ON USB KILLER DEVICES AND THE NEED FOR MORE AWARENESS ABOUT IT

Prof. Omkar J. Bapat

Assistant Professor
Sri Balaji Society's Balaji Institute of Management and Human Resource Development
Admissions Department
Sri Balaji Society, Pune, India

Abstract: **'Universal Serial Bus' devices or USB Devices and USB enabled ports have become indispensable in the days of today. Once limited to Computers (PC's and Laptop/Related 'top' computers) they are being found 'everywhere', in powered vehicles, boats, aircrafts, power tools, medical and medical diagnostic equipment, testing and measurement equipment and so on. It is possible today to transfer the entire volume of the Library of Alexandria (before it was burnt down) into a small USB Storage drive, the size of a Double AA dry cell battery. This ubiquitous presence of the USB is in its way a danger to devices as a few USB based devices have been built which use electric power acquired from the device, wherein USB enabled port is present and uses the electricity to 'fry' the circuits of the device, destroying it or damaging it for good. There is an immediate need for creating awareness about these 'snakes that bite the feeder's hand' so that the majority users of the devices, wherein USB ports are present do not fall prey to these unscrupulous devices. This discussion paper on USB Killer devices is more of an 'informatory' paper than a 'technical' paper but it is clear that more research is needed to develop a sense of awareness and alertness about these dangerous devices so that expensive and indispensable, equipment wherein USB enabled ports are present are kept safe.**

Introduction:

Computer devices have been with us in some form or the other since the last two thousand or more years. A good example for this is the 'Antikhera Mechanism[1]' which is said to be a ridiculously advanced celestial object position calculator for its age as it was dated to have been created between the years 100 to 205 BC. Technological advancements were made in leaps and bounds since the death of Christ leading to several 'automatons' being built, which fulfilled several purposes ranging from entertainment to religious. One of the most 'advanced' automata were built by the legendary French watchmaker, Pierre Jaquet Droz between the years 1768 and 1774. The name 'Jaquet Droz' is still synonymous with quality, uniqueness and taste in the world of wrist watches and other time keeping and display mechanisms. Pierre Jaquet Droz's automata[2] were said to be the most complex and intricate piece of machinery ever built in that age. Three of them: 'The Writer', 'The Draughtsman' and 'The Musician' were built to be so 'perfect' that any person would mistake them for a genuine human being and not a machine. An example can be made of 'The Writer' automaton which was able to reproduce any written message (within the set character limit) on a sheet of paper.

The automaton simply did not print the requested message, it 'wrote' it using an ink pen with its hands, striking awe and fear into the viewer's thanks to its eerily human like body movements. The Writer was also said to be the world's first programmable computer[3] and comprised of around 6000 moving parts.

Even if they were far more advanced than any device when they were invented, automatons could only perform the tasks or purpose they were built for. To fill in the lacunae for the performance of multiple tasks, 'mechanical computers[4]' were built. They have been with us in some form or the other since the last hundreds of years. Initially designed for computing planetary positions (Antikhera Mechanism), mechanical computers soon were built for solving one of the most persistent issues of life: computation of mathematical problems (Example: Gottfried Wilhelm Leibniz's Mechanical Calculator built in the year 1694 and Curt Herzstark's Curta Calculator[7], built in 1948). Along with providing answers to given mathematical problems, these computers tackled other problems such as calculation of tide heights (William Thomson's Ball and Disk Integrator built in 1886), for precision target acquisition and aiming for anti-aircraft warfare (Mark I Fire Control Computer built by Hannibal Ford of the Ford Instrument Company[8] between the years 1939 to 1945), for plotting the 'real time' position of a spacecraft in orbit around the earth (GLOBUS IMP Navigational instrument[5], built by the Specialized Experimental Design Bureau of Spacecraft Technology (SOKB KT) in the year 1960) and for calculating changes in a nation's economy (Monetary National Income Analogue Computer[6], built in the year 1949 by economist Bill Philipps).

