Killing Your Device via Your USB Port

Olga Angelopoulou[1], Seyedali Pourmoafi[1], Andrew Jones[2], Gaurav Sharma[1]

[1] Cyber Security Centre, University of Hertfordshire, United Kingdom
[2] Cyber Security Centre, University of Hertfordshire, United Kingdom, Edith Cowan University, Australia
{o.angelopoulou, s.pourmoafi, a.jones26, g.sharma5@herts.ac.uk}

Abstract

The USB killer is a testing device that has been marketed as having been designed to test the limits of the surge protection circuitry of electronics. The device can 'fry' an electronic device in a fraction of a second. The aim of this research is to identify to what extent the data that is stored on the device can be destroyed when utilising the USB Killer 2.0 since it could potentially become the weapon of a malicious user with access to a device with an active USB port. The authors conducted a series of experiments utilising the USB killer in different hardware configurations. The paper introduces the USB protocol and discusses the functionality of the USB killer before outlining the experiment and presenting the results of the study.

Keywords

USB killer, USB based attacks, USB ports, data loss, social engineering

1. Introduction

The USB Killer is a USB thumb drive that allegedly destroys the physical component of any hardware device that it is connected to it via an active USB port. The device is exploiting the USB surge vulnerability (USB Kill, 2019; Dark Purple 2015) on devices with a USB port and has been mainly designed and manufactured to test hardware components for protection from power surges and electrostatic discharge.

According to recent studies, USB port related attacks are being utilised by attackers over the years (Nissim et al, 2017; Clark et al., 2011; Pham et al., 2011; Neuner at al., 2018). Attackers often take advantage of the popularity of USB thumb drives to perform unauthorized access to data. The USB killer though holds unique characteristics as it can destroy a standalone device if there is direct access to that host whether it is a computer or a mobile phone. The device has received extensive press coverage since there are no similar commercial devices available (Anthony, 2016; Whitaker, 2017; Murgia, 2015). There is a focus on the fact that the USB killer can destroy not only computers, but any device with an active USB port from printers and photo kiosks to cars.

In principle the USB killer charges its capacitor from the USB port and then discharges high voltage until it reaches ~ -240V. This is achieved in a fraction of a second resulting to a non-functional system. The manufacturers claim that, based on their testing, only Apple devices are hardware protected against a USB power-surge attack (USB Kill, 2016) and they extensively discuss their approach towards publicly disclosing the vulnerability and commercialising the USB killer as a product.

The aim of this study is to identify the extent to which data can be destroyed when the USB Killer is used on machines with different configurations. The current version of USB Killer is 3.0. However, when the experiments were conducted for this research USB Killer 2.0 was the latest version of the device.

The manufacturers claim that:

> *"when tested on computers, the device is not designed or intended to erase data. However, depending on the hardware configuration (SSD vs Platter HDD), the drive controllers may be damaged to the point that data retrieval is impractical."* (USB Kill, 2017)

The device is designed to be used as a testing device. However, as a method of attack on a hardware platform it could be used as a weapon in the hands of a malicious user aiming to take advantage of their physical access to a system. The concept of this research was that the USB killer could be utilised as an anti-forensics tool. A malicious user could permanently destroy a hard disk drive that contains potential evidence by surging excess electrical power to the system with malicious intent.

Therefore, a testbed of computer systems with different configurations was prepared in order to run experiments on different devices that contain data storage media aiming to identify whether any damage was caused to the media that resulted in the data being destroyed or made unavailable. The experiments that were designed for this preliminary study were based on the official statement that the USB killer may potentially damage a hard disk drive.

It appears the popularity of USB mass-storage devices is constantly increasing since they are portable and affordable both for legitimate and malicious users. The USB killer is another USB device that made its way to the open market and appears that it could play a role in the cyber security scene since the damage it can cause is currently unclear and it can pose as a risk both for physical and hardware security.

