Secure USB Usage in Industrial Settings

This paper will explore the risks of USB in an industrial setting and present an outline of a secure USB solution that is suitable in combination with a multilayered security approach to protect industrial control systems. The target is to improve control system safety, reliability and availability and to protect against the physical, economic and social impacts that are associated with industrial security lapses.
INTRODUCTION TO USB SECURITY ISSUES IN INDUSTRIAL CONTROL SYSTEMS

A malware that MIT Technology Review refers to as the world's most murderous malware and that introduced itself to the world in an attempt to blow up a petrochemical plant in the Middle-East is now reportedly spreading to North America and the rest of the world. This happens at a time when there are more than 2.5 million industrial robots being employed in world wide industries ranging from automotive, electrical/electronics, metal/machinery, plastics/chemical to food and beverage.1 All these systems are not vulnerable to the specific attack, named Triton, but many shared common weaknesses. These machines and their supporting systems are commonly equipped with the ubiquitous USB computer interface that we all know so well from our desktops. The USB port introduces opportunities for maintenance, statistics and much more but also requires procedures and measures to be in place to safeguard the organizations that utilize them. But beyond headline grabbing attacks, stakes are high as captured by this quote from IT security researchers2 in Wired regarding a generally applicable USB attack:

“Physical sabotage: Tweaking an industrial robotic arm to cost millions of dollars worth of product defects, and possibly to damage the machinery itself or its human operator.”3

In addition to the industries that utilize robots there are many that also rely on operational technology (OT) networks, and they have a high reliance on the USB port. Operational technology intense industries include: oil & gas, power and utilities, chemicals manufacturing, water treatment, waste management, transportation, scientific experimentation, critical manufacturing, building management and automation, building lighting controls and automation.

These OT networks are often air-gapped, fully or in part, from the IT network to avoid the threats of the online world jumping into the network in the non-carpeted areas of organizations. Many safety standards and certifications such as ISO 27001 require this air-gap, between IT networks and OT networks, to be handled in a controlled manner. The OT networks contain ICS (Industrial Control Systems) often structured as a SCADA (Supervisory Control And Data Acquisition) system/network or a DCS (Distributed Control System). These will contain robots, PLC (Programmable Logic Controllers) and IIoT (Industrial Internet of Things) devices that may need to receive or submit data loads over a USB mass storage interface.

---

3 https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/
USB SECURITY PROBLEMS

The standard USB mass storage interface in itself offers very limited security controls. A USB device that presents itself according to the USB standard will in general, gain full access to the parts of the host system that are warranted by the device type, be that as a mass storage device or keyboard. This general trust enables, for example, the rise of the highly useful OTP (One Time Pass) devices such as the Yubikey which injects an authentication string via USB over the HID (Human Interface Device) protocol. It is the same general trust that introduces the attack referred to as the BadUSB or USB Killers that we will now explore. But before we get ahead of ourselves let’s sort the possible attacks into some main categories.

Malicious hardware

The main offender of breaking the trust of the USB protocol is what is referred to as the BadUSB. These devices are, in short, imposters. They pose as trusted devices but, in fact, carry a malicious attack often in the form of a keystroke injection attack. The poster child for this type of attack is the RubberDucky produced by Hak5. At one point even the Yubikey could be retooled to carry a malicious payload. By no means are these the only culprits as others have utilized general purpose computing platforms such as the Arduino or Raspberry Pi to mount the same attack. The knowledge and financial threshold for an attacker is extremely low, as there are prepackaged attacks available and prices start at a few dollars.

Electrical attacks

The lack of surge protection introduces an additional trust issue for USB interfaces because they will freely offer power to anything that is plugged in. This is what spawned what is referred to as the USB Killer. The device uses the power supplied from the host machine to load up and then it zaps the electrical load back into the host machine over the power pins of the USB port. This causes a surge and often a full electrical failure of the host. The USB Killer is the equivalent of throwing a wrench into a moving machine but it is using the USB port and it leaves less traces of what maleficence has occurred. The end result is a powered down robot with no real apparent traces of what has taken place.