The computer devices we use today are radically different than their ancestors as a single system can perform more functions than a hundred different mechanical computers and automatons. Computers took a 'great leap ahead' with the invention of the 'Universal Serial Bus' technology in the year 1994[9] by Ajay Bhatt of the INTEL company and the USB Implementer's forum, comprising of noted technological companies such as, Intel, Microsoft, Compaq, LSI, Apple and Hewlett-Packard. The invention created a 'revolution' in computing technology as it 'liberated' several individual and group serial and parallel ports and other input ports wherein raw data entered the computer CPU unit and left it as processed information. The overall size of computers got reduced paving the way for more miniaturization and economy. The USB hubs were more 'tolerant' unlike the ports of the age before USB[10] which could be called as 'spoilt' as they required a lot of attention and had difficulties in 'sharing'

computing power with other expansion cards. Since they behaved like 'divas' users had to often spare some time for configuring and troubleshooting them. Far thinking computer manufacturers such as Apple, saw the benefits of USB and decided to 'replace' the older legacy ports with USB ports. The 'Imac G3' is an example of this decision as it favored USB hubs more over the older portals and paved the way for the inclusion of more and more USB portals for convenience and ease of operation for the consumers. The latest version of the USB 'USB 3.0' offers superhuman like speed when it comes to data transfer rate (maximum up to 4.8 GB per second) when compared to the 12 MB per second of the USB 1.0 version at the time of the invention of the USB technology, more than twenty years ago.

However, this technology has its own dark side, which soon saw fruit a few years in the future following the invention of the USB storage drive[11] in an Israeli Company, M-Systems by its employees, Amir Ban, Dov Moran and Oron Ogdan in the year 1999. Hackers soon saw the potential of the USB drive and the USB hub for causing mischief and for more serious damage and sabotage opportunities. This led to the innovation of the 'USB Killer[13]' device which true to its name, kills[36] a computer system, rendering the laptop, desktop and or other on-board USB enabled and or USB hub onboard devices and equipment, unable to function as it should. We can consider this USB killer as a 'Stonefish', a fish noted for its poison and camouflage abilities[12] which, true to its name resembles a 'stone' and is oft mistaken for one by fishes to their disadvantage as it gobbles them up from the murky depths. Not only fish, human beings and other large sized animals have known to make the same mistake as they are dispatched to hell, faster than a pistol shrimp can pop a bubble. Not only does this fish kill when it is alive, it is known to kill even after it is dead. Like a stone fish it is difficult to identify a USB Killer device as it looks very similar to an 'ordinary' USB device or a USB storage drive and 'kills' the body (computer) on being touched (inserted into the USB Hub). A good way to identify it is to dissect it as the internal components of a USB killer are radically different than an average USB drive. However, this is not practical and thus the threat of a USB Killer device hangs over the head like a prides of lions in the Savannah. Prevention is better than cure and the only way to prevent a USB Killer from 'being true to its name' is to acquire a 'gatekeeper' device which prevents this device from damaging the computer. The gatekeeper device 'USB Killer Shield[14]' was invented by the company that invented the USB Killer as a poison is useless without an antidote.

Review of Literature:

The idea for writing this paper came into the author's head when he read about and viewed a couple of videos on YouTube describing the destructive power of the USB Killer devices. The simplicity of this device is in proportion with its deadliness as it works by drawing in and storing electricity from the very computer it is plugged into and then releasing it back many times stronger into the computer. We can compare this device like the 'viper' from the story of 'the farmer and the viper'. Majority of the content available on the internet describes this device and its effects, however very few content is available which discloses how to protect one's computer system from this device.

Further, Matthew Tischer, Zakir Durumeric, Sam Foste and Sunny Duan, Alec Mori, Elie Bursztein and Michael Bailey (2016) have described that people in general do not think twice much before plugging in any USB Storage media device or a similar looking device found or picked up from an unknown place or if the same was received by a non-trustworthy person. It could be said that the people in general trust their computer system's Anti-Virus Software to 'handle' any viruses, worms or trojans along with other forms of malware if present in the USB storage media devices.

