# An Enhanced Approach for USB Security Management

Daniyal Naeem

# Technical Report

RHUL–ISG–2020–8

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

# Student Number: 100885268
# DANIYAL NAEEM

# Title: An Enhanced Approach for USB Security Management

**Supervisor: KEITH MAYES**

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Daniyal

Date: 01-07-19

# Acknowledgement

I would like to acknowledge the help and support given to me by my supervisor Keith Mayes (Professor of Information Security – Royal Holloway, University of London) over the past year. His valuable experience helped me progress my project work and my time in BT.

# Contents

# Abstract

The portability and high data transmission speeds of USB Flash drives are increasingly making them a preferable medium for data transfer and storage. These portable devices are offering users expedient access to personal and business data on the go. However, with the increased usage of these devices, the associated risks have also escalated. At present, USB devices are found to be a major source of spreading malware (malicious programs) and data exfiltration. These devices provide malicious insiders with the opportunity of stealing data inconspicuously since these can be hidden very easily due to their small size, and it is quite tricky to track their usage. This report scrutinizes the existing USB security solutions that are falling short of the requisite security targets. It is argued that the enhancement of existing USB security architecture and reworking on the security policies is the only approach to make USB sticks a secure data storage option. A novel USB monitoring system is developed here based on the identified vital security attributes, and conclusions are drawn through the comparison of the devised solution with the existing ones.

# 1. Introduction

The contemporary situation of ubiquitous surveillance practices and augmented focus on data collection and processing has resulted in several threats to the protection of data. Various means (government, financial institutions, online shopping stores, etc.) are used for collecting this data, either knowingly or unknowingly. In recent times, data protection is being given paramount importance, and every other organization is facing the constant pressure of improving data protection practices. The value of data protection cannot be undermined as the amount of data created and stored is growing at a very fast pace. Moreover, the incessant cases of data leakages are also forcing organizations to verify and enhance their adopted data protection techniques.

There are various cases where a huge amount of sensitive data had gotten into the wrong hands due to inadequate security measures. For instance, eBay, (the online sale giant), Uber (a multinational transportation network company), Facebook (one of the biggest social platforms) and WhatsApp (a popular messaging app all around the globe), all have suffered major cybersecurity breaches in the past few years (Armerding, 2018). Most of the times when breaches are triggered due to data leakages, companies have to face embarrassment, public inquiry and judicial and financial penalties that then specifically encouraged the companies to put the efforts of strengthening data security.

There are different reasons for the current data security breaches. At present, multiple gadgets are employed for accessing the internet, transferring pictures to computers (e.g. digital cameras) and transferring data within devices (e.g. USB sticks). All these devices pose a threat to the protection of sensitive data. There are USB controller chips that are incorporated in most of these peripherals which can be reprogrammed. The attacker can manipulate these chips to insert malicious code, which makes it very easy to hack a computer when the device is plugged in. Among these, the USB storage devices have particularly gained substantial worth in the current market because of its effective data transmission facility and ease of use. However, data theft and malware insertion are the major threats linked with USB storage devices. Thus, the only practical solution is to take proper security measures; else these devices will remain one constant threat to data security.

## *1.1* ***Background***

In recent times, the rapid development of technologies has made the availability of various innovative peripheral devices possible, which have also resulted in an easy and swift process of data transfer. Most of these peripheral devices are connected to the computer using the USB port. USB flash drive is among one of the most popular peripheral devices in the market. Various types of data transferred through the USB port poses great chances of computer crimes unless proper security measures are taken.

This section gives an overview of these major computer crimes, highlighting the importance of USB memory sticks and talks about the security threats associated with these storage devices.

### 1.1.1 Computer Crimes

In the modern world, the speedy growth of computers and networks has crafted various opportunities for carrying out criminal activities. The computer crimes, also sometimes referred to as Cybercrimes, are not just limited to hacking, unauthorized access, spamming, phishing, but also include general misuse of resources, industrial espionage, identity theft, and online frauds, etc (Bregant & Bregant, 2014). Some of the major types of computer crimes are discussed as follows:

- ***Theft***

Identity theft and data theft are considered to be the two major types of theft in the cyber world.

Identity theft is the use of illegal methods for acquiring personal information like phone number, address, passport number, date of birth, name, credit card details, email ID, etc. This information can then be used by the stealer for gaining access to bank accounts and using one’s identity for carrying out other fraudulent activities. Skilled identity thieves use different methods like phishing or skimming for stealing personal information. In the phishing approach, they extract information by pretending themselves as a reliable authority. However, a small device named skimmer is employed in the skimming technique for obtaining the required personal information.

On the other hand, data theft is the theft of personal or managerial data with the intent of attaining confidential information or compromising privacy. Data theft is a growing issue for big firms as well as for individual computer users. Moreover, the conventional type of stealing that sensitive data involves the theft of the source like a tablet, laptop or a USB stick. One such event was reported in the United Kingdom, where a laptop having data and saving account details of around 2000 people got robbed from an employee of HM Revenue & Customs, UK (Evans, 2017). Another similar event occurred in 2014, where a fine of $150,000 was levied on a small Massachusetts physician practice when an unencrypted USB stick having medical records of 2200 patients got stolen. This fine was principally charged because of the failure of the company in defining proper data handling procedures (Solutions, 2017).

These cases have pointed out several shortcomings on the organization's end, e.g. allowing the employees to carry sensitive information on a flash drive or storing unencrypted data on a flash drive, laptops, etc. In addition to these, there also appears a lack of security measures within the organization firm or insufficient capability of carrying out risk assessments in handling sensitive data.

- ***Fraudulent Activities***

Online fraud has presently turned out to be one of the most common computer crimes worldwide. According to the Crime Survey of England and Wales (CSEW), almost one in ten people are falling victim to some sort of online fraud (Evans & Scott, 2017). The most common type of online fraud is phishing, which is the process of collecting personal information through websites or emails claiming to be legitimate.

Another type of online fraud is Fraudulent "Pop-up Windows" that is often employed for obtaining personal data and injecting malware. Pop-up windows appear mostly due to the programs called "spyware" or "adware" that are installed on the computer (Tripathi, Nigam & Edla, 2017). These programs are mostly hidden within free downloaded programs and they usually appear after analyzing the victim's web activity. A lot of these programs permit risk-free advertisements, but a few of these contain "Trojan horses" that can record one's keystrokes or relaying information to unauthorized sources (HHSB, 2019).

Vishing or voice phishing is another common type of online fraud. In this case, for instance, a person receives a call from someone posing to be a representative from the bank asking for authentication details (Cyber Cell Delhi, 2016). The innocent customer provides such information, only to find later that his or her bank account has been compromised.

- ***Copyright Infringement***

Copyright infringement has been termed as theft, piracy or violation of the exclusive rights of copyright holders through the illegal use of a copyrighted work or material. The key reasons behind copyright infringement are the inability to pay high prices requested by legal sellers, and the unavailability of the product in the country or language of the end-user. The advancements in digital technology and increasing reach of the internet have primarily resulted in anonymous copyright infringements all around the globe (Crawford, 2012).

- ***Cyberterrorism***

Cyberterrorism is a politically motivated use of information technology and computers for causing widespread fear or severe disruption in society. For example, a simple false message that is spread through the Internet regarding any attack at a certain time and place can be a case of cyberterrorism. The cyberterrorism activities can be performed over private computer servers as well as against secured government or other restricted networks. The viruses can be introduced by the wrongdoers into the vulnerable networks; moreover, they can launch denial-of-service attacks and deface websites (Janczewski & Colarik, 2008).

- ***Attacks on Individuals and Organizations***

It is quite possible to attack an information system of an organization either physically or remotely. Physical attacks involve penetration into the physical security of the information protection systems. These include an attack on machines/computers or data storage devices associated with important facilities. This may also involve injecting malware or ransomware through the insertion of malicious USB stick into the system. The irrecoverable loss of expensive equipment and essential records can cause catastrophic damage to the organization due to these sort of attacks. Therefore, it is a critical requirement to protect such physical assets like servers and computers by means of efficient security techniques, such as the use of face recognition, retina scan, thumbprint, access card, two factor etc. for authentication and authorization purposes. Moreover, it is not just important to invest in physical security measures, but also to train and enforce staff for following the best security practices. This includes using strong passwords, taking care of their personal devices such as USB sticks and locking computers when they are not being used, etc.

Remote attacks are the cyber-attacks on a system that do not require direct physical access to the system. Most of the time, the motive of remote attacks is to compromise the confidentiality and availability of the target by viewing or stealing data illegally and to introduce viruses or other malicious software on the system to cause damage on the network. Denial of Service (DoS) attack is also one of the most widely known remote attacks on systems, which mainly targets specific red side facing websites and associated servers. This attack is aimed at crashing a network by flooding it with false requests, thus reducing the network availability for the legitimate user. Although typical DoS attacks do not cause loss of important information/assets or theft but they can still result in great time and money loss for the victim (Carl, Kesidis, Brooks & Suresh Rai, 2006).

Distributed Denial of Service (DDoS) is a powerful form of DOS attack in which several compromised systems infected with a Trojan, are employed for targeting a single system. The main difference between a DoS attack and a DDoS attack is, DoS attack generally involves one workstation and one IP for flooding a resource. In the case of DDos attack, it uses multiple IPs and workstation for flooding the targeted resource, as shown in **Figure 1**. The DDoS attack is considered to be a prime concern in Internet security nowadays because these sort of attacks usually make a network or website unavailable by crashing or flooding it with too much traffic.

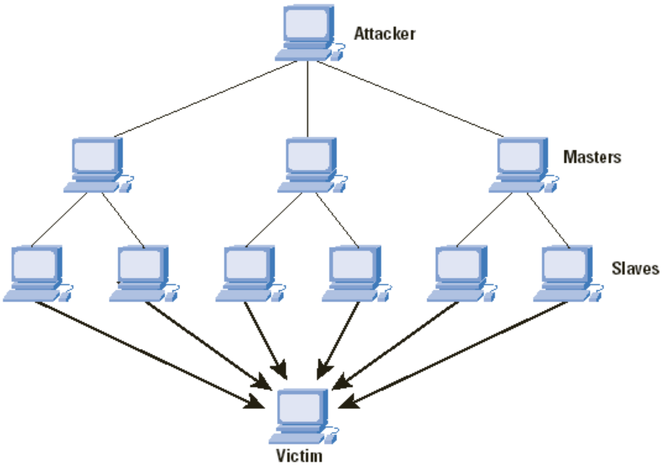


**Figure 1: DDoS Attack**

There are also some other types of attacks as well, such as a side-channel attack, fault attack, etc that can harm a computer (Standaert, 2009). A fault attack is when an integrated circuit or its state is intentionally manipulated, with the purpose of provoking an error within the integrated circuit so that the device is moved into an unintended state (Janczewski & Colarik, 2008). The goal here is to access the secure critical information or to disable the internal protection mechanisms. A side-channel attack is the one on a computer system that is based on information gathered through the physical implementation of a computer system, instead of exploiting the limitations in the implemented algorithm itself. Examples of such attacks are cryptanalysis and software bugs (Walters, 2012).

All the above mentioned computer crimes can have serious societal effects including a threat to national defense, psychological mess and economical disrupt, etc., which is mainly caused due to reduced productivity, wasted time and loss of data and revenue. However, these computer crimes can be restricted by properly analyzing their behavior and understanding their impact on various social levels.

### 1.1.2 Universal Serial Bus (USB)

USB is an interface that is supported by many OS including Linux, Mac, Windows, and others. It has been in the market for close to two decades and its usage is increasing exponentially. A USB port is intended to make the connection of peripheral devices with PCs, laptops and mobile phones a bit easier. Any device can be recognized automatically once it is plugged into the USB port depending on the OS and drivers installed, without any intervention of user through commands or clicks (Axelson, 2005). The USB port is now commonly used for video game consoles, home stereo equipment, television, printers, keyboards, storage devices or even for USB Rubber Ducky and Bad USB for malicious intent.

The process of connecting a USB cable or USB device with the workstation is quite straightforward and it gets connected to the system without essentially restarting the system. In order to facilitate users in using USB devices, a certain symbol is used for denoting USB connections around the port and connector. There are different types of USB connectors, available in the market, as shown in **Figure 2**; where Type A and B connectors are the most commonly used ones.

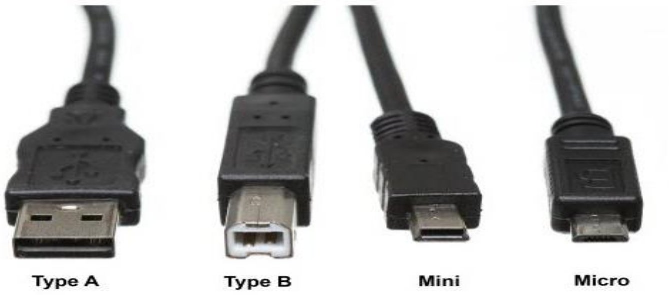


**Figure 2: Types of USB connector**

The pin configuration for these commonly employed USB connectors is shown in **Figure 3**. There are four shielded wires, two of these are for power (+5V and GND) and the other two are for data (labeled as Data+ and Data-).

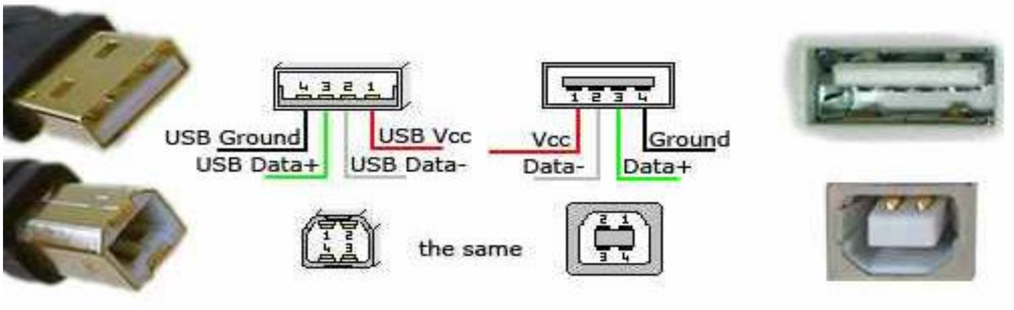


**Figure 3: USB Pin Configuration**

### 1.1.3 USB Flash Drive

A USB stick is simply a plug-and-play storage device which stores data in flash memory and since Flash memory is non-volatile and can be reprogrammed and erased electrically. Thus, it is essentially an electrically erasable programmable read-only memory, commonly known as EEPROM. The USB sticks are commonly employed for convenient and speedy transfer and storage of information.

A USB stick can carry any sort of data such as backups, important files, executable applications and it can even carry one’s favorite settings. Moreover, it is also suitable for running diagnostics for troubleshooting computer problems and can even launch an Operating system from a bootable USB.

The below section mainly talks about the storage capacity and data transfer rates of the available USB sticks. It also covers the advantages, disadvantages and working of these devices.

- ***Memory of USB Flash Drives***

The very first USB stick with 8MB storage capacity was launched in the year 2000. At present, USB stocks come in storage capacities of up to 2 terabytes (TB), depending upon vendors.

- ***Evolution of USB Flash Drives***

**USB 1.0** was pioneered back in 1996, for replacing peripheral connecting interfaces and reducing the complexity of both software configuration and hardware. It had two versions: USB 1.0, which offers a 1.5 Mbps data transfer rate and USB 1.0 high-speed with a 12 MBPS data transfer rate. The issues in version 1.0 were later fixed in the updated version 1.1 that was released in 1998 and was more extensively used.

**USB 2.0,** commonly referred as Hi-Speed USB, was launched in 2000. This was developed by Compaq, Philips, NEC Corp., Microsoft, Lucent Technologies, Intel and Hewlett-Packard. This version offers an extreme data transfer rate of up to 480 Mbps, which was an enactment boost by up to 40 times than the previous version. USB 2.0 also offered enhanced peripheral support that was extended for including network adapters (particularly Bluetooth), CD writers, video cards and digital cameras. In addition, USB 2.0 actually boosted the popularity of flash drives that enable physical transfer of data on the go.

**USB 3.0,** referred as SuperSpeed USB, was launched in 2008. It was developed for reducing power consumption and increasing the data transfer rate. A 10 times increase in data transfer rate was seen from Hi-Speed USB to SuperSpeed USB, which reached up to 5 Gbps. USB 3.1, recognized as SuperSpeed+, was introduced in July 2013. This version particularly amplified the rate of data transfer as compared to previous versions.

