible to manipulation because they gain easier access to the host machine. Once connected, they can pose as a peripheral, such as a mouse or keyboard, or even simply perform the action of injecting the malicious payload or of executing a code on the host machine that would further weaken the system.

The use of malicious HIDs has revealed the existence of poor data encryption within computers, which allows attackers to intercept the communications flowing within the computers operating system. For example, using a computer for tele-communication purposes on application software systems may lead to information security breaches. This happens if end-to-end encryption is not correctly configured. Hence, when a malicious HID is plugged in (e.g. a rubber ducky), it will tap into the duplex communication pathway and steal sensitive information (Acar et al., 2019). This vulnerability is portrayed by system assets such as operating systems where their internal settings may be at risk. In addition, the application or operating system settings may differ in terms of security. For example, skimmers are deployed by cybercriminals on account of the vulnerability of system

misconfigurations. This happens because the magnetic stripes on the ATM cards have not been equipped with enough security configurations that will enable them to evade the threat of credit card skimming (Scaife et al., 2018). Operating systems that are not updated regularly are highly vulnerable to the use of malicious HIDs. This is because the unpatched software is out of date and thus security configurations within the system application software will not be supported by the Vendor OS. As such, cybercriminals tend to track users with unpatched or outdated system software, as it will be easy to compromise, access and retrieve sensitive information and data (Zhao & Wang, 2019). Cybercriminals can also brute force themselves into a network, bypassing firewalls by guessing passwords and user credentials. The fact that credentials are weak and can be guessed provides a seamless entry to penetrate organisational systems. Figure 1 summarises the vulnerabilities and associated attack vectors.