Nir Nissim, Ran Yahalom and Yuval Elovici (2017) have described that there are a sum number of 29 ways wherein USB storage media devices can be used for spreading malware and other malicious and hazardous executable programs into computer systems. It may be possible that the latest versions of the popular anti-virus programs and softwares might prevent their users from being the victims of the attacks but the 29th attack: USB Kill cannot be stopped by the anti-virus programs as they is no way to detect it as it requires physical verification, before inserting the device in question in the computer system.

Further, news has come in of several unidentified USB Storage media sticks being left in letterboxes and other public locations in Australia[16]. The police there are warning the citizens not to blindly plug the media into their computers as they might be infected with undesirable programmes. A question[17] was asked about this phenomena on the popular information creation and sharing website 'Quora' wherein a sum number of 84 registered users of the site responded to the question when they were sked to disclose whether they too found a USB storage media stick in an unknown place and whether they accessed it and if they did access it, what content was found inside it.

The answers revealed that the users who answered the questions disclosed that they accessed the USB storage media sticks after it was deemed to be 'clean' by their computer system's anti-virus program. A few respondents disclosed that they did not access the device, fearing that it might be a 'UBS Killer'. They further warned the users about the same and spoke about the hazards of accessing unknown USB storage media devices.

The information disclosed by the users revealed that majority of the information present in the USB storage media devices was general in nature: Word documents, PDF's, Excel Sheets, PPT Documents, images, audio and video files. A few users reported finding content which was of pornographic in nature. The users also reported that the devices they accessed contained personally identifiable details such as scanned copies of personal documents: Passports, Credit card numbers and intimate photographs. The information disclosed in the answers revealed that the respondents tried to contact the 'owners' of the USB storage media devices from the information within them and returned the said devices to them, post contacting them. The respondents who could not contact the owners, disclosed that they kept the devices for themselves after deleting and removing the data contained in it by formatting them. Amongst all the users, none of them reported of being a victim of the USB Killer device.

It may be possible that majority of the USB storage media devices being found were of a genuine case of misplacing by mistake and were not the result of a malicious plot to cause damage to computer systems by unknown parties.

The researcher also found a White Paper on Endpoint Connectivity authored by Blake Markhan (2017) wherein the USB Killer was described and the need for modification of the USB Hub devices for ensuring endpoint connectivity security was stated.

It is clear that there is a vast ground for research into identification and detection of USB Killer devices and for developing protection mechanisms against them so that physical infrastructure security and integrity of the USB hub enabled devices can be maintained so that one will be protected in a better way against these stonefishes, until the vulnerabilities that created their existence in the first place is cured for good.

How does the USB Killer device work?

The 'idea' behind the creation of the USB Killer device was first thought out by a Russian hacker, going by the pseudonym, "Dark Purple[21]" who created a 'proto type' USB Killer device to highlight a key flaw in the build of the physical hardware component unit of the computer (The body of the computer). In an article written by him on a Russian website[22], Dark Purple claimed that the 'USB Killer' device had the ability to destroy any electronic or electric device which has USB Hub or a USB Host interface. If we look around us today, we will find a number of devices wherein USB hubs are presents in our homes, consumer devices, specific use devices, vehicles, boats and aircrafts and so on.

The USB Killer is simplicity in itself. The physical device has a bunch of 8 and above capacitors, soldered on to it. When the USB Killer device is plugged into the USB Hub enabled device, it receives the electricity from the device (DC to DC) and uses it to build up charge in the capacitors. Once the capacitors are charged, the electricity (between minus 200 to 220 volts) is 'dumped back' into the device. This 'charge and discharge' cycle continues until the USB Hub enabled device is unable to provide electricity to the USB Killer device or until it is destroyed, both ways harmful to the USB Hub enabled computer device or other similar device or devices.