- ***Working of USB Flash Drives***

USB flash drives have attained considerable attention in this era of computer technology. The major elements of a USB flash drive include a crystal oscillator, a NAND flash memory chip, a USB mass storage controller and a male type-A USB connector. The USB connector serves as a line between the computer and the device. The mass storage controller has a small RISC processor and some on-chip memory, which can be RAM and ROM. The main task of data storage is done by the flash memory chip and crystal oscillator which generates clock signals and controls the data transfer of the device.

- ***Pros and Cons of USB Sticks***

The several advantages offered by these tiny, yet effective devices are as follows:

- USB sticks are portable and lightweight.
- These devices are robust and can withstand dust, scratches and mechanical shocks. These are not affected by magnetic fields and are generally waterproof.
- The flash memory is non-volatile, thus data can be retained on USB flash drive for a long time period
- These are simple plug-and-play devices, which makes these a user-friendly and convenient ways of transferring data between computers.
- These sticks also do not need any external power supply or batteries to do their job

Apart from the above-mentioned advantages, there are a few downsides of these devices:

- The main limitation of the USB flash drive is its ability to handle a limited number of write cycles before it flops.
- The USB flash drive can be lost easily due to its small size.
- Data leakage is the main concern since these drives are hard to track and portable
- A security breach could occur if the USB device is infected and is then plugged into a system.

### 1.1.4 Risks Associated with USB Flash Drives

Technology has witnessed substantial developments in the past few decades from floppy disks to flash drives, CRT to LED monitors and many others. These technological advancements have offered numerous improvements, which have come at the cost of several security risks; for instance, the existing USB devices, on one hand, have successfully replaced several PC connectors, addressed the usability issues of current interfaces, and enabled higher rates of data transfer for external devices. However, on the other hand, the insertion of personal storage devices (digital camera, USB drives, and other peripheral devices) into the PCs for uploading data (music, photos, wallpaper, etc.) over the internet could turn out to be a major security threat (Walters, 2012). The user may have innocent intentions, but this can put the data into a considerable risk by exposing the host devices to malicious files.

Generally, there can be up to 8 USB ports in a standard corporate PC, some of which are needed for peripherals like security token reader, mouse or keyboard. However, there are typically one or more unused ports usually left behind (Walters, 2012). An organization might opt for disabling the USB ports by means of ADM template (typically employed by system administrators for applying group policy changes within a Microsoft Active Directory environment or on a single machine for security purposes) and Windows Group Policy (explained later). But in both cases, the administrator, unfortunately, does not get the requisite granular control through this. So, it becomes nothing or everything, i.e. at an endpoint, either all the USB ports are entirely available or completely disabled (Walters, 2012). Since most of the endpoints have mandatory USB port requirements, thus this control will serve as an ineffectual idea.

An alternative to this involves the insertion of epoxy glue in USB ports that are unused. Here, epoxy glue is a type of glue that is best at filling gaps between parts and has tremendous structural strength. The advantage of this approach is its simplicity and cost-effectiveness. But the chances of fire, electric short and long-term computer devaluation are the main drawbacks associated with epoxy glue usage (Moskowitz, 2006). Thus, it is hard to imagine risking it all, causing permanent damage to possibly costly business equipment. Certain vendors also try to sell the plug-in USB locks for securing the unused ports from being prone to risks like data leaks (Bem & Huebner, 2013). But this approach does not stop the user to unplug an existing USB and insert an illegal storage device in replacement.

However, it is quite impossible to ban the use of USB storage devices since countless benefits are offered by these (Tetmeyer & Saiedian, 2010). Thus the practical approach is to examine the risks associated with using USBs, as discussed in the following segments, and come up with a solution to counter threats and enhance security. The primary security risks in using USB storage devices include:

- ***Malware Propagation***

Malware propagation by means of USB devices has posed a serious security challenge since it is quite difficult to detect and contain it (Tian, Bates, Butler & Rangaswami, 2016). The more threatening part of this risk is that the user might not be able to realize that his computer has been infected by malware. At present, security companies have reported a rise in malicious applications that use USB flash drives and other removable media as a propagation method.

In fact, there was a virus outbreak that forced the US Army to go ahead and ban the usage of USB storage devices in the year 2008, when a variant of the SillyFDC worm called Agent-BTZ beset the Army. This attack turned out to be the worst breach in the history of US military security (Shachtman et al., 2008). Agent-BTZ is mainly a computer worm that infects USB flash drives with spyware that spreads by copying itself to flash drives, using the following commonly employed propagation methods:

- *File copy approach*

In this technique, a malicious application installed on a contaminated workstation makes copies in shared networks, local drives and even on every storage device connected with the infected system. The malicious file is mostly titled as an exciting filename for luring a victim to launch the file, which then causes the execution of malicious code. Once the malware gets into the system, depending on how it's written, it can then also access the address book from the computer and can easily spread the virus further by automatically sending emails to all the contacts in the system

- *AutoRun.inf modification method*

The operating systems including Microsoft Windows have a functionality known as "AutoRun" (at times called Autoplay). This functionality is mainly designed for performing several actions that are executed automatically upon insertion or removal of removable media from a computer. In this method, an AutoRun.inf file is created on every available drive, which makes the data vulnerable. So, when an affected USB is inserted into another PC, malicious software starts automatically even without the user’s knowledge.

- ***Data Loss***

USB drives come in various sizes and shapes with tremendous data storage capacity. Although these devices can store and transfer data quite easily, the stored data is prone to be compromised (Network Management Solutions, 2014). All one needs to do is connect the USB device with the target machine and get all the required data such as credentials, browser history, etc. In addition to this, the loss or theft of a USB storage device can also result in the disruption of company reputation.

- ***Hacking***

A very important feature of USB drives is that they can serve as a "PC on a stick", making use of specific utilities and platforms like BartPE/PeToUSB (application for formatting and making bootable USB), UNetBootin (allows one to create bootable Live USB drives for Linux distributions, Mac and Windows without burning a CD) and UBCD4 (a bootable recovery CD containing software employed for diagnosing, restoring, or repairing almost every computer issue). But this feature permits the hacker to replicate the entire windows with the help of a simple USB (Network Management Solutions, 2014). When the malicious user is done with such activity, he simply disconnects the USB device and there will be no traces of such activity on the computer.

Similarly, certain terrorist groups use encrypted communications software on a USB device. One scenario could be, a terrorist visiting a cyber cafe and connecting his USB device that contain software like ‘Mujahideen Secrets 2’ and using this, he can then send files, emails, or do chatting using military-grade encryption (AES-256). Now, all it takes is to simply unplug the device and no trace will be spotted where the fraudulent activity took place unless you do some digital forensics on it (Bem and Huebner, 2013).

- ***USB-based Attacks***

Some of the organizations have banned the use of USB sticks since along with the previously discussed threats, USB flash drives also have the potential of being employed as hacking tools. In recent years, an insidious type of USB-based attack has emerged known as BadUSB. A BadUSB can register itself as different types of devices for carrying out covert actions on the host system.

One such type of USB is USB Rubber Ducky, also known as Rubber Ducky penetration testing tool. USB Rubber Ducky was launched by Hak5 and it includes an SD slot and a 60MHz programmable microcontroller. The USB rubber ducky is a keyboard emulator disguised in the case of a USB stick. This has been used by hackers, pen testers and IT professionals since 2010 due to its covert design, formidable hardware and simple scripting language. Apparently, it looks like an innocuous USB stick, but it is registered as a USB keyboard once plugged into the system and fires off a keystroke payload at lightning speed. It only takes a few minutes for malicious hackers to steal usernames and passwords with the help of USB Rubber Ducky. However, physical access to the target system is a major requirement for using USB Rubber Ducky. Furthermore, one also needs to write malware to be injected into the device.

One more such type of device is USBdriveby, which can be worn even around one’s neck. It has the capability of covertly and quickly installing a backdoor for overriding the DNS settings of any unlocked device in no time. The applications that are launched using USBdriveby can evade local defense, such as IDS or firewall, and can alter DNS settings as well. Moreover, no additional permissions are needed by these applications and the actions performed by them are also neither detected nor blocked by the machine (Bem and Huebner, 2013).

Another major type of threat associated with USBs is a USB keylogger. A USB keylogger covertly logs every single key pressed on the keyboard. It has the potential of capturing credit card numbers, passwords, personal messages, emails and everything else typed by the victim. A Keylogger can be installed by anyone having access to the system and malicious intent. USB keyloggers are sometimes also regarded as a type of malware. This is because they can covertly run in the background and capture any data for as long as they can evade detection.

Another notorious device is USB Killer that appears to be a USB flash drive but sends high-voltage power surges to the host device. These powerful surges are a subtle threat to the system hardware. These devices are basically designed for testing components for protection against electrostatic discharge and power surges. However, these can be employed by attackers for destroying the internal circuitry of the targeted system.

## 1.2 *Past Works in USB Security- Literature Review*

Data is quite easily and efficiently transferred via USB flash drives, but the popularity of this USB interface has led to substantial security concerns (Detwiler, 2003). For instance, a simple computer is used for storing extremely confidential business data and anyone having access to that system can easily copy the data through a USB device, and the job becomes easier in the absence of an access control mechanism. Therefore, the design of a secure access control mechanism is crucial for preventing data leaks and protecting the confidentiality of data. The authentication process is employed in several past studies and is found to be a preferred security measure. Generally, human authentication can be done based on three factors, i.e. what one knows (password), what one has (physical asset, such as storage device) and who one is (biometric).

Multi-factor authentication schemes are also employed for security purposes, which involves more than one factor (out of the three mentioned above) for authenticating users (SolarWindMSP, 2016). In this case, the user is required to authenticate himslef with at least two different factors. These factors can be the password (something one knows), a card (something one has) or biometric (something one is) depending on the process requirement. This makes quite tricky for the person with malicious intent to bypass multiple authentication factors simultaneously (Zorouni, 2006).

In 2010, Yang, Wu, and Chiu came up with a two-step protocol that involved a multi-authentication process for USB Security System. The protocol put forward by (Yang, Wu & Chiu, 2010) consisted of three phases:

***The Setting of System Environment:*** For effective control of data transfer through USB interface between the USB storage device and computer, any user wishing to transfer a file from (to) storage device has to first acquire approval of the authentication server ‘AS’. After that, the user is permitted to transfer data using the USB interface. During the user verification process by AS, a session key is shared between AS and user for encrypting all the transmitted files, in order to protect the confidentiality of all files saved on USB devices. Here once the transmission is ended, the access to USB is restricted again until the next successful authentication is done. Furthermore, the same authentication process has to be followed for decrypting the encrypted USB data through the acquisition of the shared session key (Chen, Qin, Yu, 2012). Moreover, upon completion of the file encryption/decryption process, the shared key is removed as well for ensuring the system security.

***Registration:*** Every user is required to first register himself at the authentication server. This is a fundamental step for becoming an authorized user and acquiring the license of system access through a USB interface.

***Authentication and Encryption of Data:*** Every time a user wants to access USB ports, he must provide his credentials (identity and password) for getting verified from the server (Yang, Wu & Chiu, 2010).

In this scheme, any successful authentication requires the users to simultaneously provide the right password and details of their storage devices. For obtaining a protocol of better security control for USB storage devices, (He, Kumar, Lee & Sherratt, 2014) they came up with a 3-step authentication scheme. This involved biometrics, password, and storage devices from the user. The scheme presented by (He, Kumar, Lee & Sherratt, 2014) included an additional step of biometric verification, which is intended to enhance the protocol security. This step also involves the exploitation of XOR and elliptic curve cryptosystem (ECC) operations for increasing protocol efficiency. However, (He, Kumar, Lee & Sherratt, 2014) protocol is not able to withstand a replay attack and the password guessing one, which is a backlash here. Further, the multiple factor security protocol at the user-level made it hard to copy or share data, considering the strong and irrational assumption. Essentially, this assumption violated the security description of the three-factor verification system. Thus, this protocol failed in achieving three-factor authentication, and is not deemed to be a practical and effective authentication method for USB data storage devices.

To put it short, the literature review showed that there is room for research in the field of USB security along with the development of an ideally secure USB monitoring system and some strong policies should also be devised for ensuring the safe use of personal storage devices.

## *1.3 General Steps for Securing Personal Storage Drives*

According to the findings deduced from literature, the following main steps can be taken by every organization for optimally securing personal storage devices, both off and on the network.

- Identify and announce the organizational policies for personal storage devices
- Whitelist the approved storage devices
- Ensure the complete encryption of devices
- Ensure that the users do not dodge security measures
- Maintain data logs
- Ensure there is a recovery/backup for all the data, where the data backup idea is applied to all the personal storage devices
- Have a comprehensive plan for controlling the use of removable devices within the environment
- Manage USB drives issued by the company

## *1.4 Attributes of a Typical USB Security Solution*

The following key attributes of a typical security solution have been identified through the available content on USBs and to design any successful application or policy related to USB security.

- ***Locations***

The policy set must include the implementation of the varied location-dependent set of rules for using the USB port. Whenever the laptop or computing devices are at some riskier space, for example, airports or restaurants, then such policies would be of great help for restricting access to important data if the device gets stolen or misplaced. For instance, if the device is within the authorized location, then the user might have read-write access, but will not be granted write access outside the defined premises to ensure data integrity.

- ***Data Logging***

The USB Security solution should have strict policies for keeping a track of policy enforcement actions. The policy must have an appropriate solution to be active in case of suspected attack or any attempt of unauthorized access (Scharmatinat, 2015).

Such a tracking process is crucial for not only tightening up the security solutions but also for keeping the organization in sync with data-control and privacy rules specified in Government approved rules and regulations. The admin must have the audit information such as the user who transferred the data to a USB, the amount of data transferred and the kind of files that was transferred. When there is a data breach, this information will facilitate the organization in finding out where and by whom the breach happened.

- ***Control and Limit***

USB devices can have limits according to the role of the user within the organization. For example, an employee belonging to one department might not need certain executable files belonging to a different department. In such a case, these files can be blocked and verification can be done for avoiding copying of such crucial data (Scharmatinat, 2015). Some unexpected threats can be prevented if such strict policies are followed.

- ***Protection against Malware***

The organization can make sure that all USB devices are thoroughly examined for any malware before providing system access (Scharmatinat, 2015). A separate malware scanning station can be established for scanning USB drives, before their connection with the corporate network.

- ***Disable Autorun***

This feature automatically causes any removable media like USB storage drives to access the file and run the executable program when they are plugged into the USB port. If this feature is disabled, the entry of some malicious code via the USB drive can be prevented.

- ***Educating Employees***

Many times, employees put the organization at risk because of ignorance. For the implementation of a strict USB Security control system, it is essential to offer regular training to the employees regarding the security practices for USB usage (Misra & Dubey, 2015). This will assist both employees and management staff in extracting the maximum benefits of USB sticks, without facing any major security issues.

## 1.5 *Existing USB Security Systems*

In large enterprises, central device management is often employed for managing controlled access to USB devices. Such a structure either requires an on-premises server configured as a domain controller or a centralized Azure cloud service with configured Azure Active Directory. In these cases, the servers and workstations requiring access control to USB attached storage are centrally managed using domain accounts and must be either member of the Windows domain or members of the Azure Active Directory with Microsoft InTune primed for hardware management. Following are the most commonly used methods in most of the currently employed solutions:

1) Hardware designed using binary decision approach, in which all USB storage devices are either allowed or denied
2) Hardware employing whitelisting with respect to the manufacturer, where USB storage devices made by a specific manufacturer(s) are allowed only
3) Hardware-based on whitelisting by attribute, where USB storage devices with specific serial numbers, model numbers, or hardware encryption are allowed
4) User-based classification, wherein the presence of any of the above-mentioned hardware profile only users having privilege profile or certain role are permitted the usage of USB storage devices.

Encryption capability is also found to be a key requirement in most of the current security solutions since several regulatory and legislative requirements require the encryption of sensitive data. Data encryption is known to be the safest way of protecting confidential information. During encryption, the sensitive data or information is converted into an indecipherable code while in storage or transit. This averts any illicit access from harmful third-parties and facilitates in achieving confidentiality, which is one of the three main pillars of information security. The encryption of data on mobile devices, hard drives, computer and USB flash drives will prevent the data misuse, in case the device is stolen, lost or hacked.

Keeping this fact in view, hardware encryption is incorporated by several USB storage device manufacturers in their devices. The big giants, Apple and Microsoft, have also provided their users with the option of encrypting data on USB storage devices. However, this feature was not available when they rolled out their native full disk encryption solutions. Besides that, there are a number of third-party software solutions that sense whether a USB storage device is encrypted and capable of supporting encryption.  In such a scenario, the third-party solution can be configured to force encryption of the data as it is being written to the USB storage device.