USB jumping malware

How do you maliciously affect an offline network? For the still unknown authors of the malware Stuxnet the answer was easy, hitch a ride with any USB drive you can find and at some point your malware will find its target industrial control system. It might take ten jumps or it might take 1000 jumps. Silently the Stuxnet bided it’s time until it one day arrived at its target, an engineering workstation, and eventually, the PLCs at Iran’s Natanz uranium enrichment facility. The attack destroyed an estimated 1,000 centrifuges. The Stuxnet attack and technology spawned more ICS specific threats, utilizing USB such as Trisis. Trisis, sometimes referred to as Triton or Hatman, is able to force a malfunction in the Triconex Safety Instrumented System (SIS), a popular logic controller made by Schneider Electric. These

4 https://www.usb.org/defined-class-codes
5 https://shop.hak5.org/products/usb-rubber-ducky-deluxe
6 https://www.blackhillsinfosec.com/how-to-weaponize-the-yubikey/
7 https://maltronics.com/collections/malduinos
8 https://hackaday.io/project/17798-diy-usb-rubber-ducky
9 https://usbkill.com/
10 https://www.cyberscoop.com/stuxnet-type-attack-airbus-cybersecurity/
11 https://www.msp360.com/resources/blog/triton-malware/
controllers are primarily used to manage physical equipment in nuclear power plants, oil and gas production facilities and paper mills. These attacks can have extraordinary consequences and as reported in 2019 by MIT Technology Review: “The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.” This prompted MIT Technology Review to name it “world's most murderous malware”. The reason for this is a high-profile attack that TechCrunch summarized as an attempt “to blow up a Saudi petrochemical plant”.

The generally applicable PCL weakness that is being utilized in these attacks is the devices lack of payload verification through cryptographic signatures as they, more or less, digest what they are presented with - provided that the format is correct.

In this context, it should also be noted that, any regular desktop computers in the OT networks of course can be infected with more standard malware attacks. An example is the Spora ransomware that was spotted in early 2020 and that can spread using generic USB drives.14

**AN INDUSTRIAL USB SECURITY SOLUTION**

Handling security in an ICS setting generally requires a multi-layered approach as recommended by NIST in the Guide to Industrial Control Systems Security; USB protections are a few pieces of what forms a complex protection puzzle. Specific to USB drive usage the ICS-CERT, the National Cybersecurity and Communications Integration Center has issued guidance specific to USB drive usage that advise users to establish strict policies for both enterprise and ICS networks. How these policies are laid out will be specific to the organizations but by creating a general practical layout based on the guidelines, we present the pieces that can be put into place depending on the scenario at hand. The physical layout of facilities and OT networks can, as we all know, differ greatly from the single industrial facility to the spread out network of an electrical grid operator. DataLocker offers professional services that can advise on specific configuration options for the case at hand.

Our general proposed solution consisting of the following pieces will meet these policy criteria by:

1. Standardizing the use of trusted, managed and secure USB devices for the OT network
2. Establishing a strict perimeter around the OT network when possible with data passing through a white station (kiosk) which is a type of boundary protection device
3. Installing USB port control software on all desktop computers in the OT network
4. Ensuring that the secure USB devices can be sanitized between usage cycles or on a set schedule
5. Scanning all files for malware and verifying the hash of firmware data loads that are destined for systems that are unable to verify the correctness of the data load themselves

We will now look closer at each piece of the proposed solution.

---

13 https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/
15 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82v2.pdf
Standardized USB devices in the OT network

Physical security controls should be in place to ensure that only selected trusted, managed and secure USB devices are allowed onto the OT network. This part of the solution takes out the threat of the malicious hardware attacks and the main attack for electrical attacks. Some OT networks will be harder to control in terms of which devices are allowed physical access so the measure often needs supporting measures to be fully effective.

DataLocker offering
Especially for OT networks the DataLocker Sentry K300 has been proven to be very effective. The keypad device can both be fully managed and audited when attached to desktops but also has the ability to mount as flat removable media with controlled standalone unlocks. The ability for standalone unlocks are crucial to allow PLCs and IoT devices to read and write data loads. The Sentry K300 also has the ability for sanitation of the media using cryptographic erasure, this is crucial to ensure the compartimalization in some networks. Cryptographic erasure can also be part of a regulatory requirement to ensure that sensitive data is destroyed once the mission is completed.