Deep Purple's prototype device was developed into the USB Killer device by a company based in Hong Kong[23] named, HK Elechouse Electronics Technology CO Limited and is sold by the company on all leading online shopping portals and from its own website[24]. The reason why the USB Killer device works is because majority of the USB enabled electric and electronic devices and computers made, sold and used today are not built with 'Optical Isolation Protection[25]' which uses an application of the 'Photo electric effect' discovered by Albert Einstein and Max Planck. An Optical Isolation unit[26] comprises of two elements: A light source (LED Bulb or a similar light source) and a light (photo) sensitive detector. These two elements are positioned in a way wherein the light source faces the light sensitive detector and is connected to the electrical circuit transforming the connected elements into an 'optocoupler'. Unlike an electrical transformer which works using 'electromagnetic induction', optocouplers 'transmit' electricity via light emitted from the LED bulb in a proportionate intensity as per the electricity flowing through it. The light emitted from the LED falls upon the photo sensitive detector, releasing electricity for the device to be used in its components. Since no direct electricity flow occurs here, the electronic device is more 'insulated' than other devices which do not feature this application. As of now, consumer electronic computers and other devices built by the Apple Company[27] have these optocouplers included in their build and in the peripherals and power supply units[28] rendering them more or less 'safe' in the face of the USB Killer devices.

Apart from Optical isolation, a device has been created which can be used to prevent USB Killer devices from harming one's computer systems. The device is called as 'USB Killer Shield[29]' and is built by the same company that developed the 'production version' of the USB Killer from Deep Purple's prototype. This device is touted to 'protect' any USB enabled device from USB Killer devices and is a must have device, if one is paranoid about safety regarding USB storage media devices. Noticing the increasing usage of USB cables being used for data transfer as well as for charging USB enabled devices, the USB Promoters Group announced a new protocol[30] to deal with the hazards of faulty or malicious Type 'C' chargers and devices.

The protocol was created in an attempt to fix the problems and issues identified and experienced by the users who were using the Type C standard enabled devices as a convenient way to charge their smart devices and transfer data, wherein more work could be done with few cables. Post application of the protocol, the user will be able to set standards, wherein they will be able to choose whether to use the USB chargers that are compliant with the standards or to decide whether to prevent them from interacting with the computer system until such time wherein their authenticity is verified. The protocol decrees that this verification will be done, immediately when the cable is connected so that neither data nor power is transmitted to the host device. This protocol is a welcome step in the new direction, but it remains to be seen whether a fresh set of protocols are announced to deal specifically with USB Killer devices.

Need for awareness about USB Killer

A cursory search[31] run on the Search engine Google with the search string "Buy USB Killer Online" revealed a sum number of 32 lakh results. Many of the listed web links were of popular e-commerce companies such as Amazon wherein the USB Killer device was listed for sale and various other websites describing the hazards of the USB Killer devices. Further, a news report[32] published in the popular news website Dailystar.co.uk revealed that the USB Killer devices 'sold out' almost immediately after it was placed on sale online. It is clear that majority of the persons who purchased the USB Killer device, bought the devices

for other purposes than 'testing of vulnerabilities' in USB enabled devices, because if the former was true, the device would not have sold out like 'hot cakes' as claimed by the news article.

Further, it is not that difficult to build such a device from scratch. As described[33] in this video uploaded on YouTube by an electronic hobbyist, Kedar Nimbalkar, one can build such a device using basic tools and ordinary daily use objects such as anti-mosquito tennis rackets. Kedar Nimbalkar also described the construction of the USB Killer device on a video[34], uploaded on YouTube. It is very difficult to distinguish a USB Killer device from an ordinary USB device if the former is disguised to look nearly or exactly alike like the latter.