This paper reviews USB related attacks and the role of the USB killer, then briefly discusses the USB protocol and presents the functionality of the USB killer. The design of the experiments and the results of the study are presented. The paper concludes by presenting how this study is planned to be expanded on additional electronic devices in the foreseeable future.

2. USB related attacks and the USB killer

Technological evolution motivated 'illegal' actions and transactions to be transferred from the physical and tangible domain to the digital and computerised world. The long list of cyber dependent attacks (Tetmeyer and Saiedian, 2010) is constantly expanding, including more and more sophisticated methods of compromise. Mohay et al. (2003) predicted several years ago that "*computers will probably be involved in crimes that no one has ever imagined*". Indeed, we constantly experience crimes we had never previously imagined taking place in the cyberworld; attacks against critical infrastructure, data breaches, and malware are only a few examples.

A list of software or hardware vulnerabilities could be quite extensive, accompanied by a similarly extensive list of attacks that either take advantage of the intense 'investment' on online sources or were strictly born by the technological evolution. The Universal Serial Bus (USB) was introduced to the general public in the middle of the 1990s and it immediately gained popularity due to its versatility, while the first USB thumb drive was introduced in the beginning of 2000. Nowadays the USB port is considered as the most popular port since multiple types of peripheral devices connect via the USB for data transfer.

However, the USB port and to some extent USB mass-storage devices have been widely utilised by attackers with malicious intentions. The USB thumb drives can easily get lost or even intentionally carry stolen sensitive or malicious files from insiders or malicious actors. As a result, they have been considered a significant source for data leakage and this is a downside of their major advantage of portability.

Tischer et al. (2016) conducted one of the most recent social engineering experiments, aiming to identify whether users will still collect and plug in to their computers USB thumb drives they may find. They presented interesting results since 98% of the devices were collected from their drop locations, while 45% of the participants opened at least one file on the USB thumb drive. Multiple risks can be related with such a social engineering attack with malware distribution coming up first on the list. A similar type of social engineering scenario where USB killers are dropped randomly in high pedestrian traffic locations with the intention to randomly destroy devices and causing denial of service should not be ignored.

The world has seen various forms of USB based attacks; Pham et al. (2011) divide them in software attacks on host computers and software attacks on USB devices. Most of the attack types involve a malicious payload. However, over the years accessory devices such as Rubber Ducky and BadUSB (Neuner et al, 2018) have come to the market and have seen extensive popularity, primarily supporting the argument that they are being developed for testing purposes.

Data exfiltration is one of the most common attacks related to USB devices as they work in two directions (Nissim et al, 2017). They compromise the host in such a way that that they can steal information from connected USB storage devices and leak sensitive information through a malicious USB storage device. Another type of attack involves the USB Ethernet adapter that acts as a DHCP server. Additionally, attackers may use USB thumb drives to upload a payload to other systems and manipulate system settings (Nissim et al, 2017).

Nissim et al (2017) present a historical list of USBs based attacks since 2010. The USB killer is listed as the most recent type of attack and the only one that is solely composed from electrical hardware components. The current version of the USB killer discharges capacitors straight into the data lines of the USB port. As a result, there should be no traceable evidence on the device to indicate that damage was caused by a USB killer. However, the physical damage that is caused from the USB killer could be enough forensic evidence to indicate the use of the USB thumb drive with the intentional result of an inoperable system and possible data destruction. It is still unclear though to what extent the use of the USB killer is distinct and that other sources that could result to an inoperable system can be excluded.

The human factor plays a key role in the exploitation of USB based attacks on unprotected devices. A very recent case involves the conviction of a graduate from the College of St. Rose in Albany, New York who pleaded guilty for intentionally destroying over 57 computer systems on campus by plugging in the USB killer (Bradbury, 2019). It is particularly difficult to predict what type of a USB device might be connected to an exposed USB port. It is also very difficult to predict the intention of an individuals with physical access to a device with an exposed USB port.