Nevertheless, there are few limitations in all the above-mentioned approaches for USB security. The binary decision approach in (1) is not a practical approach, as it can either permit access to malicious users or block access for authorized ones. In the next methods (2) & (3), the user is bound to get a USB drive of a certain specification, which makes it somewhat unfavorable approach from the user's perspective.  The last approach (4), where users having certain privileges or a specific role are permitted the use of USB storage devices, appears to be quite tricky from the management perspective. Since here, the managers must keep an extensive record of users, their roles and the privileges offered to them. Therefore, such a solution is needed that could be installed on a workstation and involves user-based authentication for controlling access and use of USB ports.

## *1.6* ***Problem Statement***

USB has been invented for replacing various PC connectors, which address the usability problems of available interfaces and streamline configurations of device software. USB has also facilitated higher data transfer rates for external devices. However, with the evolution of USB devices, predominantly flash drives, the security risks and threats associated with them have also evolved. The available solutions fail in providing complete security against the outsider and insider attacks, and all the USB ports are either enabled or disabled in most of the existing solutions.  Moreover, the techniques opted in the past are not easy to use, either too complicated/ impractical or very difficult to manage, and thus not been successful in combating the security threats completely. This project specifically targets this issue and will come up with a practical, user-friendly and reliable security solution. The proposed solution will facilitate both individuals and organizations in the secure usage of USB ports and data storage devices.

## *1.7 **Report Layout***

This project report has been divided into 7 main chapters. The first chapter provides an introduction to the main concept, discusses the past efforts done in this regard and develops a basic understanding of what the report is all about. The second chapter identifies the key operational requirements for developing an effective USB security solution. In the third chapter, a comprehensive analysis of existing USB security solutions is done and the limitations in existing solutions are identified. This is to highlight the need for an improved USB security system that could overcome the shortcomings in the existing approaches.

Chapter 4 is the key chapter, which talks about the proposed solution and presents the prototype, architecture and complete working proof of concept. In the 5th chapter, the in-depth analysis of the proposed concept is carried out, which involves a comparison of the presented idea with the past solutions, risk assessment and a mention of advantages and limitations of the prototype. This is followed by a conclusion and future recommendations, which make the 6th and 7th chapter of this report respectively. The final section covers the bibliography and appendixes.

# 2. Identification of Operational Requirements for USB Security Solution

Large-scale data and security breaches due to USB storage devices are reported quite frequently, which have a devastating impact on the involved individuals and organizations. In response to the escalating cybersecurity threats, regulatory bodies across the world are increasing pressure on organizations for the protection of sensitive data. Thus, the organizations are looking for an ideal USB security solution based upon the three key pillars of effective security strategy, i.e. confidentiality, integrity and confidentiality. The primary operational and security requirements for an ideal USB Security solution are identified in this section, by taking some help from the NCSC guidance Leaflet (Provided in Appendix B).

The USB security solution must be able to fulfill the following major operational requirements:

- Unfailingly identify the user requesting access to the physical USB port (s) without relying on normal system authentication
- Authorize the user for carrying out one or more of the following activities on storage devices attached to the physical port:
    - read – read or copy data on the device attached to the host workstation
    - write – write new data or modify existing data on the attached device
    - execute – execute applications that may exist on the attached device without the need of modifying host workstation
- Perform the above activities with no constraint of central directory service or a persistent network connection between client and server
- Record the events related to operations of the application and stores them into a protected log file on the workstation including the following:
    - login/logoff success and failure of application super-user
    - use of high privilege success and failure
    - success or failure of user creation/modification/deletion process
    - authentication success and failure
    - authorization success and failure
    - read/write/execute operation success and failure
    - application start-up
    - application shut down

- Create alerts that can be communicated to an application administrator based on information recorded in a configuration file.  Alerts should also be written to a log file together with other significant events of the following occurrences:
  - Application superuser login failed attempt
  - Use of elevated privilege success and failure
  - User creation/modification/deletion success or failure
  - User authentication failure
  - User authorization failure
  - Read/write/execute operation failure
  - Application start-up success and failure
  - Application shut down success and failure

Moreover, the solution must use some sort of technique that only detects the insertion of storage devices and asks for authentication; ignoring the insertion of input devices, like keyboard and mouse, etc. through USB ports. Another major requirement for the successful implementation of the USB security system is to emphasize the blocking of USB ports instead of only blocking the USB flash drive itself. The reason being, USB ports allow connection to USB drives for transferring data within devices but at the same time, these ports expose the systems to potential loss of important information and introduction of viruses. Therefore, the controlled use of these USB ports could be a supplementary protection layer, which can considerably reduce security breaches without hampering the productivity and flexibility needs of a company.

Moreover, each USB flash drive must be scanned by an AV for any threats or malware, before any user interaction with the USB is happened. This is an essential requirement for protecting the system from malware threats and viruses, which can effortlessly sneak into the system through a USB flash drive insertion. In addition to this, several kinds of USB management software should be employed for controlling the transfer of data. Such software must be able to run on any operating system and should have the ability to control computers remotely. The security system must also be able to counter USB threats immediately even without an internet connection.

In a nutshell, an ideal USB security solution must be designed that fulfills all the above-discussed requirements. Moreover, in the case of disabling the use of USB storage devices, the use of USB keyboard, printer and mouse should not be affected.

All the major requirements for an ideal USB security system, which have been shortlisted in this chapter, are summarized as follows to be used as a reference in the coming chapters.

**Table 1: Summary of Operational and Security Requirements**

| S.No. | Essential Requirements of Ideal USB Security System |
|---|---|
| 1. | To authenticate every user that tries to access USB port |
| 2. | To authorize the user for carrying out read, write or execute functions |
| 3. | To log all the event details |
| 4. | To send alerts to the administrator regarding any unusual activity |
| 5. | To verify only USB devices and not the non-storage ones (mouse, keyboards, etc.) |
| 6. | To block USB ports and not the USB devices |
| 7. | To provide support to different operating systems |
| 8. | To scan the USB device by an Antivirus software |

A novel idea for a USB security system will be presented in the following chapters, by keeping in view these operational and security requirements. Moreover, these requirements will be used later to analyze the existing USB security solutions and to verify the practicality of the proposed solution.

# 3. Analysis of Current Market Solutions for USB Security

Considering the previously mentioned operational and security requirements for an ideal USB security solution, this section reviews and analyzes the currently employed solutions for controlling the access and use of USB storage devices. This section also identifies the shortcomings of existing applications and highlights the need for a new solution in light of these shortcomings.

## 3.1 *Microsoft Stand-alone Workstation Group Policy*

Microsoft Group Policy is an attribute of the Microsoft Windows family of OS, which controls the user and computer accounts. This policy provides centralized design and management of OS, user settings, and applications within an Active Directory environment. Local Group Policy is a version of Group Policy that permits Group Policy Object management without Active Directory on standalone computers. This local group policy application can be used for controlling access to USB Ports and attached storage devices on stand-alone workstations. The group policy options can apply controls at both hardware levels and user-level. Presently, there are various built-in Group Policy controls, which can facilitate an administrator in controlling removable media access and restricting the installation of new removable devices (Moskowitz, 2006).

For the management of group policy settings, the administrator is required to be a member of the Local Admins and must be authenticated to the workstation using local credentials or Microsoft personal credentials. It is possible to add individual users to the workstation in the same manner. Users must also be authenticated to both the workstation and the application. Once the users are added, the administrator has to use local computer management for ensuring the presence of users in the Local user group only. Audit policies on the stand-alone workstation keep a check on the events being generated and if they are written to the appropriate event logs on the workstation.

A detailed procedure for blocking Removable Media and USB drives using Group policy is provided in Appendix A (Section 1). The group policy settings have presently become more comprehensive compared to those in the past. However, they still fall well short of what might be considered a true security control for USB ports. Only a few aspects of port usage are controlled by this policy and there is no comprehensive protection strategy for providing security and flexibility. Moreover, Group Policy is an effectual configuration control, but it is not possible to rely upon it for crucial security control.  As the attackers with knowledge can easily overcome the protection attributes of Group Policy.

## *3.2 Microsoft Windows Domain Active Directory*

The creation and management of controls for USB storage devices and physical USB ports in an on-premise domain are the same as discussed above for a stand-alone workstation. Although, the key difference is that here group policy management for hardware and users takes place at the domain controller and at the forest root domain controller (if applicable). In this scenario, both the workstation and the user must be members of the Windows domain.

The Domain Administrator configures and manages USB port and device controls at the domain or enterprise level, through these group policies.  While group policies are inherited, more restrictive group policies at lower level branches of the tree can override those of the domain or the enterprise (Bruzzese, 2016).

In this case, the administrator is only required to get him verified within the domain and is also provided access to the group policy editor.  The physical USB ports of the workstation are controlled through the hardware-specific group policy options. The users accessing the particular workstation, where the controls are in place, will authenticate to the domain and are controlled by the user-specific group policy options. The audit policies here determine the generated events, which are stored on each workstation and collected by the domain controller at the domain level or forest level, as appropriate.  The control of the port and user-based activities on the workstations within a domain/forest has the same weakness as the individual workstation, as far as flexibility or granularity is concerned.

## *3.3 Microsoft Intune*

It is a cloud-based mobility management tool for helping organizations in controlling mobile devices that are employed by users for accessing corporate data and applications (Eby, 2019). The working of Microsoft Intune is quite similar to the Windows Domain model.  It was developed by Microsoft for providing a solution for controlling mobile devices via Azure Active Directory. The configuration for restriction settings of devices in Microsoft Intune is included in Appendix A (Section 2).

These devices can be administered by using stand-alone application or group policies applied through Azure Active Directory membership, as well as the In-Tune capabilities available through Microsoft 365 E3 and higher.  Organizations with Office 365 can procure the same capabilities through the addition of Microsoft's Enterprise Mobility + Security Suite. The features and capabilities available through Intune are the same as those available for workstations in an on-premise Windows Domain. Intune has the ability to protect on-premises data and email so that the mobile device can access them safely. Microsoft Intune provides the option of denying "write access" to the removable data drives that are not protected by BitLocker. The USB drive will be mounted as read-only (Sabhi Haider, 2018). The link to the policy of Microsoft Intune for disabling USB drives not being protected by BitLocker encryption is provided in Appendix A (Section 3).

Windows Defender ATP allows installation and usage of only specifically approved peripherals by creating a custom profile in Intune and configuring DeviceInstallation policies (Justinha & Chen, 2019). With this rule, admin can prevent or audit unsigned or unreliable executable files from running through USB removable drives, including SD cards. The technique of controlling USB devices through Windows Defender ATP is comprehensively given in Appendix A (Section 4).

## 3.4 *Symantec Endpoint Protection – SEP*

SEP is an endpoint protection application, known primarily for its protection against malware and ransomware attacks. Moreover, this application can control access to attached USB storage devices using either the hardware-based scheme or user-based scheme. In the hardware-based scheme, the allowed devices are generally whitelisted based on the manufacturer and device ID. While in the user-based scheme, the user is permitted to access USB devices and perform certain operations based on the user's group membership (Fossi, Egan, Haley & Johnson, 2014).

Deployed as an on-premise solution, SEP offers unified management across virtual and physical platforms, with granular policy control for improved scalability and flexibility. The controls based on hardware remain incorporated with the machine, and the users interact with USB attached storage as per the attributes assigned to that USB device. For instance, if a USB stick manufactured by PNY with device ID 123 is only allowed read access on a particular PC, any user (including a privileged user) will be limited to read access on that device when attached to that particular workstation. On the other hand, if a domain administrator has a USB stick that he carries around to collect information from local event log files, then user-based control should be implemented and the authority to write to that USB stick will travel with the domain administrator, regardless of which system he logs into.

The detailed procedure of blocking or allowing particular devices in SEP through Application and Device Control (ADC) is given in Appendix (Section 5).

## 3.5 *USB Lock RP*©

USB Lock RP is a real-time, on-premises application offered by Advanced Systems International, with the purpose of providing central management, monitoring, and blocking of USB access to computers within the network. The key objective of USB Lock RP is to offer advanced USB lockdown for protecting window endpoints due to data loss and malware, by limiting unauthorized wireless adapters, portable devices and removable drives (Arrospide, 2019).

This application only works with Windows devices and works in either a physical LAN or Wireless LAN environment. Moreover, it offers protection to windows servers and workstations in business computer networks that store sensitive data. Whitelisting is used to authorize specific USB removable devices based on hardware ID. The system also works with USB over Network software for controlling access to USB devices on remote workstations or servers. The application can force any data written to an authorized device to get encrypted during the "write" process. Moreover, this application (discussed in Appendix A Section (6)) offers easy client deployment by means of Group Policy.

## 3.6 *Endpoint Protector*

Endpoint Protector is a suite of three products from CoCoSys aimed at addressing issues encountered by individuals and organizations. The products range from a standalone application (Endpoint Protector Basic) to a cloud-managed solution (My Endpoint Protector) to a fully functioned Endpoint Protector application. The fully functioned Endpoint Protector application contains multiple features supporting endpoint-based data loss prevention, mobile device management, and USB device control. All three have device control, logging capabilities and support Windows and MAC OS/X (Torbin, 2016).

The cloud-managed solution and the fully-featured application each can enforce encryption based on the content of the file being copied. Moreover, the fully-featured application supports MAC OS/X, Linux, and Windows.

In the fully functioned application, clients for Linux, MAC OS/X, and Windows systems are deployed from a central appliance that is available as a hardware appliance or a virtual appliance. The management application allows the administrator/superuser to control both USB ports and devices from a central location, as long as the devices are on the network. The management application is also available as an Amazon EC2 Instance.

USB port control is managed according to the physical attributes of each managed system. USB storage can be managed based on hardware ID, manufacturer or several other attributes. Furthermore, it is possible to employ whitelisting to restrict which USB devices can be attached to the managed system.

## *3.7 GFI EndPointSecurity*

EndPointSecurity from GFI is a Windows-based application that runs on both workstations and servers. The application is centrally managed and offers both event logging and alerting functionality. The application emphasizes on the encryption of data being stored on the USB stick. However, in the case of unencrypted data on a newly attached USB storage device, the user is asked by the application to create a password and use that for data encryption to get usage permission (Posey, 2011).

The EndPointSecurity management station continually monitors the local network for new computers connecting. Depending on the configured policies, the automatic detection can run at one of several preset intervals, and notify the administrator of any new systems. Again, depending on the policy, the application can automatically install an EndPointSecurity agent on the new system and apply a default policy to protect the new system going forward (GFI, 2008).

With the ReportPack, the application can generate various reports and statistics about USB attached storage regarding access events. Moreover, it can also create a list of file names copied to and from the network to the device, and most active devices. The application can apply group-based access policies based on Active Directory membership of the users.  It also generates alerts for certain identified activities and logs events to the central manager.  Both whitelisting and blacklisting can be configured to further refine access controls.

## 3.8 AccessPatrol

AccessPatrol application is developed and marketed by CurrentWare, and it only runs in a windows environment.  It is possible to set controls at the user level or device level. Access Patrol fundamentally has all the main control that other applications and processes for controlling USB attached storage have. Moreover, this application is centrally controlled and generates a number of canned reports (Currentware, 2019).

Although logging is done for collecting and retaining data that can assist in measuring activity levels over a time period, however, the events are not logged in a usable format. Moreover, no alerts are generated under certain conditions like failed logins in real-time or near real-time.

The application does have a couple of interesting features.  Policies are configured while the workstation is connected to the local network hosting the central manager stick with the workstation when it is not connected to the local network. Access to USB storage devices can be relaxed during non-work hours to allow employees to listen to recorded music or the like.

## 3.9 The Need for a New Solution

After reviewing the applications in the current market, it appears that none of these meet the security and operational requirements discussed in chapter 2. There is not a single existing optimal method for offering complete protection to USB under different circumstances. Some of the offered solutions are expensive or have a tricky implementation process and a few need extensive setups, whereas some cause damage to the system upon which they are implemented. A number of these controls considerably reduce the overall usability that results in unsatisfied users and long-term productivity loss. Consequently, there is a dire need for an innovative security solution that can fulfill the previously discussed operational and security requirements for a USB security system.