Apart from optical isolation, USB Authentication[35] is a good way to protect one's computer systems and other similar USB enabled systems from the hazards of the USB Killer devices. However, seeing the ease in which the USB Killer devices can be constructed and the expensive damage they cause to computer systems and other similar USB enabled systems, it is clear that not much time is with us until protection mechanisms are created for all the USB enabled devices we use as prevention is truly, better than the cure.

Conclusion:

It is hard to imagine a life without USB devices as they are one of the 'must have' appendages of the computer devices and other similar devices. Thus they have become as indispensable for us as economically priced Wi-Fi, large sized data plans and data storage devices. The indispensability of the USB device is in its own way, a hazard as it can be used to gain access for malicious and destructive intent into a computer system. A sum number of 29 ways[18] have been identified wherein the same can be done. This, in addition into the ridiculously easy way for acquiring the USB killer devices by purchasing or by building the same by one's own self has made it clear that there is an immediate need to protect one's computer system from harm as it is far better to prevent the disease before it occurs than to spend time in finding a cure, after it has been infected.

References:

1. MATTHEW TISCHER, ZAKIR DURUMERIC, SAM FOSTE AND SUNNY DUAN, ALEC MORI, ELIE BURSZTEIN AND MICHAEL BAILEY, Users Really Do Plug in USB Drives They Find, May 2016 IEEE Symposium on Security and Privacy (SP).
2. NIR NISSIM RAN YAHALOM YUVAL ELOVICI, USB Based Attacks, August 2017, Computers & Security (COMPUT SECUR) Journal.
3. BLAKE MARKHAM, Endpoint Connectivity, 2017, August 2017, NCC Group White Paper, NCC Group.

Articles and Websites:

[1] Encyclopedia Wikipidea, Antikyhera Mechanism, https://en.wikipedia.org/wiki/Antikythera_mechanism
[2] Encyclopedia Wikipidea, Jaquet Droz Automata, https://en.wikipedia.org/wiki/Jaquet-Droz_automata
[3] Suzzanah Hills, Was this automaton the world's first computer?, http://www.dailymail.co.uk/news/article-2488165/The-worlds-Mechanical-boy-built-240-years-ago-engineered-act-writing.html
[4] Encyclopedia Wikipidea, Mechanical Computer, https://en.wikipedia.org/wiki/Mechanical_computer
[5] Yurii Tiapchenko, S.A. Borodin, A.F. Yeremin, S.T. Marchenko. Slava Gerovitch (Translator), Information Display Systems for Russian Spacecraft: An Overview, http://web.mit.edu/slava/space/essays/essay-tiapchenko1.htm
[6] Encyclopedia Wikipidea, MONIAC, https://en.wikipedia.org/wiki/MONIAC
[7] Encyclopedia Wikipidea, Curta Calculator, https://en.wikipedia.org/wiki/Curta
[8] Encyclopedia Wikipidea, Mark 1 Fire Control Computer, https://en.wikipedia.org/wiki/Mark_I_Fire_Control_Computer
[9] The authors, Allusb.com, History of USB, http://www.allusb.com/usb-history
[10] Andrew Cunningham, Ars Technica, A brief history of USB, What it replaced and what has failed to replace it, https://arstechnica.com/gadgets/2014/08/a-brief-history-of-usb-what-it-replaced-and-what-has-failed-to-replace-it/
[11] Encyclopedia Wikipidea, History of the USB Flash drive, https://en.wikipedia.org/wiki/USB_flash_drive#History
[12] The authors, Spotmydive.com, 10 Masters of undersea camouflage, https://www.spotmydive.com/en/news/10-masters-fish-of-undersea-camouflage-scuba-diving
[13] USBKILL Company, USB Killer Tester, https://usbkill.com/products/usb-killer-tester
[14] USBKILL Company, USB Killer Device, https://usbkill.com/, USB Kill
[15] Matthew Tischer, Zakir Durumeric, Sam Foste and Sunny Duan, Alec Mori, Elie Bursztein and Michael Bailey, Users Really Do Plug in USB Drives They Find, https://zakird.com/papers/usb.pdf
[16] Larisa Cosis, The Unknown danger of USB Sticks in letterboxes, https://www.endpointprotector.com/blog/the-unknown-danger-of-usb-sticks-in-letterboxes/
[17] Quora.com, There are some recent cases of receiving random USB sticks that may contain malware or ransomware in letterboxes in Australia. Have you ever found a USB stick in a random location or received one in the letterbox?, https://www.quora.com/There-are-some-recent-cases-of-receiving-random-USB-sticks-that-may-contain-malware-or-ransomware-in-letterboxes-in-Australia-Have-you-ever-found-a-USB-stick-in-a-random-location-or-received-one-in-the-letterbox
[18] Nir Nissim Ran Yahalom Yuval Elovici, USB Based Attacks, https://www.researchgate.net/publication/319050539_USB-based_attacks
[19] Blake Markham, Endpoint Connectivity, https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2017/ncc-group-whitepaper_endpoint-connectivity.pdf