Some organisations consider preventative measures in their information security policies and disable the auto run functionality of USB thumb drives or completely disable USB ports to prevent users plugging in random USB devices. Others are equipped with USB port blocks and lockers to prevent data leakage, data theft and unauthorised uploads to devices, a method that works equally well for the USB killer.

3. The USB Protocol

The Universal Serial Bus (USB) is an interface that allows communication between devices. The protocol is made up by several interconnected layers of protocols (see Figure 1). Unlike other serial devices though the format of the data is not defined [30]. There are different transfer rates on USB devices that vary depending on the standard of the device and the generation it belongs to. Table 1 compares the four USB generations and outlines their speed in terms of transfer rates.

The transactions of USB data are split up into the following main actions:

1. Token Packet - Header defining what is expected to follow
2. Optional Data Packet - Containing a payload

3. Status Packet(s) - For acknowledge transaction

Version	Speed	Bit/Sec
USB 1.1	High Speed (HS)	1.5 Mbps
	Full Speed (FS)	12 Mbps
USB 2.0	High Speed (HS)	480 Mbps
USB 3.0	Supper Speed	5 Gbps
USB 3.1	Super Speed Plus	10 Gbps

Table 1. Comparison of four USB generations

The USB connection has four different types of data transfer: 1. Control 2. Isochronous 3. Bulk 4. Transfer.
The Control will establish the control exchange configuration, set-up and command information between the device and the host. The host can also send command or query parameters with control packet (Axelson, 2019).
The Isochronous transfer use by time critical streaming devices such as video-camera and speakers. The Isochronous is time sensitive so despite its limitation it can guarantee the access to the USB bus as well as data stream between the device and the host in real time so there won't be any error crushing.
The bulk type transfer is mainly used for printers or scanners since this type of devices tend to receive more data compared to any other devices connected through USB hubs and the time delivery is not crucial.
The transfer type is used by peripherals sharing a small amount of data that needs immediate attention. It is used by devices to use servicing from the PC hosts. Therefore, devices like mouse, keyboard and USB thumb drives belong to this category.
The USB thumb drives are extremely versatile since they are treated by a system as mass storage devices and require no additional drivers to function. The popularity of the USB thumb drives is related to their portability, ease of use, size, capacity and durability.

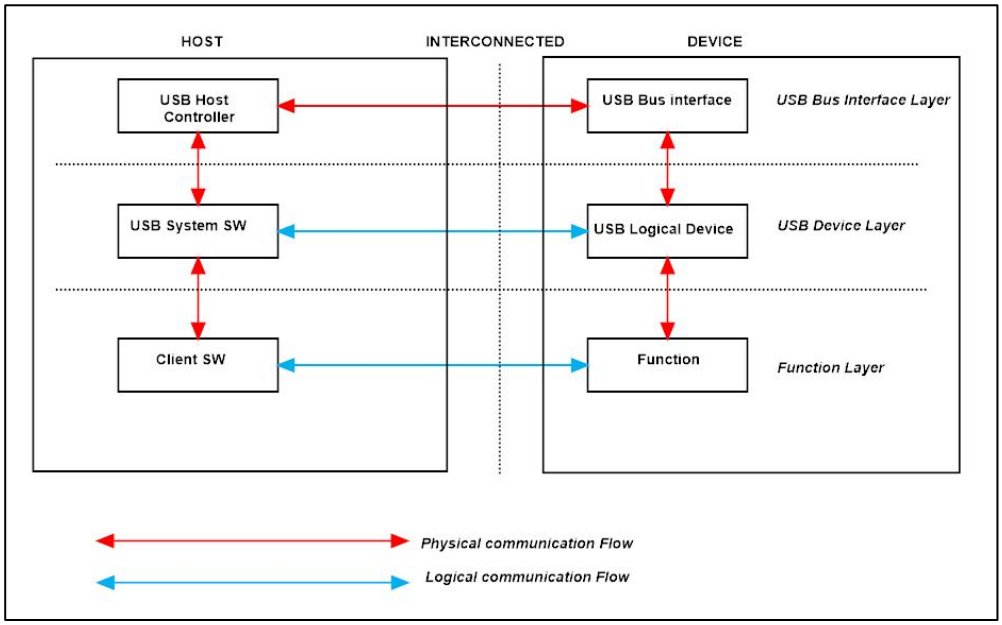

Figure 1: USB Layers (adopted by Murphy, 2017)