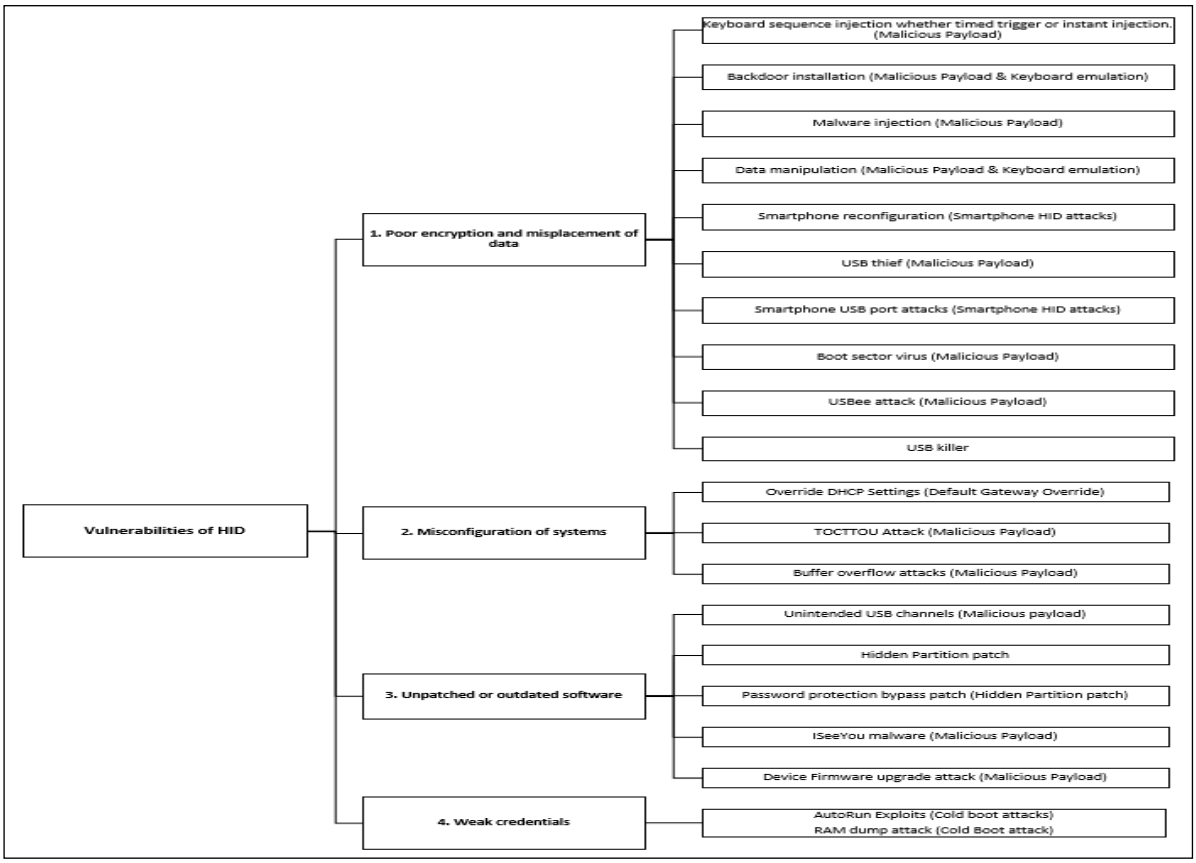

Figure 1. A classification of HID attacks attributed to system vulnerabilities

Threats from Malicious HIDs

Threats from malicious HIDs include system infections, keyboard emulations, smartphone-based attacks, cold boot attacks, default gateway overrides and hidden partition patches. Malicious HIDs have been able to spread malicious payloads into computer systems and software. Examples of such malicious HIDs are BadUSBs and rubber ducky USBs. The payload is stored as a program within the logic memory of the drives and gets injected into the computer once the drives are plugged in. Thereafter, malicious commands are sent to the computer, leading to the spread of different payloads, such as viruses, worms or Trojans (Nissim et al., 2017). Keyboard emulation is a form of attack executed through the use of a rubber ducky, where keystroke injections are spoofed and imitated using a normal USB device. In smartphone-based HID attacks, the smartphone can be used as a rubber ducky against Android or Windows, where the attacker's smartphone serves as a connected keyboard (Wang & Stavrou, 2010). For this form of attack, Android drivers that interact with Android related devices are overwritten and their interaction with Android devices is altered. The drivers are configured to interact with devices such as keyboards and mice, so that they can be used as gateways for cyber adversary practices (Nissim et al., 2017; Bojovic et al., 2019). In the cold boot attack, also known as the RAM dump attack, a USB drive plugged into a computer is used to retrieve dynamic data from secondary memory. This is achieved by incorporating a memory dumper that extracts data that has been left over from secondary memory. This mostly happens when booting is done through a USB device (Anderson & Anderson, 2010). The Default

Gateway Override attack is performed through programmable logic circuits or microcontrollers, which are programmed to act as a USB flash drive that will be identified by the computer as a normal USB. Once the USB is plugged into the USB port, the microcontroller emulates a USB Ethernet adapter, which hijacks local traffic by overriding DHCP configuration (Rodríguez Ocasio, 2019). However, in the hidden partition patch attack, the objective is to determine how a covert and concealed storage partition located within a USB could be achieved through reprogramming. This covert partition allows the USB to store ex-filtered data from the connected computer (Anderson & Anderson, 2010). Table 1 links the multiple HID attack vectors with the corresponding HIDs used to carry out the attacks. Numerical values are assigned to each malicious HID below.

USB ninja **–** USB cable with Bluetooth capability that can receive transmissions from other Bluetooth enabled devices in order to implement malicious payloads or scripts.

1. *Wi-Fi HID WHID injector* **–** wireless peripheral that can be reprogrammed to deliver malicious payloads wirelessly.
2. *Rubber ducky* **–** USB enabled HID that can imitate a peripheral such as keyboard or mouse in order to take control of the host machine.
3. *BadUSB* **–** reprogrammed microcontroller that can deliver malicious payloads or run malicious scripts.
4. *Skimmers* **–** devices used to mimic the appearance of HIDs and are used to scan magnetic strips in order to extract the information stored on them.

Table 1. Mapping HID attack vectors with the HIDs

Attacks	HIDs	Reference
Malicious payload	1,2,3,4	(Nissim et al., 2017; Zhao & Wang, 2019)
Keyboard emulation	3,5	(Nissim et al., 2017; Bojovic et al., 2019))
Smartphone-based HID attacks	1,2	(Wang & Stavrou, 2010; Potocky & Štulrajter, 2022)
Cold boot attacks	1,4	(Anderson & Anderson, 2010; Pham et al., 2011)
Default gateway override	3,4	(Nissim et al., 2017)
Hidden partition patch	1,4	(Anderson & Anderson, 2010; Pham et al., 2011)

The HID Threat and Vulnerability Model (HidTV)

This section discusses the HidTV model (Figure 1) that aligns the three constructs – the malicious HIDs, the corresponding multiple exploitable vulnerabilities and the attacks that are targeted at the systems based on the exploitable vulnerabilities – in an effort to demonstrate the link between them. We performed a comprehensive study of five HIDs that can be leveraged to perform malicious actions, followed by four major vulnerability categories leading to six major attacks (figure xx). In this respect, a combination of these three constructs leads to 55 different attack vectors. For instance, the USB ninja HID can be leveraged to exploit three vulnerabilities, namely poor encryption, misconfiguration and malicious payload execution, leading to 10 attack vectors.