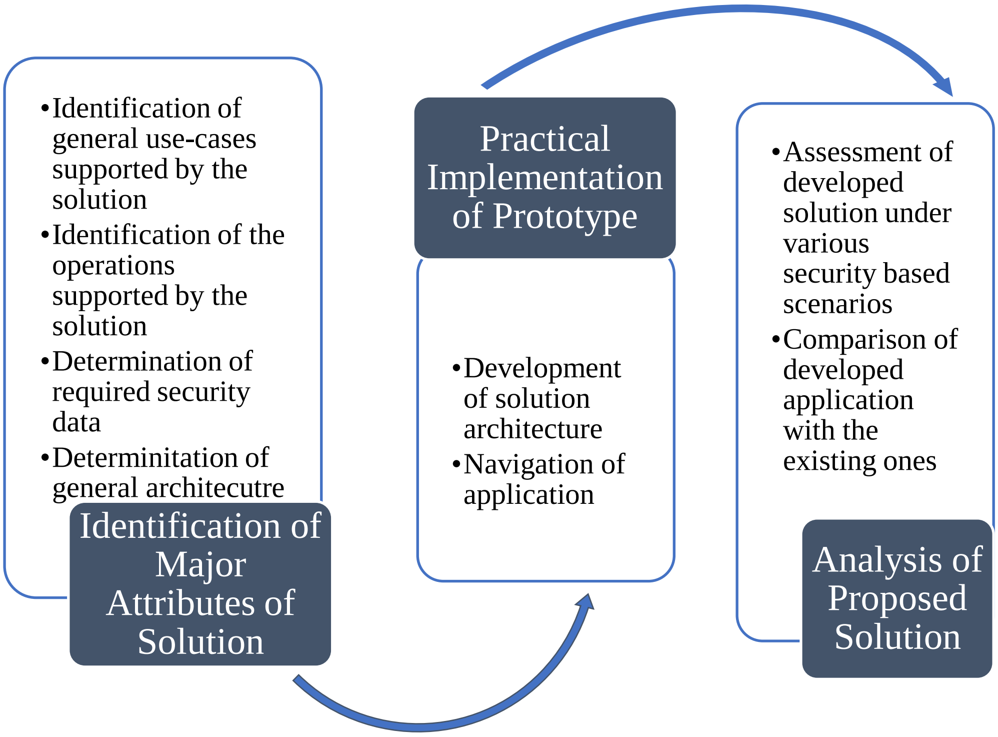
Through the solution envisioned by this project, the administrator can easily control selected workstations used by different users that have unique device access requirements. Additionally, the first iteration is intended to work on standalone devices without the need for a Windows Domain infrastructure. Future releases will be developed to support directory structures found in on-premise Windows Domains and Cloud-based Azure Domains.

This project will provide a more universal solution for Windows 8.1 and Windows 10 environments. Moreover, it does not depend on whether the machine is managed through a complex on-premise Windows Active Directory infrastructure or controlled through cloud-based Azure Active Directory and InTune. In the presented security approach, the USB ports are essentially blocked and will open once correct credentials are provided by the user to the controlling application. The proposed application will also determine if the authorized user can perform the read, write and execute operations, as per the permissions provided to them by the application admin and every user activity will be logged. The following chapter provides a comprehensive idea of the presented solution.

# 4. Proposed Solution

The extensive review of available literature and the study of existing USB security systems have highlighted the need for an improved mechanism for secure usage of USB flash drives. The USB security systems are found to be an essential element of organizational security, which facilitates in avoiding data theft while offering protection against the malware possibly injected through the users' USB sticks. Several USB security mechanisms are currently employed but none of these is efficient enough to fulfill all the major requirements identified in chapter 2 of this report. Moreover, the existing methods also have certain limitations in the case of insider and outsider attacks and theft/loss of USB flash drives, etc. Therefore, a novel mechanism has been devised that may serve as a productive addition in the domain of USB security. This chapter provides a generic overview of the proposed solution with emphasis on the flow charts, processes and measures that will be taken for achieving the proposed plan.

The theoretical evaluation of this concept is deemed essential at this point since it will facilitate in conceptualizing the study in a broader perspective. The proposed methodology is divided into three main steps as shown below:


•Identification of general use-cases supported by the solution
•Identification of the operations supported by the solution
•Determination of required security data
•Determininitation of general architecutre
Identification of Major Attributes of Solution
Practical Implementation of Prototype
•Development of solution architecture
•Navigation of application
•Assessment of developed solution under various security based scenarios
•Comparison of developed application with the existing ones
Analysis of Proposed Solution

- **Step 01: Identification of Major Attributes of Proposed Solution**

The initial step in this regard is to identify the general usage of the proposed solution, the operations/functions supported by it, the type of sensitive data required by the application and the general architecture of the planned solution.

This proposed solution will be aimed at offering a secure usage of USB flash drives and hindering any harmful activities or security threats associated with it. For this purpose, unlike the past approaches, the proposed solution will focus on blocking USB ports rather than USB devices, which is a key requirement of an optimum USB security solution, as discussed in section 2. It will also be made sure that the developed application only asks for verification if the user tries to access USB port for storage devices and allows them to use non-storage devices like mouse, keyboard, etc. without going through the authentication process.

The general architecture of the proposed solution will involve a local workstation with a user interface having the proposed application installed in it, and a remote server for monitoring the activities carried out at the user-end. The development will be done on the Windows platform (preferably Windows 8 or 10) and C# and C++ will be employed for programming different operations within the application. For efficient management of the system, the roles and privileges of both administrators and users will be identified at first. For the admin end, the application will be developed such that the administrator gets the authority to add or remove users from the database. Moreover, the admin will have the option of defining the privileges of every user for carrying out different functions (read, write, execute, etc.). Keeping in view the 2nd requirement of the USB security system, as identified in chapter 2, a proper database will be maintained for keeping a record of users and the permissions assigned to them by the administrator.

On part of the user, the application will require him to present his login credentials that include username and password. These credentials will be required every time a user wants to access a USB port for using his USB flash drive. The planned process for user-authentication has been depicted in **Figure 4**. Here, upon connecting the USB device with the host computer, the user will be asked to enter the login details that will be checked against the backend database, and once the right details are provided then the port access will be granted, else it will remain blocked in case of wrong login details. This step will be in compliance with the first major requirement of the optimum USB security solution (as mentioned in section 2), i.e. to authenticate every user that tries to access USB port. Moreover, for additional security measures, the users' passwords will be encrypted and hashed for ensuring the security of this sensitive information.

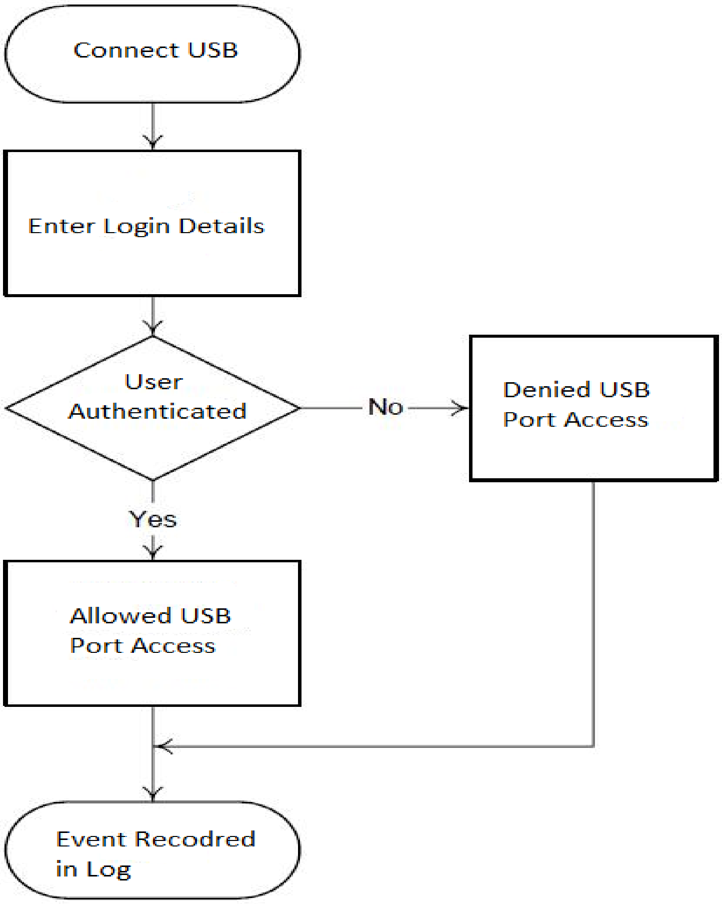


**Figure 4: User Authentication Process**

This step is further elaborated in the following sequence diagrams:

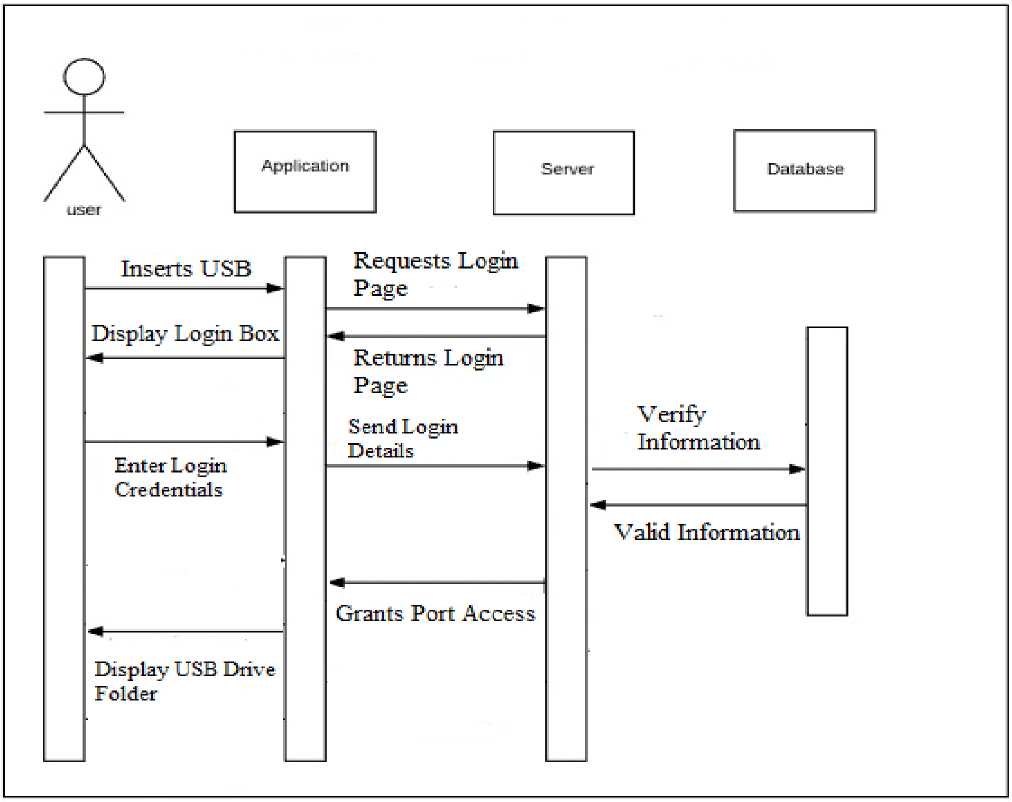


**Figure 5: Sequence Diagram for Successful USB Port Access**

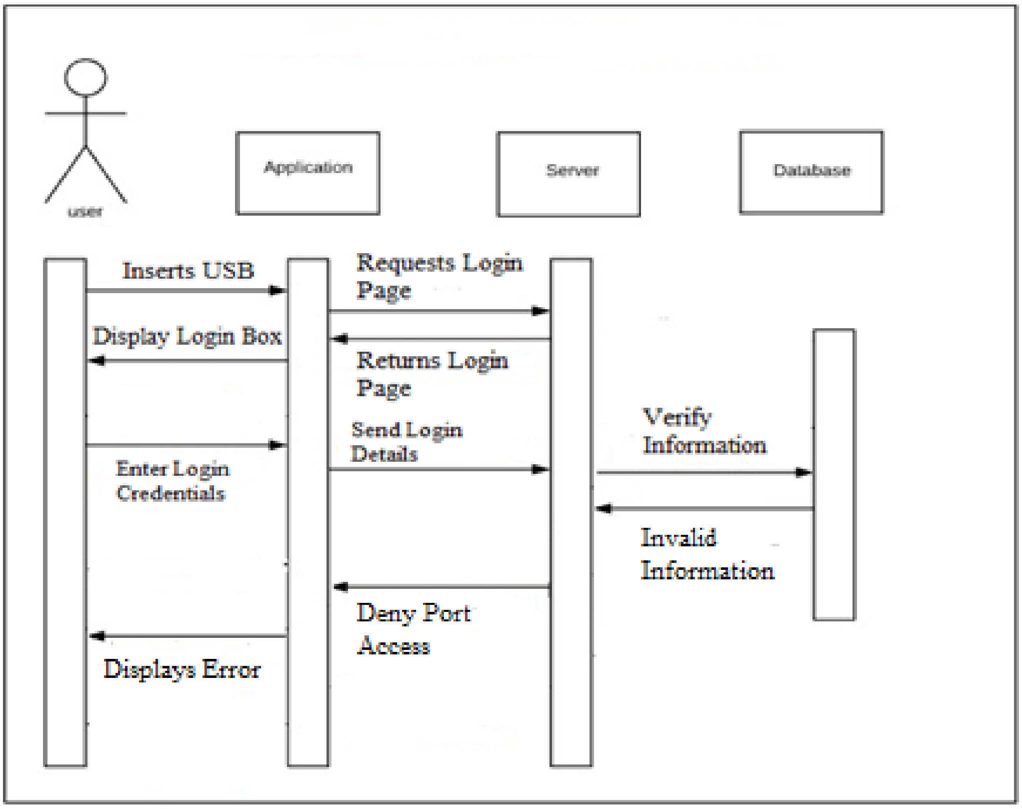


**Figure 6: Sequence Diagram for Unsuccessful USB Port Access**

After that, the next key requirement of the log management facility will be integrated into the prototype. Presently, log management has earned a substantial significance in security applications, as it helps in keeping a check on anomalies, errors or other suspicious activities that are deviated from normal. Such doubtful activities include unauthorized logins, password changes, malware detection, new user accounts, file name changes, etc. The application will also be integrated with an Active directory and centralized logging capability, e.g. SIEM, for enabling the administrator to view the runtime logs of different workstations in future release.  All the logs collected from different workstations will be sent to SIEM, which dumps syslogs from various workstations. These will be then sent to local log collectors which then pass it on to a master log collector. The master log collector will be used to categorize these logs into separate fields like username, time, authentication (failure, success), actions (read, write, execute) and eventID (which is unique every time). These categorized logs can then be seen by an administrator on the Web-front GUI of a SIEM.

This step will be followed by integrating the feature of generating alerts to the management regarding any suspicious activity taking place and then forwarding those alerts to a designated email so that the admin can carry out any countermeasures in real-time.

To put it short, the main operations of the proposed solution will be to differentiate between user and administrator privileges (ACL), to identify only storage device and then prompt the authentication popup followed by the password verification and granting/denying port access, and allowing activity depending on the privileges set for that specific user. The complete solution will involve a workstation within a domain environment so that multiple workstations can be managed accordingly. The application will be centrally installed on every workstation and a specific domain controller will house the event logs and the administrative console for the application on the domain. Here, all the activities will be centrally managed by the administrator for all the workstations, with no need of manually logging onto a workstation.

In a nutshell, an overall sketch of the implementation of the proposed solution will be as in **Figure 7**. This solution is expected to offer optimum security in case of an insider/outsider attacks, USB-based attacks and theft/loss of USB flash drives.