The USB killer is a thumb drive and belongs to the transfer type of device, while it discharges high voltage through the USB port. One of the main issues which still has not been addressed with the USB peripheral device, is that the USB protocol does not dictate any device authentication. That leaves any system vulnerable as the USB hubs blindly trust any information announced by its connected device (Anderson and Anderson, 2010). Figure 2 visualises the normal principle of any USB device connected to the system and how the end point would interact with the system. In this instance, the device accepts the connected USB device as any transfer type device. This also applies to the USB killer. In this case the user would expect the system to automatically load the content of the connected USB device. However, when enough information about the device is not obtained it could lead to an attack vector, such as the USB killer (Anderson and Anderson, 2010; Wang and Stavrou, 2010).

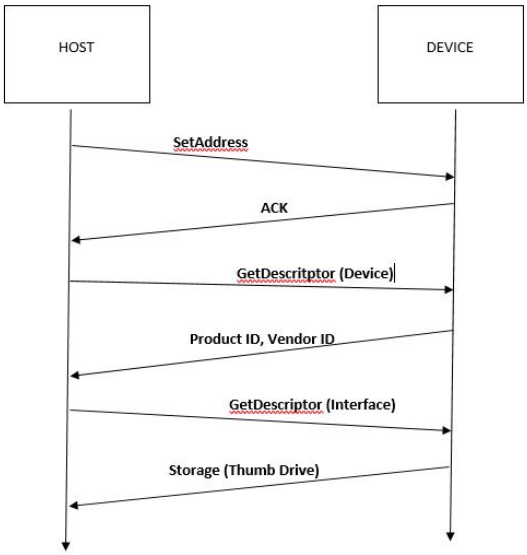

Figure 2: The USB protocol device communication (adopted by Wang and Stavrou, 2010)

4. Experiment design

For the experiment results to be reliable, several hardware configurations were used for the execution of testing the functionality of the USB killer.

The hardware architecture and the design of the motherboard was studied in the initialisation of this research and it was found that there are differences between those used in laptops and desktop computers when it comes to designing the hardware components (Nohl et al, 2014, Trusted Computing Group, 2009). It was also noted that the type of memory and the CPU clock speed might have an effect in the outcome of experiment's result. Therefore, it was considered as a best approach to conduct experiments on devices with different configurations and different types of CPUs and memory. These can be found in table 2. Since the initial argument is that the machines will be deemed inoperable after the use of the USB killer, the systems that were configured for the experiments were older and outdated for daily use. The aim was to identify the extend of the damage that could be caused and whether there would be any damage on the data that is present on the hard disks.

For constancy of the experiments two desktop computers and two laptops with different hardware configurations were used. The aim was to identify whether the design of the electronic circuits on the motherboard could present any differences on the results after the USB killer is used.

The hardware and software configuration for the different experimental setups are as follows:

1. The first system is an Intel Pentium 2 V.99GHZ Toshiba Tectra M2 laptop with 80 GB SATA hard drive and 1 GB DDR2 RAM. The operating system installed is Windows XP Professional version 2002, service pack 3.
2. The second system is an Intel Core 7300 2GHZ Toshiba Tectra A9 with 275 GB solid state drive (SSD) and 2 GB DDR3 RAM. The operating system installed is Windows XP Professional version 2002, service pack 3.
3. The third system is an Intel 7th generation (i7) with 160 GB solid state hard drive and two modules of 4 GB DDR4 RAM. The operating system installed is Windows 8.
4. The fourth system is an Intel 7th generation (i7) with 500 GB SATA hard drive and two modules of 16 GB DDR4 RAM. The operating system installed is Windows 7 Enterprise.