The WHID injection can be used as a potent tool to exploit three vulnerability categories, leading to 13 attack vectors. Similarly, the rubber ducky can be deployed to target three vulnerability categories, resulting in 13 attack vectors. Not far behind is the BadUSB that exploits three vulnerability categories that can initiate 11 attack vectors. However, due to its lightweight feature, the skimmer exploits just two vulnerability categories, leading to eight attack vectors. Altogether, the 55 attack vectors highlight the potential of a hacker who can leverage HIDs to bypass security controls and perform malicious operations.

An HID is a very usable and common tool endorsed by organisations and adopted by the internetworked user to interface with the computer systems. With billions of HIDs being used by internetworked users for input and output processes, they provide a seamless avenue of opportunity for hackers to leverage them as a tool for bypassing IT controls to perform and execute malicious actions. At the same time, they present a formidable challenge for IT security managers to detect, prevent and mitigate threats and attacks owing to the inherent accessibility provided by the respective operating systems, which allow the HIDs to interface with the system. As such, mapping the HID vulnerabilities and HID-leveraged attacks to specific HIDs provides valuable information for IT security administrators/managers who deal with security concerns and HID manufacturers. The model thus provides not only a detailed map and attack vector path for the HID but also illustrates the impact of these attacks on the system.

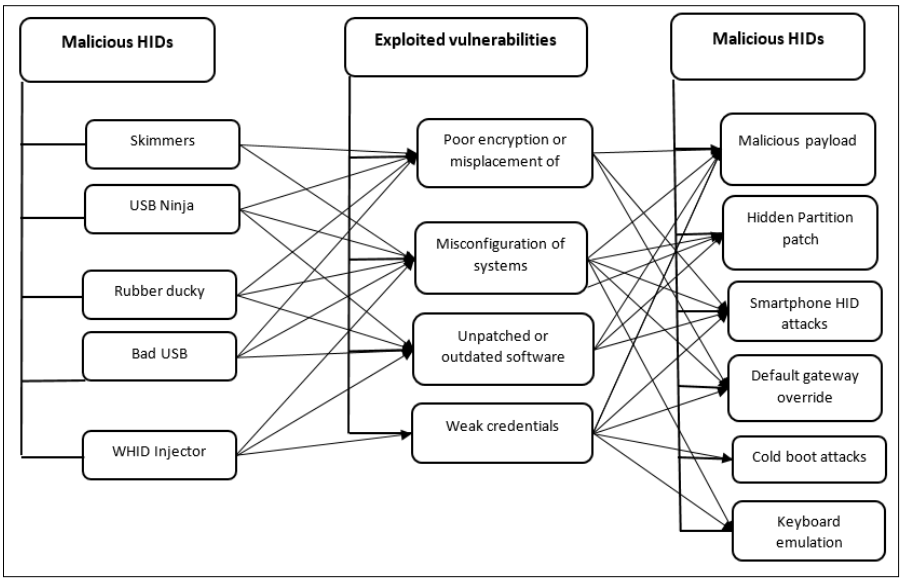

Figure 2. The HID threat and vulnerability model

Conclusion

In this paper, we conducted an extensive study on how HIDs can be leveraged to perform malicious activities, the vulnerabilities that are exploited by malicious HIDs and the attacks that can be performed. In this regard, we listed 55 attack vectors attributable to malicious HIDs. Furthermore, we aligned the HIDs to the respective system vulnerabilities that can be exploited and the corresponding attacks that can be performed. Despite their high threat potency and successful penetration of systems, malicious HIDs and their deployment are a scantily researched topic. As such, the model provides IT security managers and device manufacturers with detailed guidelines on specific areas of concern, including device misuse, the specific vulnerabilities associated with each misuse and the attacks that can be performed through the exploit. The main limitation of this research is the evolving and potential overlapping of HID categories, vulnerabilities and attacks owing to the dynamic nature of cyber-threats. One or more vulnerabilities can overlap, leading to a novel vulnerability that can be exploited that is not in this research domain. Furthermore, due to the evolving nature of HIDs, it was not feasible to incorporate the entire scope of HIDs that are available and globally used in specific industry sectors. However, future researchers could expand this model by adding and categorising HIDs from different sectors as well as adding countermeasures to the model. This would not only add considerable value to the model but also provide valuable control measures for IT managers and HID manufacturing sectors, including the IT security industry, enabling them to devise feasible solutions for countering this threat from a device perspective.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Technology, Engineering and Science (www.icontes.net) held in Antalya/Turkey on November 16-19, 2022.

References

Acar, A., Lu, L., Uluagac, A. S., & Kirda, E. (2019). An analysis of malware trends in enterprise networks. *International Conference on Information Security*, 360-380.