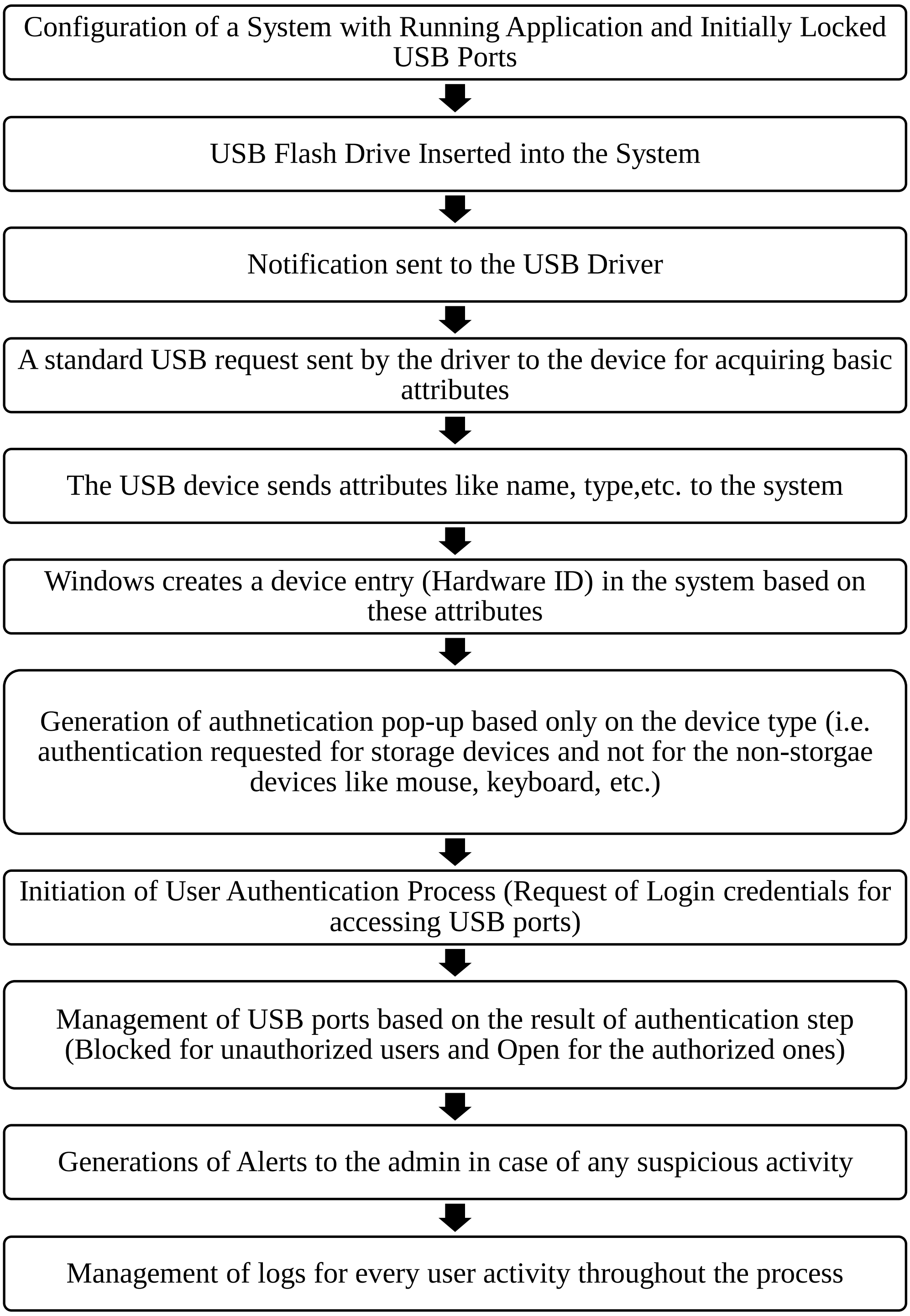

Configuration of a System with Running Application and Initially Locked USB Ports
USB Flash Drive Inserted into the System
Notification sent to the USB Driver
A standard USB request sent by the driver to the device for acquiring basic attributes
The USB device sends attributes like name, type,etc. to the system
Windows creates a device entry (Hardware ID) in the system based on these attributes
Generation of authnetication pop-up based only on the device type (i.e. authentication requested for storage devices and not for the non-storgae devices like mouse, keyboard, etc.)
Initiation of User Authentication Process (Request of Login credentials for accessing USB ports)
Management of USB ports based on the result of authentication step (Blocked for unauthorized users and Open for the authorized ones)
Generations of Alerts to the admin in case of any suspicious activity
Management of logs for every user activity throughout the process

**Figure 7: Flow Diagram of the Proposed USB Security Management Process**

- **Step 02: Practical Implementation of Prototype**

A general idea of the proposed solution has been discussed in this chapter that seems quite convincing, but the practical implementation of this idea is very much needed to determine the feasibility of its implementation on the chosen platform, to determine the required memory and to assess its speed and usability in real-time. Since it is quite tricky to predict the feasibility, performance and resource requirements of the proposed solution, therefore, a proof-of-concept will be implemented and discussed in this report. For the practical implementation, a number of technical attributes will be identified, which include information regarding the opted platform, programming interface, programming language, important dynamic link libraries, database, employed protocols, and chosen encryption techniques. These will be discussed thoroughly in the next chapter. Once the prototype is implemented, then a proper application navigation process will also be discussed in the coming chapter for easing the process for both users and administrators.

- **Step 03: Analysis of Proposed Idea**

After the successful implementation of proof-of-concept, a detailed assessment of the proof-of-concept will be done under various scenarios, considering inner and outer attacks, theft or loss of device and similar. Furthermore, the developed solution will also be compared with the existing solutions presented in chapter 3, on the basis of the operational and security requirements identified in chapter 2. This will be helpful in determining whether the solution is practically feasible, offers acceptable performance and fulfills the major security requirements or not.

# 5. Implementation of Proposed Solution

This section focuses on the practical implementation of the proposed application. It presents the prototype and architecture of the projected solution, followed by the demonstration of the developed solution.

## *5.1 Implementation of Prototype*

A prototype has been developed initially, keeping in view the operational requirements of the USB security solution, discussed in section 2. Proper local credentials have been assigned in the developed prototype so that they could be used in port management and user authentication process. Moreover, the application administrator has got several privileges, including user access control, enabling/disabling permissions, creation/deletion of users and keeping a check on logs, etc. Here the application users are the members of the local users' group and are validated by the workstation. In usual conditions, the application users must get verified first by the workstation and then by the application as well. However, this prototype has its own user list and authentication process and the presence of a user on a local workstation is not compulsory. The application will ask for verification every time the user tries to access the USB port.

Keeping the significance of data logging as mentioned in the previous section, the attributes of event recording, log management, and alert generation are also added in this prototype. All the events taking place are recorded and proper logs are maintained within this application which are then sent to a designated email address every 24 hours. In a real-world scenario, logs from different machines are stored locally and are transferred to the local agent of a log collector. Afterward, all the local log collectors usually send their logs to one point, where the administrator can view the logs mapped to different users and different machines. All these events are mainly logged in a file, which is located in the application folder of the user workstation and can only be accessed by the administrator.

## 5.2 *Solution Architecture*

This section highlights the key technical attributes of the implemented prototype and includes the navigation process for facilitating the users of this developed system.

### 5.2.1 Technical Details of the Proposed System

The total size of the developed end application package is only 1.2 MB, which contains some DLLs (dynamic link libraries used by the program for calling upon existing functions), actual application and backend database of users. This application size indicates the memory space to be occupied by the application on the host device. Considering the speed of the process, it takes around 5-7% of the process used when the application is running, which can be reduced further in the future release.

Following are the other technical details of the proposed system, including information about the employed encryption algorithms, programming language, database, protocols, functions and important files:

- **Operating System:** Windows 8.1 and Windows 10

- **Win32 API (application programming interface):** It is the set of functions used for creating and managing a user interface, giving access to computer resources, offering security, networking, incorporating graphics and multimedia, troubleshooting applications and monitoring performance. In this study, it is used for detecting USB insertion or any file changes. DeviceloControl, a Win32 API function, has been used for locking, unlocking and ejecting USB flash drives. While another important Win API function called a FindFirstChangeNotification function, is used for detecting file changes.

- **Programming:** C# language is used here for designing the GUI, so it is a must to have a corresponding .NET framework installed on the client's computer. The backend processes like encryption, USB plug-in detection, etc. are programmed using the C++ programming language. C++/CLI (C++ modified for Common Language Infrastructure) has facilitated in accessing the .NET framework within C++.

- **Backend.dll file:** This is one of the most important files for this application, which contains codes for asking passwords from users, ejecting USB drives, and sending logs to the admin email, etc. This file will be hidden in the program files directory as the installer installs the software (Note: The installer has not been created yet) and currently the file in not hidden.

- **Socket protocols**: In general, socket protocols assist in transporting application data from one system to another (or from one process to another within the same machine). Here, Socket protocols are employed in the proposed application for carrying out communication between client and admin applications.

- **Encryption:** AES 256 (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm, which is used here for encryption purposes. When information is sent by the client, the data gets encrypted and will be decrypted once it is received by the admin console. Elliptic curve Diffie-Hellman key exchange algorithm has been used in this project for trading passwords or keys for the encryption process. Moreover, BCrypt API is also used here for hashing (to transform a string of characters into a typically shorter key, representing the original string) and encryption purpose.

- **Database:** Newtongsoft's JSON library is used in this case for saving the credentials of users. The current database of the developed USB monitoring system contains UserID, encrypted passwords, and privileges offered to the users.

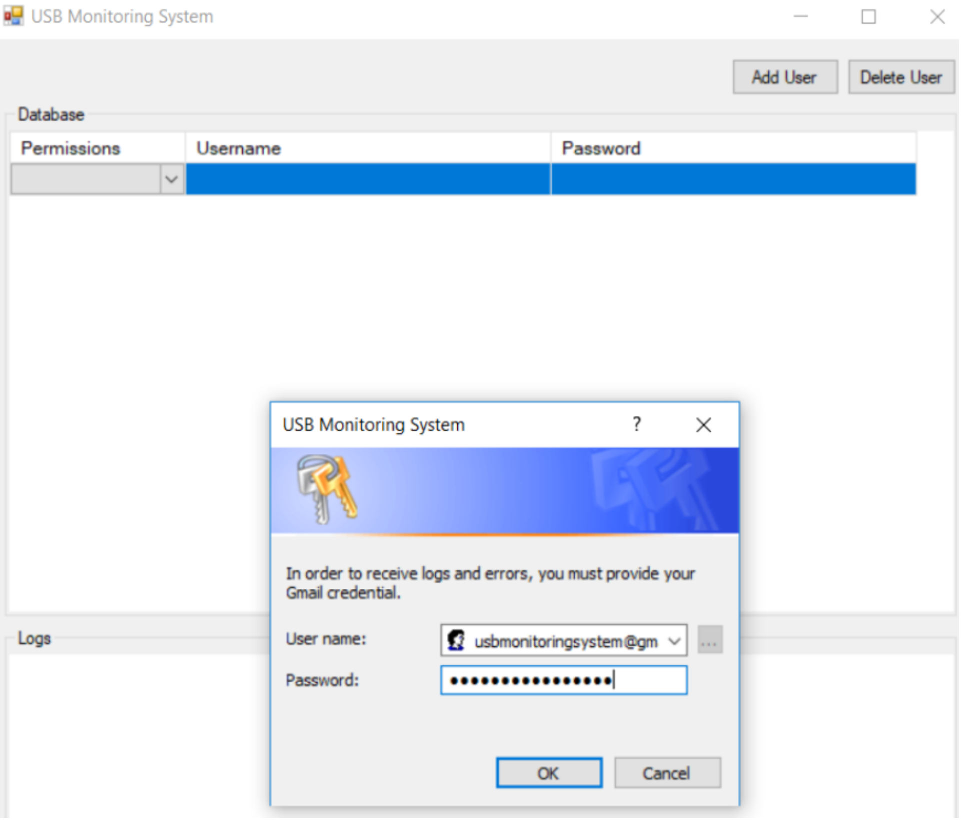
This prototype is solely applicable on Windows 8.1 and Windows 10 since some of the functions used in this application are only available in these two Windows operating systems.

### 5.2.2 Navigation of Developed Application

User navigation is usually the most important aspect of any application from the user's perspective as it determines a path that must be followed by users and administrators for doing each task. User navigation enables users to navigate into, across and out of the tasks and content pieces within the application. The user navigation aspect of this prototype is shown using the following screenshots of the developed application, with the perspective of both users and administrators

- ***Navigation of Application from Admin Perspective:***

The administrative user must first log into the application using his/her credentials, as in **Figure 8**.



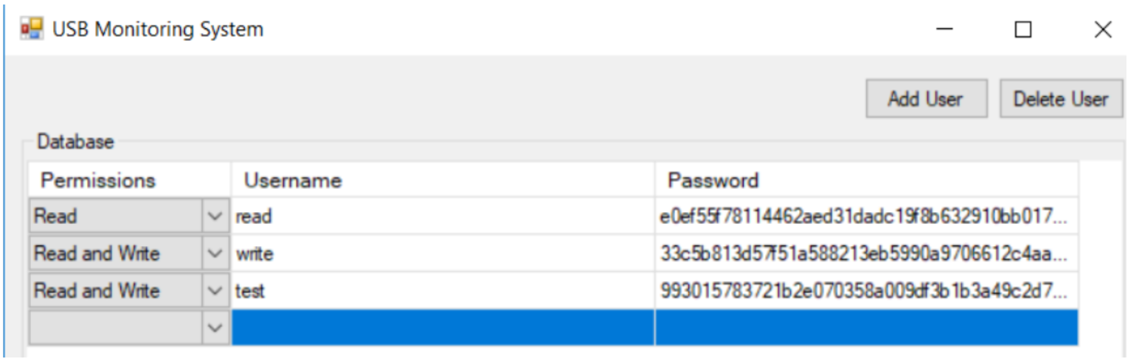
In order to receive logs and errors, you must provide your Gmail credential.

User name: usbmonitoringsystem@gm

Password: ••••••••••••••••

**Figure 8: Administrator Login**

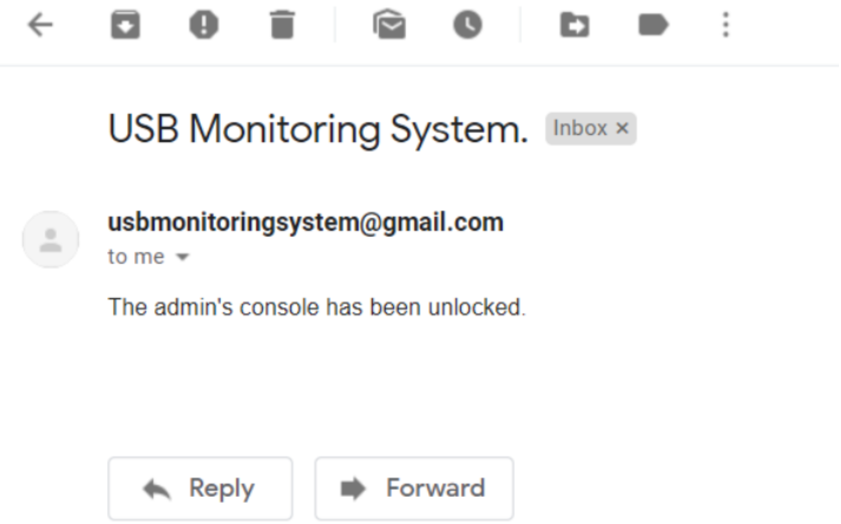
The next step is to create a proper list of authorized users and provide privileges to them accordingly, as highlighted in Figure 9. Note: (Once the application is re-opened by the administrator the Plaintext Passwords are converted to encrypted passwords as shown in the below figure)



| Permissions | Username | Password |
|---|---|---|
| Read | read | e0ef55f78114462aed31dadc19f8b632910bb017... |
| Read and Write | write | 33c5b813d57f51a588213eb5990a9706612c4aa... |
| Read and Write | test | 993015783721b2e070358a009df3b1b3a49c2d7... |
| | | |

Figure 9: User Database

Every time the Admin Console is accessed, an alert will be generated and then sent to the administrator email account as shown in Figure 10.



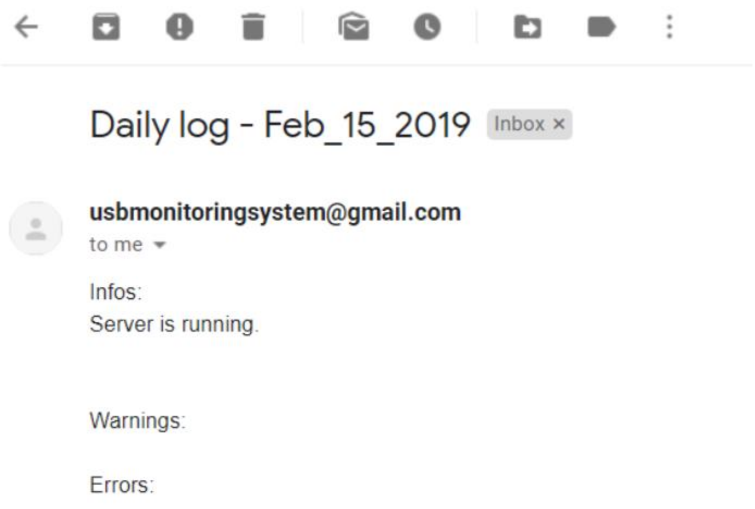
USB Monitoring System.

usbmonitoringsystem@gmail.com
to me

The admin's console has been unlocked.

Figure 10: Email Alert to Admin

In addition to this, daily logs of application events are also maintained and mailed to the administrator email account. This is to facilitate admin in analyzing warnings and errors, if any, on a regular basis and take requisite measures accordingly.



Daily log - Feb_15_2019

usbmonitoringsystem@gmail.com

to me

Infos:
Server is running.