The original hard disk on laptop 2 was changed from a SATA disk to an SSD in order to compare the behaviour between a SATA (system 1) and an SSD disk (system 2) on a laptop when a USB killer is plugged in. The reason being that the SSD has a different hardware design to an electromechanical hard drive. In an SSD the data is stored on interconnected flash memory chips that retain the data even when no power is present. Systems 3 and 4 are desktop computers and a similar approach on the disks was followed. The operating system installations on the machines are clean and selected based on hardware compatibility. There was no further data added on the system, since the main scope of the experiments is on identifying whether any data would be destroyed, and this could be identified on the operating system level.

The experiments were conducted with a USB Killer v2.0 pro kit standard edition that comes with a testing shield and adaptors for testing mobile phones. The experiments intend to demonstrate the damage that can be achieved if a device is exposed to a USB killer with an active USB port.

The first phase of the experiment was conducted with the USB killer being plugged in on each of the four devices that were configured for this purpose. The second phase of the experiment is bifold and involves the forensic examination of the disk with the use of a write blocker and EnCase v8 and the testing of the RAM and graphics cards aiming to identify any damage that might have been caused on the disk and the other components.

	Type and Model characteristics	Processor	HDD	RAM	Operating System
1.	Laptop computer TOSHIBA TECRA M2 Model No PTM20E-4MP1F-EN Serial No X4710443G	INTEL PENTIUM 2 GHZ V.99 GHZ	SATA 2.5 HITACHI HTS548080MSAT00 80 GB	1 GB	WINDOWS XP PROFESSIONAL VERSION 2002 SP 3
2.	Laptop computer TOSHIBA TECTRA A9 Model No PTS52E-01V00YEN. Serial No 67093396H	INTEL CORE (TM) 2 DUO T7300@2 GHZ	SSD Crucial 275GB MX300	2 GB	WINDOWS XP PROFESSIONAL VERSION 2002 SERVICE PACK 3
3.	Desktop PC Intel Desktop Board: MICRO ATXLGA1155 SOCKET Q67 SERIES BIOS version: SWQ6710H	INTEL I7 2600 CPU@3.4 GHZ	INTEL SSD 545S S2CW 160GB	8GB (2x4GB)	WINDOWS 8.1 PRO
4.	Desktop PC Intel Desktop Board: MICRO ATXLGA1155 SOCKET Q67 SERIES BIOS version: SWQ6710H	INTEL I7 2600 CPU@3.4 GHZ	SATA 3.5 HDD 500GB WD5000AAKX	16 GB (2x8GB)	WINDOWS 7 ENTERPRISE

Table 2. Experiment's hardware configuration

5. Experiment results

The experiments were conducted in an isolated laboratory environment aiming to minimise the risk of causing any further destruction or damage to devices. The USB killer was plugged on one device each time and the tests were video recorded. Despite the fact that in Franceschi-Bicchierai (2015) doubts were raised that there would be visible 'burn' when the USB killer is plugged in a device, our experience showed that every time we plugged in the USB killer to conduct the experiment, a visible spark, a wisp of smoke and the smell of burned electronics were present.

The first phase of the experiment was conducted on each machine according to Table 2. It only took a fraction of a second from inserting the USB killer device to each system for it to go 'dead' with a small electric flash visible from the motherboard components. Both the laptops as well as the desktop computers failed immediately after the USB killer was plugged in. It was expected and pre-defined that the systems would become inoperable when the USB killer would be plugged in.