[20] Yang Su, Daniel Genkin, Auto-ID Lab, Yuval Yarom, Data 61, USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-su.pdf
[21] Dark Purple, USB Killer device, https://kukuruku.co/post/usb-killer/
[22] Dark Purple, USB Killer device, https://habrahabr.ru/post/268421/
[23] USB Killer Company, Press Release about USB Killer, https://cdn.shopify.com/s/files/1/2190/5915/files/USBKill-Press-Release.pdf?14195061072213225 43
[24] USB Killer Company, USB Killer product, https://usbkill.com/products/usb-killer-v3
[25] Patton.com, About Optical Isolation, https://www.patton.com/technotes/about_optical_isolation.pdf
[26] Electronics-Tutorials.com, Optocoupler tutorial, https://www.electronics-tutorials.ws/blog/optocoupler.html
[27] Gary Jones, USB killer 2.0: Only Macbook Pro and Air protected from new weaponised circuit destroyer?, https://www.express.co.uk/life-style/science-technology/711745/USB-killer-2-0-Macbook-Pro-Apple-Macbook-Air
[28] Ken Shiriff, Macbook charger teardown: The surprising complexity inside Apple's power adapter, http://www.righto.com/2015/11/macbook-charger-teardown-surprising.html
[29] USB Killer Company USB Killer Shield product https://usbkill.com/products/usb-killer-tester
[30] Lucian Armasu, USB Type-C Authentication Protocol To Allow Blocking Of Uncertified And Malicious USB Devices, http://www.tomshardware.com/news/usb-type-c-authentication-protocol-announced,31595.html
[31] Google Search, Search string 'Buy USB Killer online', https://www.google.co.in/search?q=usb+killer+buy+online&oq=usb+killer+buy+online&aqs=chrome..69i57j0.5191j1j7&sourceid=chrome&ie=UTF-8
[32] Dave Snelling, Don't plug this in to your PC – £45 weaponised USB stick can instantly KILL any computer, https://www.dailystar.co.uk/tech/news/545717/USB-Killer-sold-out-attack-Apple-Mac-Windows-PC
[33] Kedar Nimbalkar, HOW TO MAKE USB KILLER FROM BUG ZAPPER RACKET!, https://www.youtube.com/watch?v=ux3SkJ6PMmA
[34] Kedar Nimbalkar, How To Make USB Killer : DIY in 3$, https://www.youtube.com/watch?v=82-MDymVkps
[35] Andrew Cunningham, Ars Technica USB-IF battles malware and bad chargers with Type-C Authentication spec, https://arstechnica.com/gadgets/2016/04/usb-if-battles-malware-and-bad-chargers-with-type-c-authentication-spec/
[36] Sebastian Anthony, USB Killer, yours for $50, lets you easily fry almost every device, https://arstechnica.com/gadgets/2016/12/usb-killer-fries-devices/