Anderson, B., & Anderson, B. (2010). *Seven deadliest USB attacks* (1th ed.).Oxford, UK:Syngress

Arora, L., Thakur, N., & Yadav, S. K. (2021). USB rubber ducky detection by using heuristic rules. 2*021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS).*

Bojovic, P. D., Basicevic, I., Pilipovic, M., Bojovic, Z., & Bojovic, M. (2019). The rising threat of hardware attacks: USB keyboard attack case study. *7 th International Conference on Electrical, Electronic and Computing Engineering.*

Crenshaw, A. (2011). Plug and prey: Malicious USB devices. Proceedings from *ShmooCon Security Conference.*

Datareportal. (2022). *Digital around the world*. Retrieved from https://datareportal.com/global-digital-overview

Depari, A., Flammini, A., Marioli, D., & Taroni, A. (2008). USB sensor network for industrial applications. *IEEE Transactions on Instrumentation and Measurement, 57*(7), 1344-1349.

Figueroa Lorenzo, S., Añorga Benito, J., García Cardarelli, P., Alberdi Garaia, J., & Arrizabalaga Juaristi, S. (2019). A comprehensive review of RFID and bluetooth security: Practical analysis. *Technologies, 7*(1), 15.

Golushko, A. P., & Zhukov, V. G. (2020). Application of advanced persistent threat actors techniques aor evaluating defensive countermeasures. *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*,312-317.

Hong, S., Kim, K., & Kim, T. (2019). The design and implementation of simulated threat generator based on MITRE ATT&CK for cyber warfare training. *Journal of the Korea Institute of Military Science and Technology, 22*(6), 797-805.

Karystinos, E., Andreatos, A., & Douligeris, C. (2019). *S*pyduino: Arduino as a HID exploiting the BadUSB vulnerability. *15th International Conference on Distributed Computing in Sensor Systems (DCOSS 2019).*

Microsoft Inc. (2022). *Windows 10 - Microsoft by the numbers*. Retrieved from https://news.microsoft.com/bythenumbers/en/windowsdevices

Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks. *Computers & Security, 70*, 675-688.

Nohl, K., Krißler, S., & Lell, J. (2014). On accessories that turn evil. *Black Hat USA, 1*(9), 1-22.

OPSWAT. (2014, August 26). *Detecting and mitigating USB-based threats.* Retrieved from https://www.opswat.com/blog/detecting-and-mitigating-usb-based-threats

Pescatore, J. (2019). *Sans top new attacks and threat report*. SANS Institute.

Pham, D. V., Syed, A., & Halgamuge, M. N. (2011). Universal serial bus based software attacks and protection solutions. *Digital Investigation, 7*(3-4), 172-184.

Potocky, S., & Štulrajter, J. (2022). The human interface device (HID) attack on Andorid lock screen non-biometric protections and its computational complexity. *Science & Military Journal, 17*(1), 29-36.

Rodríguez Ocasio, A. (2019). *Implementing USB attacks with microcontrollers.* (MSc). Retrieved from http://hdl.handle.net/20.500.12475/140

Scaife, N., Peeters, C., & Traynor, P. (2018). Fear the reaper: Characterization and fast detection of card skimmers. Proceedings from : *The 27th USENIX Security Symposium (USENIX Security 18).*

Tian, D. J., Bates, A., & Butler, K. (2015). Defending against malicious USB firmware with GoodUSB. Proceedings from : *The 31st Annual Computer Security Applications Conference*, 261-270.

Tian, J., Scaife, N., Kumar, D., Bailey, M., Bates, A., & Butler, K. (2018). SoK:Plug & pray today–understanding USB insecurity in versions 1 through C. 2*018 IEEE Symposium on Security and Privacy, SP*,1032-1047.

Wang, Z., & Stavrou, A. (2010). Exploiting smart-phone usb connectivity for fun and profit. Proceedings from: *The 26th Annual Computer Security Applications Conference*, 357-366.

Xu, F., Diao, W., Li, Z., Chen, J., & Zhang, K. (2019). *BadBluetooth: Breaking android security mechanisms via malicious Bluetooth peripherals.* In NDSS.

Zhao, S., & Wang, X. A. (2019). A survey of malicious HID devices. *International Conference on Broadband and Wireless Computing, Communication and Applications.*

Author Information

Mathew Nicho
Rabdan Academy
Abu Dhabi, United Arab Emirates
Contact e-mail: *Mathew. Nicho@zu.ac.ae*

Ibrahim Sabry
Zayed University
Dubai, United Arab Emirates

To cite this article:

Nicho, M., & Sabry, I. (2022). Threat and vulnerability modelling of malicious human interface devices. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 21*, 241-247.