A special report from Computer Weekly

AN ENHANCED APPROACH FOR USB SECURITY MANAGEMENT

by Daniyal Naeem, MSc (Royal Holloway, 2019)
and Keith Mayes, ISG, Royal Holloway

An Enhanced Approach for USB Security Management

Authors
Daniyal Naeem, MSc (Royal Holloway, 2019)
Keith Mayes, ISG, Royal Holloway

Abstract

USB flash drives and other USB-connected data storage devices offer a simple way of making data more portable and more easily transferrable. However, their use presents security risks that must be addressed. Apart from increasing the risk of data-theft, they have often been used to transfer malware, sometimes with disastrous results. Tracing flash drive-assisted data-theft or malware to the culprit can pose a challenge to cybersecurity professionals and managers, but the problem can be addressed with the aid of a novel USB monitoring system. This article outlines such a strategy, identifies what security attributes such a system must have, and compares the new strategy with established methods. [a]

[a] This article is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

The Risk: Misery, Ruin, and Disaster from a USB Device

Whether employees are using flash drives to transfer documents or cameras to transfer images, the simple USB port presents a potent risk. The user may not even be to blame. A reprogrammed USB controller chip can become a gateway to hackers and a company's worst nightmare. Organisations like Facebook, Uber, and WhatsApp have discovered just how damaging this can be following highly publicized data breaches.

There are two primary security problems posed by the use of USB ports for data transfer: data theft and infection by malware. An unsecured USB port and an innocent-looking data stick could make organisations the victims of cybercrimes, data attacks, physical security breaches and more.

As most of us know, these crimes can be incredibly destructive, and since the introduction of General Data Protection Regulations (GDPR), the sheer magnitude of the fines levied following data breaches has resulted in widespread negative publicity for affected companies. The cost in financial terms, in reputation, legal fees, and penalties can also be enormous.

At the same time, USB devices, particularly data sticks, have undeniable advantages. They're fast. They're easy to use, and they're effective.

Current Ways to Address the USB Threat: Methods and Shortcomings

Prevent Anyone from Using USB-Based Data Transfer (With Possible Exceptions)

One way of tackling the threat is to completely prevent anyone from using a USB for data transfer either with blocking the ports or with strict access control policies. The possible usefulness of these devices is dispensed with altogether. Security takes precedence over convenience and possible productivity benefits.

Some organisations will give the nod to the need for USB data transfer by making provision for a whitelisting process. USBs are blocked, but under certain circumstances, employees may be allowed

to use them for a limited time.

However, neither of these approaches follows the defence in depth principle. If the first layer of defence collapses, there is no second, third and fourth layer to bypass for the attacked.

Some other problems:

- **Users having trouble getting whitelisted access** owing to the policies that focus on risk avoidance. This inflexible approach could have massive costs in terms of lost productivity and lost opportunities.
- **An intruder using a computer with a whitelisted USB port** without the user's knowledge. It's easier than you may think. For instance, if you're in an appointment with your bank manager, you can easily reach the port of the computer if he or she is distracted for a moment and can insert the USB without his knowledge.
- **A heavy workload for administrators** who must now look after all the provisioning and de-provisioning of whitelisted users. They must cope with accountability issues and audit all activity stemming from whitelisted ports. As soon as whitelisting is allowed, careful asset management is also necessary. Who uses which computer? Now we must audit all this information, including activity, and all the provisioning and de-provisioning access approvals.

There's simply too much room for error, and an unbelievable amount of management challenges and hassle to face. For example, supposing a USB port is to be whitelisted:

- Under what circumstances will whitelisting be allowed?
- What is the timeframe for which whitelisting is in force?
- What activity has been logged, and is it in order?
- Are USBs being blocked at the end of the whitelisting period?

As a solution, blocking USB flash drive access in this way leaves too much room for errors, oversights, and sidestepping the system. It is simply too cumbersome to be effective, and with the buck stopping at the responsible manager's desk, he or she would rather not go there, hence the fact that most companies severely limit whitelisting.

The most primitive solution is using epoxy adhesive to physically block USB ports so that they can't be used at all. Effective? Possibly. Smart? Probably not! This extreme response is rarely used and would only be implemented if there's no other option. Who remembers Wannacry? If those infected laptops ended up in museums, they'd be glued for sure!

Go ahead with this option if you don't mind these problems:

- All the benefits of USB devices can no longer be accessed at all, ever. Data transfer becomes time-consuming and frustrating.
- The value of the machines "doctored" in this way goes through the floor.

Using Pre-Whitelisted USB Flash Drives Only

One of the most commonly implemented strategies these days is to use vendor-specific or pre-whitelisted USBs but this opens a whole new can of worms for those tasked with implementation.