However, the main scope of running the experiment is to identify if there is any data affected from the USB killer or if any other components on the testbed were affected. The second phase of the experiment aimed to identify whether this was the case. The results from these experiments do not support the argument that is made from the USB killer developers who claimed that "*the drive controllers may be damaged to the point that data retrieval is impractical*" (USB Kill, 2017). The disks were connected on a forensic examination system with a Tableau write-blocker. All four drives on both the laptops and the desktop computers were still fully functional irrespective of their hardware configuration and all the data in the disk drives was still accessible.

The next stage was to attempt to determine whether the RAM modules and graphics cards were affected or if they were still functioning. The components were removed from each machine and installed into a test environment machine. Again, both the RAM and graphics cards were functioning as normal in all four cases.

Furthermore, some further study on the motherboards of the devices was deemed necessary to identify the extent of their damage. At the time of writing it is an ongoing study to determine which chipsets on the motherboards were destroyed. However, it is confirmed that the motherboards are inoperable.

	Type and Model characteristics	Component	State
1.	Laptop computer	**Motherboard:**	Non – functional, burned
	TOSHIBA TECRA M2.	**HDD:**	**Fully functional**
	Model No PTM20E-4MP1F-EN Serial No X4710443G	**RAM:**	**Fully functional**
2.	Laptop computer	**Motherboard:**	Non – functional, burned
	TOSHIBA TECTRA A9 Model No PTS52E-01V00YEN. Serial No 67093396H	**HDD:**	**Fully functional**
		RAM:	**Fully functional**

3.	Desktop PC Intel Desktop Board: MICRO ATXLGA1155 SOCKET Q67 SERIES BIOS version: SWQ6710H	**Motherboard:**	Non – functional, burned
		HDD:	**Fully functional**
		RAM:	**Fully functional**
4.	Desktop PC Intel Desktop Board: MICRO ATXLGA1155 SOCKET Q67 SERIES BIOS version: SWQ6710H	**Motherboard:**	Non – functional, burned
		HDD:	**Fully functional**
		RAM:	**Fully functional**

Table 3. Experiment's results

6. Conclusion

The USB killer is another device added on the list of USB-based attacks. The stated purpose of the USB killer is that it is to be used as a power surge testing device. However, the question is what happens when the device falls in the wrong hands and to what extend it can affect data that resides on a system. It appears that unmonitored USB hubs can be an area of significant concern in relation to the use of the USB killer, whether an insider threat or a targeted attack against a system. If the USB killer device gets into the hands of a malicious user, it can cause damage to large computer systems, for example a data centre. The damage to the hardware can affect the use of the system and result to denial of service.

The outcome of this research indicates that the data on the hard disks that were used in the experiments regardless of their type, SSD or SATA, remained intact after the use of a USB killer. However, the damage on the hardware leads to the system being inoperable. The speediness of the USB killer could potentially destroy numerous devices in a very short time, which makes the need for vendors and manufacturers to work against the power surge vulnerability more urgent. It also stretches the need to enhance physical security on systems. The lack of the user awareness in relation to the USB killer could expose the system owners to a vulnerable situation.

Research is currently ongoing to determine which elements(s) of the motherboard are affected by the USB killer. Other research will be carried out to determine the effect of the USB killer on different electrical devices which could have had impact on their storage elements. For instance, mobiles phones or any other smart devices which can be used in order to remove the sensitive data that might be used later in a digital forensic lab to support or deny any digital cases in the cyber world.

7. References

Anderson, B and Anderson, B. (2010), "Seven Deadliest USB Attacks". Syngress, Maryland Heights, ISBN: 9781597495530

Anthony, S. (2016), "USB Killer, yours for $50, lets you easily fry almost every device", Online: https://arstechnica.com/gadgets/2016/12/usb-killer-fries-devices, (Accessed on: 10/04/2019)

Axelson, J. (2015), "USB Complete the Developer's Guide". 4th ed. Lakeview Research, Madison, ISBN: 978-1-931448-08-6

Bradbury, D. (2019), "Killer USB Breach Highlights Need for Physical Security", Online: https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1-1/ (Accessed on: 26/04/2019)

Clark, J, Leblanc, S, Knigh,t S. (2011), "Compromise through USB-based Hardware Trojan Horse device", *Future Generation Computer Systems*, Volume 27, Issue 5, Pages 555-563.