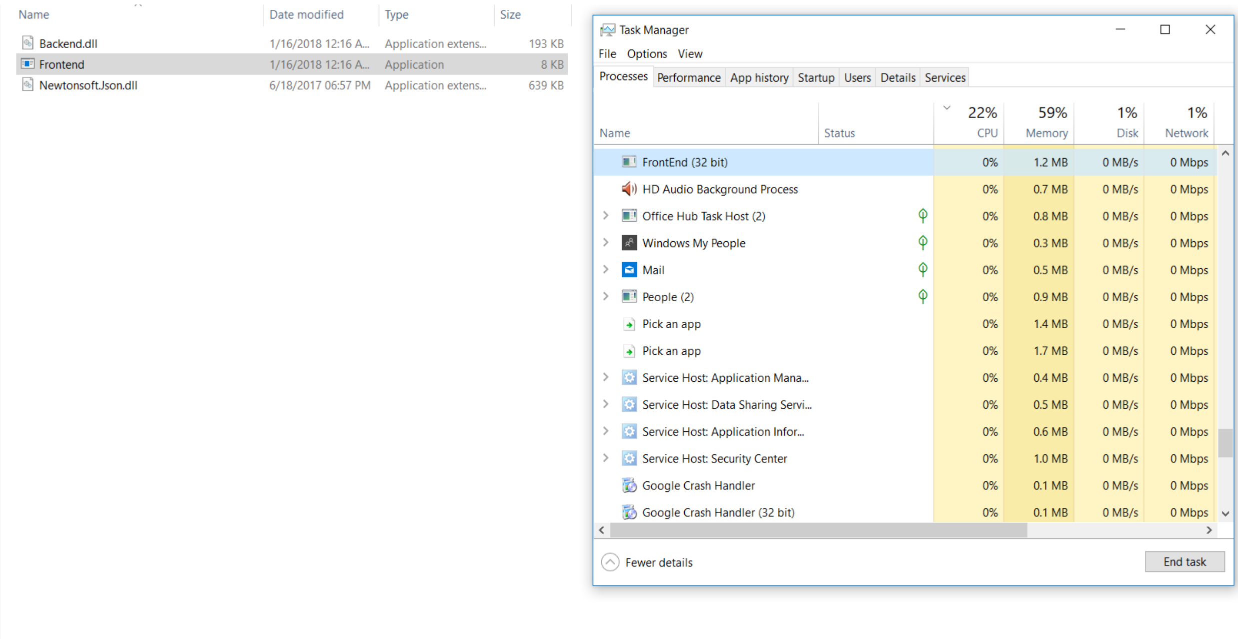
Warnings:

Errors:

**Figure 11: Daily Events Log**

- ***Navigation of Application from User Perspective***

With respect to the user perspective, the application is assumed to be running beforehand in the background, as shown in the following figure:

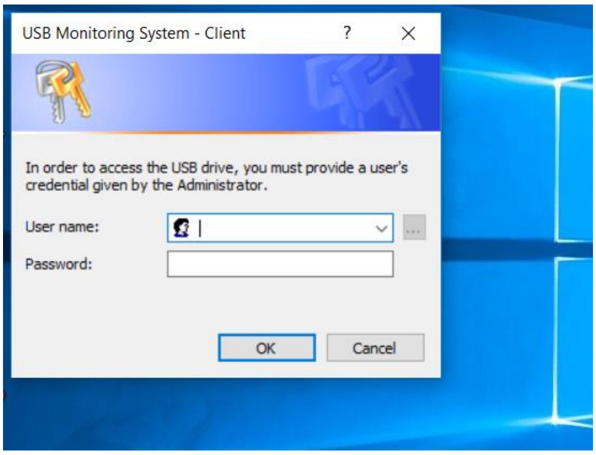


| Name | Date modified | Type | Size |
|---|---|---|---|
| Backend.dll | 1/16/2018 12:16 A... | Application extens... | 193 KB |
| Frontend | 1/16/2018 12:16 A... | Application | 8 KB |
| Newtonsoft.Json.dll | 6/18/2017 06:57 PM | Application extens... | 639 KB |

| Name | Status | 22% CPU | 59% Memory | 1% Disk | 1% Network |
|---|---|---|---|---|---|
| FrontEnd (32 bit) |  | 0% | 1.2 MB | 0 MB/s | 0 Mbps |
| HD Audio Background Process |  | 0% | 0.7 MB | 0 MB/s | 0 Mbps |
| Office Hub Task Host (2) |  | 0% | 0.8 MB | 0 MB/s | 0 Mbps |
| Windows My People |  | 0% | 0.3 MB | 0 MB/s | 0 Mbps |
| Mail |  | 0% | 0.5 MB | 0 MB/s | 0 Mbps |
| People (2) |  | 0% | 0.9 MB | 0 MB/s | 0 Mbps |
| Pick an app |  | 0% | 1.4 MB | 0 MB/s | 0 Mbps |
| Pick an app |  | 0% | 1.7 MB | 0 MB/s | 0 Mbps |
| Service Host: Application Mana... |  | 0% | 0.4 MB | 0 MB/s | 0 Mbps |
| Service Host: Data Sharing Servi... |  | 0% | 0.5 MB | 0 MB/s | 0 Mbps |
| Service Host: Application Infor... |  | 0% | 0.6 MB | 0 MB/s | 0 Mbps |
| Service Host: Security Center |  | 0% | 1.0 MB | 0 MB/s | 0 Mbps |
| Google Crash Handler |  | 0% | 0.1 MB | 0 MB/s | 0 Mbps |
| Google Crash Handler (32 bit) |  | 0% | 0.1 MB | 0 MB/s | 0 Mbps |

**Figure 12: Task Manager of Workstation Showing Running Application**

A login prompt is displayed every time the USB drive is inserted into the USB port and the user is asked to verify him by the application server for getting access to the USB port, as shown below:


USB Monitoring System - Client

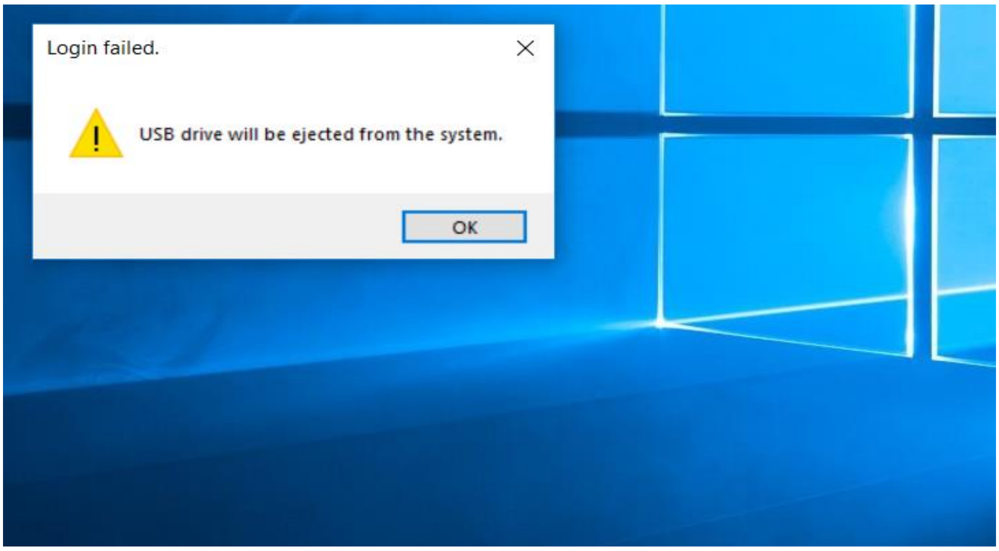
In order to access the USB drive, you must provide a user's credential given by the Administrator.

User name:

Password:

Figure 13: User Authentication

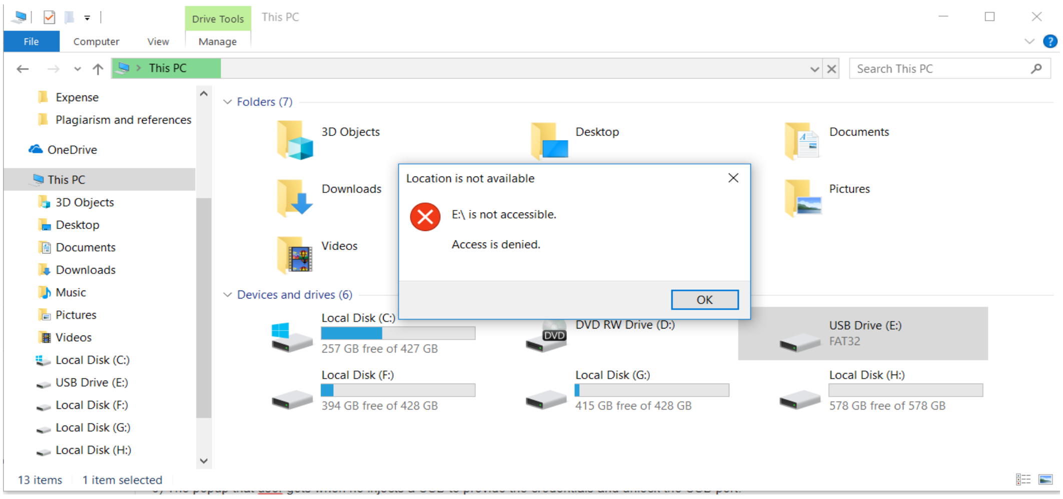
Once the credentials are entered by the user, the validity of the credentials is checked in the background and depending upon the validity, the user will be either given access or (login failed) to the port. If a wrong username or password is entered by the user, then no access will be given to the user and the USB port will remain locked, as displayed below.


Login failed.

USB drive will be ejected from the system.

Figure 14: Failed Login Attempt

This is further checked, as in Figure 15, that the unverified user is not given access to the USB drive, due to the failed login attempt.



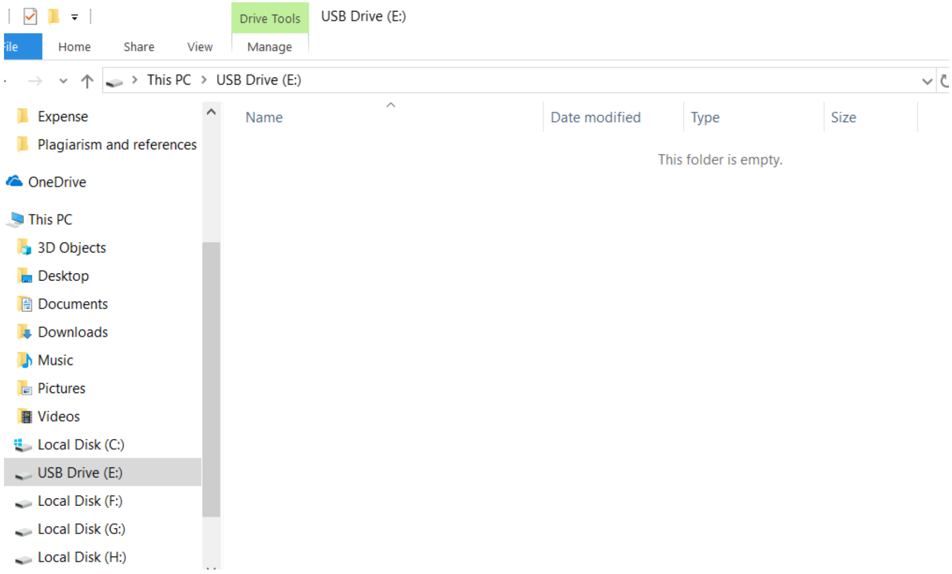
Location is not available

E:\ is not accessible.

Access is denied.

**Figure 15: Denied access for Unauthenticated User**

The user will be given access to the USB port once he is authenticated by the application server on providing valid credentials.



This folder is empty.

**Figure 16: Successful Login for Authenticated User**

This prototype is believed to be a productive solution for enhanced security of USB ports once it gets incorporated into a ‘Normal Company Environment’, meaning in a Windows Active Directory environment. In an active directory environment, all the users will have their domain credentials for authenticating themselves on to the workstation and also to the application which is controlling the USB port if they wish to use the USB port for plugging in storage devices. Once the users are verified, they will be able to perform read, write or execute functions according to the permissions set by the administrator for that specific user. However, due to the limited time and lack of resources, the application cannot be tested at a broader scale involving active directory.

Other than Active directory, there are some more features that could not have been tested due to inadequate resources and time limitation. Such as integration with the antivirus software and centralized logging capability, e.g. SIEM. Therefore, there are no screenshots available for depicting the navigation of these features.

# 6. Analysis and Evaluation

This section first performs a comprehensive assessment of the proposed solution under various security-based scenarios and deduces the response of the POC in the face of several potential threats. Furthermore, it also includes a comparison of the existing USB security schemes with the presented proof of concept, for determining the efficiency, feasibility and usability of the presented idea. The overall advantages and limitations of the developed system are also highlighted here.

## *6.1 Evaluation of POC under Various Scenarios*

It has been observed that several companies make use of BitLocker when it comes to security concerns related to USB. BitLocker is an application which encrypts the USB once it is plugged into the port so that the user can't infiltrate the data on to his own machine. However, this doesn't help if user has a malicious intent to inject malware in to the system.

There are several other techniques that companies rely on when it comes to the security of USB devices as mentioned below:

- Allow only known USB devices (limited by companies with respect to a specific vendor or by their signatures on each device) and block the rest.
- Allow only encrypted USBs
- Do not offer any restrictions and anyone can plug in any USB

Although, the above mentioned techniques are somewhat acceptable in various conditions but they are not perfect in all scenarios. The solution presented in this project uses an approach which is found to be better than the existing solution under various scenarios, as discussed below:

**SCENARIO 1: Pre-vetting of USB devices**

In some existing security solutions, the users are required to pre-vet their USB sticks from the security department before use. Vetting of USB flash drives is a troublesome approach for both users and the management department. The users in such cases have to bear the fatigue of visiting the security department for vetting their USBs. On the other hand, the Security department will have an added burden of keeping a record of every vetted device. Moreover, every time a new user will need USB for his job, he must go through a pre-vetting process for his USB. This makes it a poor security management strategy as the process will never stop due to the ever-increasing number of new users and devices. The proposed solution thus seems to be a user-friendly approach as it does not require the problematic and impractical vetting process and provides a runtime authentication solution for users.

Moreover, there are cases when a pre-vetted USB is lost and someone with malicious intents gets their hand on it or the person with pre-vetted USB decides to leave the company. In these cases, shutting down the USB and restricting its usage will be an added burden on management, which will make it an inefficient approach.

**SCENARIO 2: Someone gets access to employees pre-vetted USB**

In case of restricted USB flash drives, the maximum, an attacker has to do is to steal a pre-vetted USB. Once he succeeds in getting his hands on a pre-vetted USB, then he is free to carry out any malicious activity without being caught. But in this POC, the USB ports are restricted and even if the intruder steals the employee’s USB, he cannot access the port without correct login details.

**SCENARIO 3: Outsider Attack (Someone from outside gets access to the system)**

The presented approach is more focused on blocking the USB port rather than the USB drive itself and this significance of POC can be observed in the following scenario. For instance, consider a banking environment, where an intruder pretends to be a client and while chatting with the bank employee plugs a USB into the system with some malicious intent. In the existing solutions, the USB port is either completely active or fully inactive. So, if any port is already in use by the employee, then all the other ports must be active by default, and the attack can make full use of this opportunity. However, in the proposed solution, if a user has already authenticated him for accessing a USB port; he still must re-authenticate himself for accessing another port. This ensures that an employee already logged into the system with a certain USB will not give intruders a chance to insert their USBs without verifying them again. This makes the proposed solution an effective approach in the case of an already authenticated system.

**SCENARIO 4: Insider Attack (If an employee having valid login credentials has malicious intent)**

The presented idea is even effective when the intruder is someone within the workplace. If an employee having login credentials tries to carry out any suspicious activity, then it will be recorded in the log. The logging capability is not a part of most of the past solutions. But here, the software employed for opening/blocking USB ports keeps a record of every activity when a USB is plugged into a computer. Thus, it will be easy to trace back which employee used what type of USB in which computer and at what time. Therefore, under this approach, the users will restrain themselves from carrying out any malicious activity due to the fear of getting caught.

**SCENARIO 5: Physical Blocking of USB ports**

In a few existing solutions, the idea of physically blocking (e.g. by using epoxy glue) the unused USB ports is presented. However, even if the port is physically blocked, the attacker can unplug the employee's USB device for inserting his own USB. The POC has a solution to this issue as well, in which the intruder will be asked to re-authenticate himself even if he inserts the USB in the same port, as being used by the employee.