- **Administration is complex.** We now have to map every employee and every USB issued to them. There's also a slew of additional policies and procedures to hammer out, implement and monitor for compliance.

- **Although we now have the advantage of highly portable data, we also have USB flash drives that can be lost or stolen.** Where is it being used now? How can we disable access to its contents remotely? While there are certain cases in which we can do this, "possible" and "effective" may not fit into the same scenario.
- **Logging issues that make accountability fuzzy can also arise.** I lost my USB on a certain date, and I logged the issue as soon as I realized it. Meanwhile, the device has been used maliciously. Who is responsible? How would you know it's not me? Automated logging would be necessary, and even then, I could be the one behind the threat. But how would you prevent it or prove it?
- **Work makes more work.** Now that we have an account provisioning and de-provisioning system, it must be implemented and integrated into the "bigger picture" every time a new user arrives on the scene or an established one leaves.

What USB Security Systems Should Cover

Before we look at an easier way to clear out all the clutter from USB security, let's get down to the basics. What should USB security systems do?

Location dependent access: So, you want to work during your airport wait or make a bit of progress while you're at the coffee-shop. You're no longer in an authorized location, so no new data can be written onto the device. If it's super-sensitive stuff, you may not be able to read it either.

Activity Logs: Who transferred which data to which device? Can you rapidly track the problem to source if there is a data breach or attack?

Control and Limit the Devices: Only allowing access to files that are relevant to a department or task can help to limit possible copying of crucial data. Users have access to need-to-knows only and follow the least privilege principle.

Protect Against Malware: It's those dreaded bugs that you don't want sneaking in to your computer network. Scanning USBs with antivirus software before the user can interact with the device helps protects against malware.

Disable autorun: Autorun is one of the advantages of USB flash drives, but also a disaster if the wrong files start galloping through computer systems.

Educate employees: When people know the what and the why, they're more likely to comply. It takes training, and it takes regular reminders.

A Novel Alternative that Combines Efficacy with Cost Efficiency

All this work to control USB flash drives might tempt you to either just block all access or bury your head in the sand and wait for the next Stuxnet to hit. That doesn't bear thinking about, so – are you doomed to live with complexity or forgo all the handy benefits of USB flash drives? Neither should be necessary.

What struck me during my research into USB flash drive security, is that almost all the efforts to improve security focused on the devices. What about focussing the real point of access: the USB port itself?

With this in mind, I designed an application that covers everything we really need a USB security system to do but without the complexity, mountains of administration work, and frustration inherent in the systems currently in use. It's simple, it's novel, it's effective and the primary focus is on the port, who is using it, and what they're trying to do once they've accessed it.

To expand on this:

- All the ports are initially blocked
- We bypass the complexity of whitelisting by applying the concept of Identity and Access Management.

Access control priorities

- Deter
- Prevent
- Detect

We also keep our access control priorities in order, and my proof of concept (POC) application approach does the job.

Focus on Ports: Here's How We Fulfil These Requirements

Deter: If users must authenticate their identity before they can unlock a USB port, and they know that there's a record of all activity after that, they won't be keen to initiate malicious activity. After all, it can be tracked right back to them, and there can be no excuses or buck-passing.

Prevent: Data Loss Prevention (DLP) can be integrated with my POC application. It's a matter of ensuring that any data theft can be prevented by using content analysis techniques which can be used to trigger policy violations and prevent data loss. If somehow, the data is compromised, we can move to the next priority, namely, detection.

Detect: Since we're going to log all activity that occurs after authentication, we can build in a framework that will quickly detect any activity that might indicate malicious attempts to tamper with data or systems. The alert goes out, and the responsible cybersecurity personnel can act fast.

In short:

We **deter** or scare the possible culprit. They know we can track them down, so they're less likely to take a chance.

If our possible wrongdoer isn't scared off by knowing we can identify the source of a security breach, we try to **prevent** the action.

If, by any chance, our miscreant isn't deterred or prevented from wrongdoing, we want to make sure that we **detect** the suspicious activity quickly, allowing us to mitigate potential damage.

How It Works in Practice

Let's begin with the brass tacks. Here's a simple process flow to illustrate what happens when we use the proof of concept (POC) application I designed and switch our focus to USB ports and user authentication.