Dark Purple. (2015), Online: https://habr.com/ru/post/268421/ (Accessed on: 10/04/2019)

Franceschi-Bicchierai, L. (2015), "The 'USB Killer' Won't Fry Your Computer. Probably", Online: https://motherboard.vice.com/en_us/article/8qxbka/the-usb-killer-wont-fry-your-computer-probably (Accessed on: 17/04/2019)

Mohay, G, Anderson, A, Collie, B, de Vel, O, McKemmish, R. (2003), "Computer and intrusion forensics", Artech House, Boston, ISBN: 978-1630812133

Murgia, M. (2015), "Killer USB stick that destroys your computer in seconds on sale", Online: http://www.telegraph.co.uk/technology/internet-security/11932793/Killer-USB-stick-destroys-your-computer-in-seconds.html (Accessed: 11/04/2019)

Murphy, R. (2017), "AN57294 - USB 101: An Introduction to Universal Serial Bus 2.0", *Cypress Technical Documents, Application Notes*, online: https://www.cypress.com/file/134171/download (Accessed: 11/04/2019)

Neuner, S, Voyiatzis, AG, Fotopoulos, S, Mulliner, C, Weippl, ER. (2018) "USBlock: Blocking USB-Based Keypress Injection Attacks". In: Kerschbaum, F, Paraboschi, S (eds) *Data and Applications Security and Privacy XXXII. DBSec 2018, 32nd Annual IFIP WG 11.3 Conference, DBSec 2018, Bergamo, Italy, July 16–18, 2018, Proceedings.*

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

Nohl, K. Krissler, S, Lell, J. (2014), "BadUSB - On Accessories that Turn Evil", Online: https://srlabs.de/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf (Accessed on: 10/04/2019)

Pham, DV, Syed, A, Halgamuge, MN. (2011), “Universal serial bus-based software attacks and protection solutions”, *Digital Investigation*, Volume 7, Issues 3–4, Pages 172-184.

Tetmeyer, A, Saiedian, H. (2010), “Security Threats and Mitigating Risk for USB Devices”, *IEEE Technology and Society Magazine*, Volume 29, Issue 4, Pages 44-49.

Tischer, M, Durumeric, Z, Foster, S, Duan, S, Mori, A. Bursztein, E, Bailey, M. (2016), “Users really do plug in USB drives they find”, *2016 IEEE Symposium on Security and Privacy (SP)*, Pages 306 - 319

Trusted Computing Group. (2009), “How to Use the TPM: A Guide to Hardware-Based Endpoint Security”, Online: https://trustedcomputinggroup.org/use-tpm-guide-hardware-based-endpoint-security/. (Accessed on: 10/04/2019)

USB Kill. (2016), “USB Kill: Behind the scenes”. Online: https://www.usbkill.com/blogs/news/usb-kill-behind-the-scenes (Accessed on: 11/04/2019)

USB Kill. (2017), “FAQ”. Online: https://usbkill.com/pages/faq. (Accessed on: 10/04/2019)

USB Kill. (2019), “Home page”. Online: https://usbkill.com/. (Accessed on: 11/04/2019)

Wang, Z., Stavrou, A. (2010), “Exploiting smart-phone USB connectivity for fun and profit”. *Proceedings of the 26th Annual Computer Security Applications Conference*, pp. 357–366. ACM

Whitaker, Z. (2017), “This laptop-bricking USB stick just got even more dangerous”, Online: https://www.zdnet.com/article/this-weaponized-usb-stick-gets-even-more-dangerous. (Accessed on: 11/04/2019)