**SCENARIO 6: USB-Based Attacks**

In addition to the risks discussed above, the modern threats like USB key logger, USB killer, USB Rubber Ducky, etc. can also be encountered in POC, just by blocking the port and asking for login credentials on every access attempt, keeping in mind that the plugged-in device must not be detected as an input device by the system

## *6.2 Comparison of POC with Existing Solutions*

The existing solutions, discussed in chapter 3, are compared here with the proposed solution to draw findings regarding the usability of the presented idea. The comparison has been done based upon the key operational and security requirements discussed in chapter 2 of this report.

**Table 2: Comparison of POC with Existing Solution (1/2)**

| Requirements | Proposed Solution | 1.Microsoft Stand-alone Workstation Group Policy | 2.Microsoft Windows Domain Active Directory | 3.Microsoft Intune | 4.Symantec Endpoint Protection – SEP |
|---|---|---|---|---|---|
| 1. To authenticate every user that tries to access USB port | Carries out the user verification process every single time a user inserts USB flash drive into the USB port | Only allows users that are pre-registered through the security filtering feature to use their USB stick | The users are controlled by the user-specific group policy options and have to get verified by the domain | The user is not asked for login credentials every time. It allows usage of only specifically approved peripherals by creating a custom profile in Intune and configuring DeviceInstallation policies | Specific USB drives are whitelisted using either the hardware-based scheme or user-based scheme to access ports |
| 2. To authorize the user for carrying out read, write or execute functions | The administrator gives permission to the users for read, write or execute functions on the removable storage device | The USB flash drives are restricted by the policy for running executable files or data writing | The USB flash drives are restricted by the policy for running executable files or data writing | Microsoft Intune provides the option of denying “write access” to the removable data drives that are not protected by BitLocker. | Users can interact with the attached USB storage as per the permission assigned to that USB device. |

| | | | | | |
|---|---|---|---|---|---|
| 3. To log all the event details | Data logging facility is included in this application | All the events are logged properly | Logging facility is enabled | Data logs are maintained | All the events are recorded in logs |
| 4. To send alerts to the administrator regarding any unusual activity | The administrator is notified for suspicious alerts through email | The admin has to keep a check on the data logs through the application interface | The admin is notified about unusual activity in real-time via SMS or email | Malicious actions are detected, followed by the creation of a risk event, which can be accessed only via portal | Security alerts regarding suspicious activities are sent via mail |
| 5. To verify only USB devices and not the non-storage ones (mouse, keyboards, etc.) | The user authentication process is only for using USB flash drives and not for the other non-storage peripheral devices | One can restrict the usage of USB flash drives without affecting USB devices like printer, keyboard, mouse, etc. | The use of USB drives is restricted without affecting input peripherals | Allows installation and usage of only specifically approved peripherals by creating a custom profile in Intune and configuring DeviceInstallation policies | The setting can be made in SEP manager for blocking USB devices, excluding keyboard and mouse |
| 6. To block USB ports and not the USB devices | The scheme includes port blocking rather than USB devices | Blocks USB drives and not the ports | Restrict USB drives access | Currently, Intune can only limit USB drives and not the USB ports | Restrict USB drives access |

| | | | | | |
|---|---|---|---|---|---|
| 7. To provide support to different operating systems | The current prototype is only for Windows, but can be improved to offer support to other operating systems, including Linux and MAC | Supports Windows Vista, Windows 7 or higher | Supports Windows Vista, Windows 7 or higher | Offers support to different operating systems | Offers support to different operating systems |
| 8. To scan the USB device by an Antivirus software | The developed prototype can be enhanced to integrate an AV for scanning USB devices | The group policy settings can be used for configuring Windows Defender Antivirus | The policy settings can be used for configuring Windows Defender Antivirus | Intune can run a malware scan by using Windows Defender or Endpoint protection | Presently, an automatic System Scan in not run by SEP on the plugged-in flash drive |

**Table 3: Comparison of POC with Existing Solution (2/2)**

| **Requirements** | **Proposed Solution** | **5.USB Lock RP** | **6.Endpoint Protector** | **7.GFI Endpoint Security** | **8.Access Patrol** |
|---|---|---|---|---|---|
| 1. To authenticate every user that tries to access USB port | Verify user every single time he/she tries to insert USB flash drive into | Whitelisting is used to authorize specific USB removable devices based on hardware ID. | Whitelisting of USB storage devices can be done based on hardware ID, manufacturer or several | The verification of devices is controlled with reference to the class, physical port, file | Devices can be white-listed based on name, serial number, class, etc. |

| | | | | | |
|---|---|---|---|---|---|
| | the USB port | | other attributes | extension or device ID. | |
| 2. To authorize the user for carrying out read, write or execute functions | The admin gives permission to the users for read, write or execute functions on the removable storage device | The read, write and execute permissions are given based on device ID | Admin can deny or give permissions to a certain device. Any user with the authorized device thus gets all permissions | The system can be configured to give specific permissions to devices and users | Administrator can give certain users read-only access and other write-access too |
| 3. To log all the event details | Data logging facility is included in this application | Logs are generated and kept at Control server | Has logging capabilities | Possesses event logging function | Events are not logged in a usable format |
| 4. To send alerts to the administrator regarding any unusual activity | The admin is notified for alerts through email | The alerts can be sent to SMTP (TLS/SSL) email in real-time | The alerts are generated which can be accessed through the system status tab | When a data risk is detected, it will appear at once on the Dashboard | No alerts are generated in real-time, in case of unusual activities |
| 5. To verify only USB devices and not the non-storage ones (mouse, keyboards, etc.) | The user authentication process is only for using USB flash drives | Controls access to the USB port with no interference with the non-storage | Non-storage USB devices are ignored by the Endpoint Protector client | The use of USB drives can be restricted without affecting input peripherals | It does not block USB mouse or keyword or other similar USB devices |

| | | | | | |
|---|---|---|---|---|---|
| | | USB peripherals | | | |
| 6. To block USB ports and not the USB devices | The scheme includes port blocking rather than USB devices | Blocks illicit wireless adapters, portable devices, and removable drives | Block use of unauthorized USB devices | Blocks specific portable storage devices and not the ports | AccessPatrol works to control USB devices from accessing USB ports |
| 7. To provide support to different operating systems | The current prototype is only for Windows, but can be improved to offer support to other operating systems, including Linux and MAC | This application only works with Windows devices | Offers support to Linux, MAC OS/X, and Windows systems | Support only windows environment | Only runs in a windows environment |
| 8. To scan USB device by an Antivirus software | The developed prototype can be enhanced to integrate an AV for scanning USB devices | Antivirus software can be integrated with it for scanning authorized devices | Endpoint protector scans the device for virus detection | Data Awareness Module in this software scans the files to identify the causes of security breach | AccessPatrol does not come with a virus scan but can integrate other AVs to scan the devices |

This comparison has been carried a bit further in the following table, for drawing a crisp idea regarding the improvements achieved by the proposed solution, considering the major system requirements identified in chapter 2, **Table 1** (shown vertically in the below table) and the existing solutions presented in chapter 3 (added horizontally in the given table). A subjective scoring mechanism has been employed where the proposed solution and the existing ones will be rated on the scale of (0-3), for each of the requirements identified for an ideal USB security system (in chapter 2).

**Table 4: Comparison of POC with Existing Solutions**

| **Solutions**<br>**Requirement** | **Proposed Solution** | **Sol 1** | **Sol 2** | **Sol 3** | **Sol 4** | **Sol 5** | **Sol 6** | **Sol 7** | **Sol 8** |
|---|---|---|---|---|---|---|---|---|---|
| **1** | 3 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 2 |
| **2** | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| **3** | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 1 |
| **4** | 3 | 2 | 3 | 2 | 3 | 3 | 2 | 1 | 0 |
| **5** | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| **6** | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **7** | 2 | 2 | 1 | 3 | 3 | 1 | 3 | 1 | 1 |
| **8** | 2 | 2 | 2 | 2 | 1 | 2 | 3 | 3 | 2 |
| **Average Score** | **2.75** | **2.0** | **2.125** | **2.25** | **2.125** | **2.0** | **2.25** | **1.875** | **1.5** |

*Interpretation Score: 0 (poor); 1 (Average); 2 (Good); >2.5 (Excellent)*

The comparison of the proposed solution with the existing ones clearly indicates that the proposed solution fulfills the requirements identified for optimal USB security solution in chapter 2, with a maximum average score than all the other solutions. The existing solutions also satisfy most of the requirements but none of them offer the entire requisite attributes of ideal USB security solution. The analysis of the developed prototype thus shows that its implementation is practically feasible; it offers acceptable performance and has quantified the resource requirements.

## 6.3 *Advantages and Limitations*

The major advantage of this solution is the efficiently secured USB port that gets active only when proper credentials are provided by the users. Moreover, this is a user-friendly approach as it allows the users to use any USB device after providing valid login credentials. The theft and loss of USB flash drives are also not a major concern under this approach, as the stealer will not be able to get port access without verification of credentials.

Furthermore, this solution allows the management staff to keep well-maintained user records and keep a log of daily activities, which will eventually lead to an easier and effective auditing process. Another major advantage of this POC is that it only detects USB insertion and no pop up appears if an input device is plugged into the systems. As a result, the users are not bothered to verify them again and again just to use a mouse or a keyboard.

Besides a lot of advantages, the presented work has a few limitations as well due to being a POC. A major limitation of this POC is the requirement of an actual email address and password for unlocking the admin console. As the POC is using Google SMTP, so the authentication has to done using a verified Gmail account. One more limitation concerning user IDs is the username format, which must be like username@localhost (address of one's computer). This is because the client software itself does not know where to get the password verified, so localhost is the address to own computer.

However, these limitations are mainly because it is just a POC and implemented on a standalone workstation and such limitations can be easily eliminated in future releases with wider implementation of the proposed concept. Nevertheless, the future amendments may unfold some more limitations of this approach that are unknown at this point in time.

# 7. Conclusion

The USB storage devices have earned considerable importance in the work environment due to their portability and high data transmission speeds. However, their usage is prohibited or restricted at various levels, particularly because of the security threats associated with these devices e.g. data loss, malware insertion, etc. This report has identified the primary requirements of an ideal USB security solution, which is much needed by the present-day market. It has also highlighted various solutions opted in the past for developing USB security systems, which offer secure use of USB flash drives to some extent but have certain limitations associated with them. The major limitation of the existing approaches is their emphasis on restricting/blocking USB flash drives, rather than coming up with a feasible solution for restricting USB ports. The presented idea has led to a solution where the USB ports are blocked instead of devices, thus meeting a major requirement of the ideal USB security solution, as discussed in chapter 2. Furthermore, most of the current solutions white list USB storage devices on the basis of certain device attributes (device ID, manufacturer, etc.) or white-list user's workstation based on their job type or departments, etc. The proposed idea of asking for login credentials every time a user tries to access the port has overcome the chances of data theft and security breach in case of device theft/loss or physical access of an intruder to an employee's system. The requirement of authenticating a user on every time he plugs-in his USB flash drive, has been identified as the topmost requirement of an optimal USB security system, which has been addressed by the proposed solution in a far better way compared to the existing solutions. Furthermore, the detailed comparison of the proposed solution with the existing ones makes it a prolific addition in the domain of USB security solutions.

A universal solution for achieving USB security in Windows 8.1 and Windows 10 environments has been presented in this report. The authentication process here is user-based, where no user is granted USB port access without getting verified by the application server. The authorized users can execute, read, or write on the USB storage device based on the permissions set for each user by the application administrator, thus fulfilling the second requirement of the ideal USB security system. Moreover, the system also maintains a proper log of every activity (the third important requirement as identified in chapter 2) and also generates alerts in case of any suspicious activity and notify the administrator in real-time via mail to facilitate him in taking prompt measures. Generation of alerts has been regarded in this report as another important security requirement, which has been addressed by the proposed solution in an improved way than most of the existing solutions where the administrator is required to himself keep a check on suspicious activities through application portal or system status tab, rather than being notified in real-time via email.

This initial prototype has undoubtedly laid the foundation for the development of an ideal USB security system that will overcome the limitations of past solutions. A few shortcomings have also been identified in this report that can be eliminated by making certain amendments in the next phase of this project. For instance, offering support to various operating systems, integration of antivirus software, etc. AV integration and compatibility with different operating systems have been identified as the essential requirements of an ideal USB security system, and these can be easily fulfilled by the proposed solution in the future. These future modifications are discussed in the following section that will make this proof-of-concept even more productive and secure in the long run.

# 8. Future Recommendations

The successful implementation of this prototype and its usefulness for the practical world asks for the future extension of this project. The practicality and efficiency of this prototype can be enhanced in the future by doing some modifications/additions to the project.

Firstly, a domain controller must be created for managing multiple workstations and different aspects of this application, ranging from a single screen to maintenance of centralized log structure, which can receive events in real-time from several instances. Secondly, this prototype can be implemented further within a complex, on-premise Windows Active Directory infrastructure and it can be controlled through the cloud-based Azure Active Directory and InTune. At present, the POC is only for Windows environment and can be improved further by making significant backend changes, in order to extend support to other Operating Systems such as MAC and Linux.

Moreover, an AV component can be linked with the application, so that each USB flash drive is first scanned by AV for any threats or malware, before getting authenticated by the system. This is an essential requirement for protecting the system from malware which can effortlessly sneak into the system through a USB flash drive.

In recent times, biometric verification is offering more precise user-identification and lowering the risk of unwanted security breaches. Nowadays, biometric systems are currently incorporated in most sectors that deal with sensitive information. The integration of biometric authentication to this POC, for instance, the use of a thumb scan in additions of password can be a productive step in achieving a more secure USB monitoring system.

In the future, program codes can also be added for generating real time intruder alerts, such as having consecutive failed logon attempts within a specified period of time or where a user was found of transferring >1 GB of data. The prototype can also be extended further to include content filtering on any copied file, for keywords like credentials, password, etc, so that we can overcome the problem of sensitive data exfiltration as well.

In addition to this, certain attributes like data encryption can also be added in this application along with the proposed USB port monitoring system. By having this two factors, it is believed to be an optimal USB security system.

# Bibliography

Al-Zarouni, M. (2006). *The Reality of Risks from Consented use of USB Devices*. Edith Cowan University.

Armerding, T. (2018). The 18 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [Accessed 10 Jun. 2019]

Arrospide, J. (2019). USB Device Control - Endpoint Security Software | USB-Lock-RP. Retrieved from https://www.usb-lock-rp.com/ [Accessed 6 Jun. 2019]

Bem, D., & Huebner, E. (2007). Analysis of USB flash drives in a virtual environment. *Small Scale Digital Device Forensics Journal, 1*(1).

Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. *The Encyclopedia Of Criminology And Criminal Justice*, 1-5. doi: 10.1002/9781118517383.wbeccj244

Bruzzese, J. (2016). Tutorial: The joys of Windows Server's group policies. Retrieved from https://www.infoworld.com/article/3117286/tutorial-the-joys-of-windows-servers-group-policies.html [Accessed 10 Jun. 2019]

Carl, G., Kesidis, G., Brooks, R., & Suresh Rai. (2006). Denial-of-service attack-detection techniques. *IEEE Internet Computing*, *10*(1), 82-89. doi: 10.1109/mic.2006.5

Chen, B., QIN, C., YU, L., & JIANG, P. (2012). A secure access authentication scheme for removable storage media. *JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE*, *9*(15), 4353-4363.

Crawford, T. (2012). *The Visual Artist's Guide to Copyright Infringement, Fair Use, Compulsory Licensing, and Permissions*. New York: Constable & Robinson.

Currentware. (2019). USB Block Software - Block USB drives | DLP software. Retrieved from https://www.currentware.com/accesspatrol [Accessed 10 Jun. 2019]
Cyber Cell Delhi. (2016). Fake Call Frauds. Retrieved from http://www.cybercelldelhi.in/fakecallsfrauds.html [Accessed 10 Jun. 2019]

Debiao He, Kumar, N., Jong-Hyouk Lee, & Sherratt, R. (2014). Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Transactions On Consumer Electronics*, *60*(1), 30-37. doi: 10.1109/tce.2014.6780922

Detwiler, J. (2003). News, Tips, and Advice for Technology Professionals - TechRepublic. Retrieved from https://www.techrepublic.com/article/disable-usb-ports-to-prevent-unauthorized-data-transfers/[Accessed 10 Jun. 2019]

Eby, D. (2019). What is Microsoft Intune. Retrieved from https://docs.microsoft.com/en-us/intune/what-is-intune/[Accessed 10 Jun. 2019]

Evans, M., & Scott, P. (2017). Fraud and cyber crime are now the country's most common offences. Retrieved from http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ [Accessed 10 Jun. 2019]

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., ... & Wood, P. (2011). Symantec internet security threat report trends for 2010. *Volume XVI*.