Figure 1 shows a step by step walkthrough of what happens when a user inserts USB. In practice, it works like this:

1. As soon as the user inserts a USB, the application gets triggered and sends an alert to the backend server requesting a login page to be displayed.
2. The server returns with the login page and the application displays it on the screen.
3. The user now enters the login credentials. The application sends them to the server in hashed form and the server now checks the hashed credentials with the database and ensures there is a one to one match with the credentials it has stored.
4. If a match is found, it means that the credentials are valid. The database returns with a "valid information" prompt to the server. Similarly, if the user cannot authenticate their identity, the port remains blocked

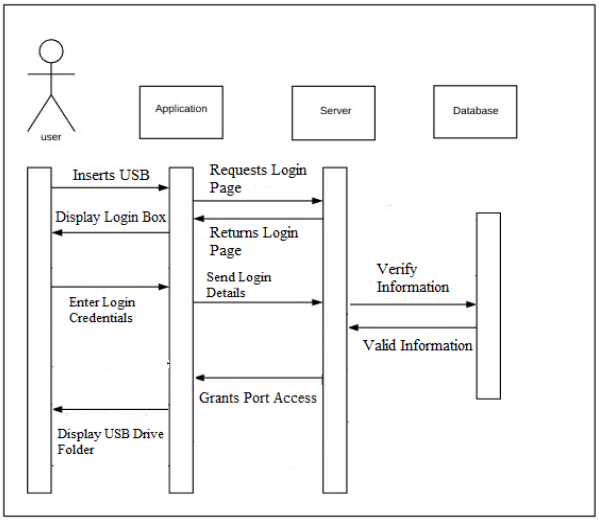

Figure 1: Proof of concept application.

5. The server now grants the port access, and depending on the user authenticated, it applies the appropriate permissions and access rights to the port which allow the user to read, write, or execute.
6. The application login prompt disappears, and the USB drive folder opens for the user.
7. Finally, every activity performed using the USB is recorded, ensuring full accountability.

All the Nasties Covered with One Simple Solution

By cutting through the unnecessary complexity of a USB device-focused approach and focussing on the ports, who is using them, and what happened during their use, we cover all the data-related nasties that give us sleepless nights:

- Unauthorized disclosure: the loss of confidential information.
- Unauthorized modification: data that is changed so that its integrity is compromised.
- Unauthorized destruction: just imagine – all your carefully compiled data vanishing into the ether, leading it to loss of availability.

We also overcome the problem of accountability. If something goes wrong, whose fault is it? How is our data being used? Thanks to user authentication, we have a full log for auditing purposes.

Finally, we have full access control. Users can be added and deleted with ease, and each user will have a set of permissions, allowing the administrator to create specific access control policies – he or she can be authorized or blocked from reading, writing, and execution activities as needed. Not allowed to run executable files? Then there's no way malware can be introduced. Allowed? Remember, the USB device is automatically scanned for viruses, so the risk is mitigated to the point where it would be very difficult to infiltrate the system. Of course, we cannot overlook the possibility of a "zero day" vulnerability being exploited. In this case, you aren't aware of the possibility of a vulnerability, and there's no easy way you could have known it was there.

Closing the Final Loophole: Encryption

The final step is one your organisation should already be implementing: data encryption. Lost or stolen USB flash drives should not contain sensitive information that isn't protected by encryption. After all, it's all too easy to lose track of a flash drive. Has it fallen into the wrong hands? If it has, you don't want the culprit to be able to get anything out of it. Good encryption makes sure they won't.

Integrating Biometrics into Authentication

Realistically, using passwords is the weakest form of authentication. ID cards or tokens partially address this, but we should always consider worst-case scenarios. Biometrics would be the likeliest to prove beyond doubt that the person accessing a system really is who they say there are. The technology is there. It's just a matter of implementing it to my POC application.

Final Thoughts

USB security is something we can't afford to overlook. Although the internet is the number one source of malware and attacks on data systems, the USB device takes second place. Once again, think Stuxnet. Wannacry was internet-based, but Stuxnet was USB-based.

Keeping information safe is another priority. No outsiders should gain access to sensitive data, and malicious insiders need to know they'll be caught red-handed and held fully accountable if they try any dirty dealings. This USB port-based approach does just that.

User education remains a vital element in the mix. We have an effective security management approach, but every user with access should know a few simple dos and don'ts. They need to be part of your organisation's policy, and there must be consequences for those who fail to comply.

Need to Know More?

Feel free to get in touch with me with your questions or comments at `daniyalnaeem@protonmail.com` - you can be sure I'll give them thought and that you'll get a timely response.

Biographies

Daniyal Naeem graduated in 2019 from Royal Holloway, University of London with a distinction in MSc in Information Security. Daniyal is CISSP certified and currently working as a Security Manager and been in the cyber security industry since 2013. His main interest includes Cyber law, Insider Threat, Identity & Access Management & Artificial Intelligence.

Keith Mayes is a Professor of Information Security at Royal Holloway, University of London, where he was formerly the Director of the Information Security Group (ISG), and the Head of the School of Mathematics and Information Security, and the Founder Director of the Smart Card and IoT Security Centre. He is a Chartered Engineer, a Fellow of the Institution of Engineering and Technology, and a board member for the International Cyber Security Centre of Excellence (INCS-CoE).

Series editor: S.- L. Ng