Setup boundary protection devices
The purpose of the boundary protection device or white station, is to create a gateway between the IT and OT network that will ensure a certain level of security is met for all data that passes on to the OT network. The white station will be designed to be the gatekeeper and the one device that meets the outside threats. There are a multitude of ways to set up a desktop machine to act as a white station, dependent on the criteria. In general the device should have an up to date anti-malware engine and have a high maintenance schedule for operating system updates. The standard hardware can also for example be complemented with an ESD (Electrostatic Discharge) protected USB hub which will protect the machine from any USB electrical threats. It is also advised to only allow one HID keyboard to prevent the majority of BadUSB threats.

DataLocker offering
By combining DataLocker technologies it is possible to create one or as many white stations as the policies may require. The DataLocker Sentry K300 can be set up to have onboard McAfee anti-malware running which ensures that USB jumping malware is stopped. When managing the DataLocker Sentry K300 it is also possible to limit which file types are allowed onto the OT network using a file restriction policy. Combining the Sentry K300 with the installation of PortBlocker, USB port control software, on a standard enclosed desktop further protection can be achieved. The PortBlocker can be set up to only allow read operations from devices coming onto the white station machine.

Control the USB ports whenever possible
Whenever possible, limit access to USB ports on PLC and computing devices that cannot be outfitted with port control software, this can be achieved with locked cabinets or physical USB lock plugs. For any standard operating system port...
control software should be installed. The logic behind this threat prevention is straightforward, by limiting the access to the port you limit the threat posed by non-approved USB devices.

**DataLocker offering**

PortBlocker port control software should be installed on all compatible machines in the OT network and IT network to enforce that only the allowed standardized devices are able to connect as USB mass storage.

**Data sanitization of storage devices**

One reasonable measure to prevent the spread of malware is to make sure that the used storage devices are wiped clean of data on a regular basis. This ensures clean control points in the operation but it can also be part of regulatory compliance to be able to prove that sensitive data is not stored indefinitely on removable media. Regular USB drives are what is referred to as data hoarders as they are built to ensure maximum life span of the device, this means that a regular storage device will only overwrite data sectors when it is absolutely necessary, no matter if the file allocation table (FAT) displays a “clean” device. This “data hoarding” has an unfortunate consequence of the regular USB device - to expose as much data as possible when it goes missing.

**DataLocker offering**

Hardware encrypted devices from DataLocker solve the complicated sanitization issue by using a method called cryptographic erasure. In short, it refers to destroying the current encryption key used to decrypt the currently stored data and generating a fresh key, the process ensures that the media is clean to meet the NIST 800-88 Guidelines for Media Sanitization. Most territories have similar standards to NIST and it can be generally said that a complete cryptographic erasure is the fastest and most effective erasure possible.

**Anti-malware and data load verification**

The white stations and any compatible end points in the OT network should be outfitted with at least one layer of anti-malware protection. The measure combats the malware in general but specifically also the malware that uses USB as a seeding mechanism. Furthermore any data loads destined for PLCs or machines that are unable to validate the data loads should be pre-verified on the white stations. This pre-verification can be achieved by verifying cryptographic signatures or hashes provided by the software vendor. This step ensures that the data loaded on the machines is the exact copy of the data intended to be delivered by the software developer.

**DataLocker offering**

The Sentry K300 from DataLocker offers both onboard McAfee anti-malware and file restrictions based on file types. The device allows an administrator to verify the MD5 hash of any stored data on the device ensuring that only the correct data loads reaches the PLCs.

---

Building the business case for better USB security

Through this short paper it has been proven how improved USB security bolster the safety, reliability and availability of industrial control systems with steps that are not invasive in terms of productivity. Having said that, about the carrot, the stick in an industrial setting is often much more dramatic than it is in an IT network. The physicality of the industrial environment often means that lives, equipment, output and surroundings can be impacted by security lapses. We have displayed that the risks of unmanaged USB usage can be significant and should not willfully be overlooked.

The exact business case will need to be adjusted for the scenario at hand and DataLocker’s partners, professional services and sales team can assist you with recommendations and pricing. This will allow you to build your business case with precision to arrive at a well-thought out and developed security implementation and cost plan.