GFI. (2008). Retrieved from https://www.gfi.nl/documents/multibrochure.pdf [Accessed 10 Jun. 2019]

GLOVER, G. (2018). The Importance of Log Management. Retrieved from https://www.securitymetrics.com/blog/importance-log-management[Accessed 10 Jun. 2019]

He, D., Kumar, N., Lee, J., & Sherratt, R. (2014). Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Transactions On Consumer Electronics*, *60*(1), 30-37. doi: 10.1109/tce.2014.6780922

HHSB. (2019). Types of Online Fraud -. Retrieved from https://www.myhhsb.com/types-online-fraud.htm [Accessed 10 Jun. 2019]

Janczewski, L., & Colarik, A. (2008). *Cyber warfare and cyber terrorism*. Hershey [Pa.]: Information Science Reference.

Jan Axelson, USB Complete 3rd, ISBN: 1-931448-02-7, August 2005

Johnson. (2017). What is a USB Device and How Does a USB Device Work?. Retrieved from https://www.cleverfiles.com/howto/what-is-usb-device.html [Accessed 10 Jun. 2019]

Justinha, & Chen, A. (2019). How to control USB devices and other removable media using Intune (Windows 10). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/device-control/control-usb-devices-using-intune [Accessed 10 Jun. 2019]

Kitchin, R. (2013). Big data and human geography. *Dialogues In Human Geography*, *3*(3), 262-267. doi: 10.1177/2043820613513388

Larson, S. (2017). Every single Yahoo account was hacked - 3 billion in all. Retrieved from https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html [Accessed 10 Jun. 2019]

Li, Q., & Chen, Y. (2009). Data Flow Diagram. *Modeling And Analysis Of Enterprise And Information Systems*, 85-97. doi: 10.1007/978-3-540-89556-5_4

Misra, A., & Dubey, A. (2015). *Android Security*. Boca Raton: Auerbach Publishers, Incorporated.

Network Management Solutions. (2014). Security Risks Imposed By The Use Of USB Drives. [Accessed on Feb 23 2018] from http://www.nmscorp.com/2014/09/security-risks-imposed-by-the-use-of-usb-drives/ [Accessed 10 Jun. 2019]

Phys. (2017). Russian cyber hacker pleads guilty in identity theft case. Retrieved from https://phys.org/news/2017-09-russian-cyber-hacker-guilty-identity.html [Accessed 10 Jun. 2019]

Posey, B. (2011). *GFI Network Security and PCI Compliance Power Tools* (2nd ed.). Elsevier Science.

Schneider, D. (2014). USB Flash Drives Are More Dangerous Than You Think. Retrieved from https://spectrum.ieee.org/tech-talk/computing/embedded-systems/usb-flash-drives-are-more-dangerous-than-you-think [Accessed 10 Jun. 2019]

Shachtman, N., Shachtman, N., Barrett, B., Barrett, B., Newman, L., & Barrett, B. et al. (2008). Under Worm Assault, Military Bans Disks, USB Drives. Retrieved from https://www.wired.com/2008/11/army-bans-usb-d/

SolarwindsMSP. (2016). Multi-Layered Network Security Strategy | SolarWinds MSP. Retrieved from https://www.solarwindsmsp.com/content/multi-layered-security-approach [Accessed 10 Jun. 2019]

Solutions, N. (2019). Security Risks Imposed By The Use of USB Drives | Network Management Solutions. Retrieved from http://www.nmscorp.com/2017/09/security-risks-imposed-by-the-use-of-usb-drives/ [Accessed 10 Jun. 2019]

Standaert, F. (2009). Introduction to Side-Channel Attacks. *Integrated Circuits And Systems*, 27-42. doi: 10.1007/978-0-387-71829-3_2

SVAN, J., & ALLEN, D. (2008). DOD bans the use of removable, flash-type drives on all government computers. Retrieved from https://www.stripes.com/news/dod-bans-the-use-of-removable-flash-type-drives-on-all-government-computers-1.85514 [Accessed 10 Jun. 2019]

Tetmeyer, A., & Saiedian, H. (2010). Security Threats and Mitigating Risk for USB Devices. *IEEE Technology And Society Magazine*, *29*(4), 44-49. doi: 10.1109/mts.2010.939228

Thorsten S. (2015). USB Security That’s What You Really Need!. itWatch, GMBH.

Tian, D., Bates, A., Butler, K., & Rangaswami, R. (2016). ProvUSB. *Proceedings Of The 2016 ACM SIGSAC Conference On Computer And Communications Security - CCS'16*. doi: 10.1145/2976749.2978398

Torbin, C. (2016). CoSoSys introduces Endpoint Protector Data Loss[...]. Retrieved from https://www.endpointprotector.com/company/press-releases/press-release-212 [Accessed 10 Jun. 2019]

Tripathi, D., Nigam, B., & Edla, D. (2017). A Novel Web Fraud Detection Technique using Association Rule Mining. *Procedia Computer Science*, *115*, 274-281. doi: 10.1016/j.procs.2017.09.135

Walters, P. (2012). The risks of using portable devices. *Carnegie Mellon University. Produced for US-CERT, a government organization. Retrieved from http://www. us-cert. gov*.

Yang, F., Wu, T., & Chiu, S. (2010). A secure control protocol for USB mass storage devices. *IEEE Transactions On Consumer Electronics*, *56*(4), 2239-2343. doi: 10.1109/tce.2010.5681109

# Appendix A- Additional Resources

1. How to Block USB Drives and Removable Media using Group Policy
   http://woshub.com/how-to-disable-usb-drives-using-group-policy/

2. Configure device restriction settings in Microsoft Intune
   https://docs.microsoft.com/en-us/intune/device-restrictions-configure

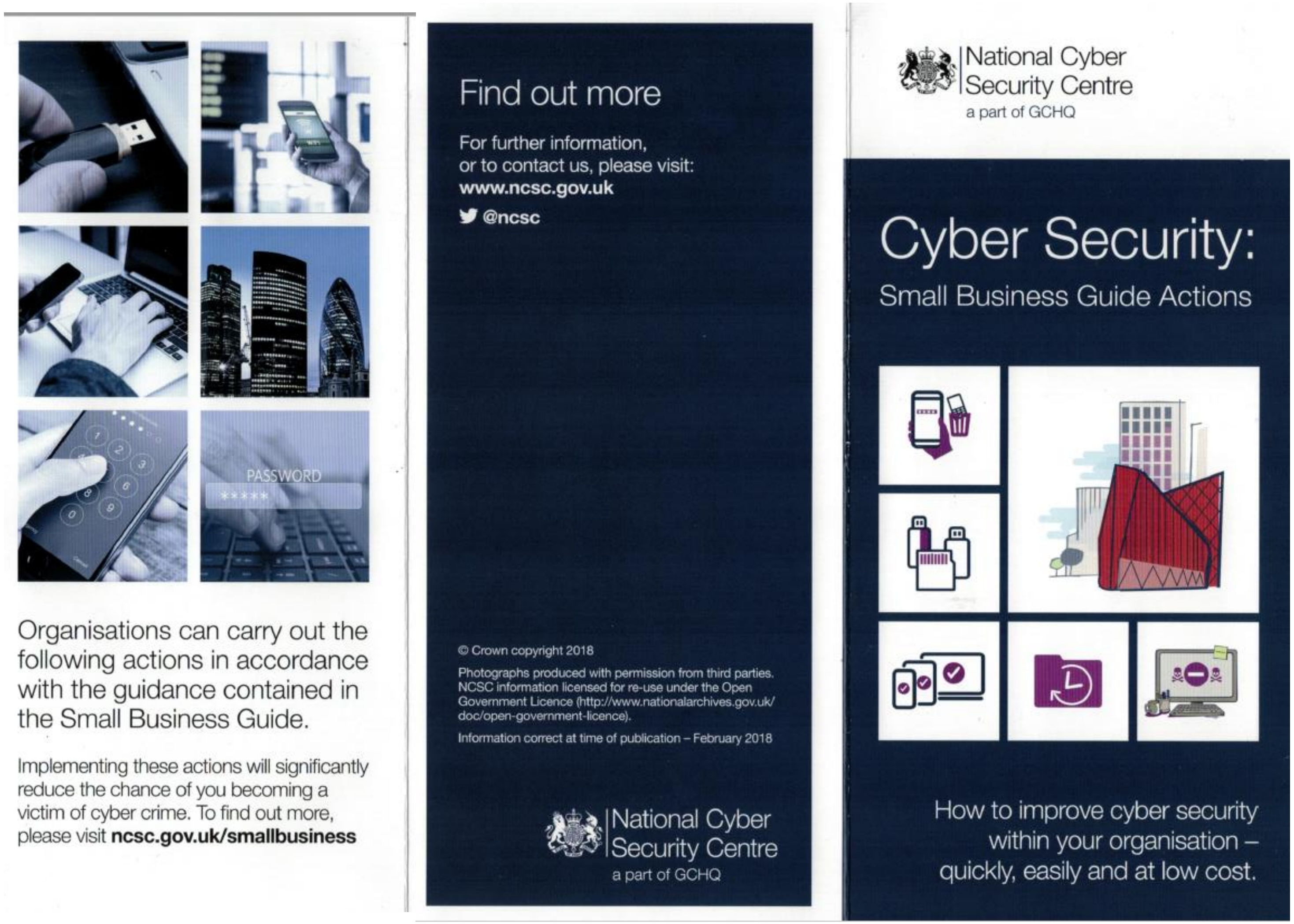
3. Intune Policy to disable USB drives that is not protected by Bitlocker encryption
   https://www.linkedin.com/pulse/intune-policy-disable-usb-drives-protected-bitlocker-haider/

4. How to control USB devices and other removable media using Windows Defender ATP
   https://docs.microsoft.com/en-us/windows/security/threat-protection/device-control/control-usb-devices-using-intune

5. Symantec End Point Protection
   https://support.symantec.com/en_US/article.TECH175220.html
   https://www.symantec.com/connect/forums/computer-mode-vs-user-mode-0

6. USB_Lock-RP by Advanced Systems International: USB Device Control Endpoint Security Software
   https://www.usb-lock-rp.com/

# Appendix B - NCSC Cyber Security, Small Business Guide



National Cyber Security Centre
a part of GCHQ

Cyber Security:

Small Business Guide Actions

How to improve cyber security within your organisation – quickly, easily and at low cost.

Find out more

For further information, or to contact us, please visit:
**www.ncsc.gov.uk**
**@ncsc**

© Crown copyright 2018

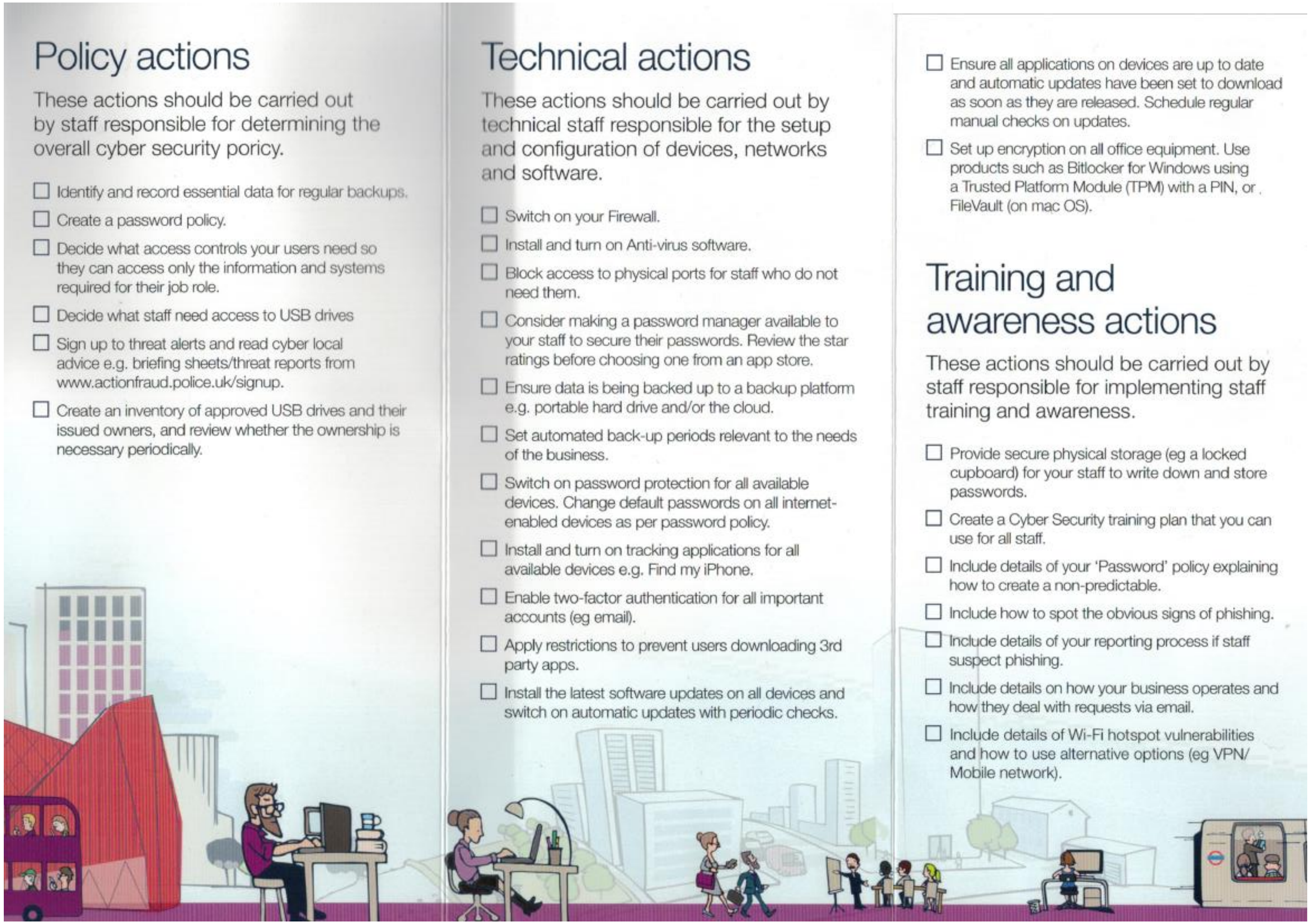
Photographs produced with permission from third parties. NCSC information licensed for re-use under the Open Government Licence (http://www.nationalarchives.gov.uk/doc/open-government-licence).

Information correct at time of publication – February 2018

National Cyber Security Centre
a part of GCHQ

Organisations can carry out the following actions in accordance with the guidance contained in the Small Business Guide.

Implementing these actions will significantly reduce the chance of you becoming a victim of cyber crime. To find out more, please visit **ncsc.gov.uk/smallbusiness**



## Policy actions

These actions should be carried out by staff responsible for determining the overall cyber security poricy.

- ☐ Identify and record essential data for regular backups.
- ☐ Create a password policy.
- ☐ Decide what access controls your users need so they can access only the information and systems required for their job role.
- ☐ Decide what staff need access to USB drives
- ☐ Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup.
- ☐ Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically.

## Technical actions

These actions should be carried out by technical staff responsible for the setup and configuration of devices, networks and software.

- ☐ Switch on your Firewall.
- ☐ Install and turn on Anti-virus software.
- ☐ Block access to physical ports for staff who do not need them.
- ☐ Consider making a password manager available to your staff to secure their passwords. Review the star ratings before choosing one from an app store.
- ☐ Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud.
- ☐ Set automated back-up periods relevant to the needs of the business.
- ☐ Switch on password protection for all available devices. Change default passwords on all internet-enabled devices as per password policy.
- ☐ Install and turn on tracking applications for all available devices e.g. Find my iPhone.
- ☐ Enable two-factor authentication for all important accounts (eg email).
- ☐ Apply restrictions to prevent users downloading 3rd party apps.
- ☐ Install the latest software updates on all devices and switch on automatic updates with periodic checks.
- ☐ Ensure all applications on devices are up to date and automatic updates have been set to download as soon as they are released. Schedule regular manual checks on updates.
- ☐ Set up encryption on all office equipment. Use products such as Bitlocker for Windows using a Trusted Platform Module (TPM) with a PIN, or FileVault (on mac OS).

## Training and awareness actions

These actions should be carried out by staff responsible for implementing staff training and awareness.

- ☐ Provide secure physical storage (eg a locked cupboard) for your staff to write down and store passwords.
- ☐ Create a Cyber Security training plan that you can use for all staff.
- ☐ Include details of your 'Password' policy explaining how to create a non-predictable.
- ☐ Include how to spot the obvious signs of phishing.
- ☐ Include details of your reporting process if staff suspect phishing.
- ☐ Include details on how your business operates and how they deal with requests via email.
- ☐ Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (eg VPN/ Mobile network).