Why Use of USBs are Not Worth the Potential Risks

White Paper

Introduction

The common practice of using USBs for ease in transferring data to industrial control systems of critical energy infrastructures can introduce cybersecurity risks. The focus of this paper is in highlighting examples of cyberattacks that were initiated by introduction of a USB onto a system connected to a critical infrastructure, along with the strong recommendation against use of USBs and the need to train personnel in their usage and associated risks.

Background

North American Electric Reliability Corporation (NERC) [1] is a non-profit international regulatory authority focused on assuring the reliability and security of bulk power systems in North America. One of the programs NERC has created is for Critical Infrastructure Protection (CIP), which has evolved to become the de facto standard for security for many utilities all over the globe. Specifically it includes guidance covering the security of electronic perimeters and protection of cyber assets. The equivalent standard in Europe is the European Programme for Critical Infrastructure Protection (EPCIP) [2]; the Central Regulatory Authority, India [3] is also expected to develop India-specific standards aligned to global best practices for utility security in the near future.

As per NERC CIP guidelines, use of USB or USB type ports is strongly discouraged because a USB port is not immune to protection from “unauthorized access”. It would be helpless against connecting modems, network cables that bridge networks or insertion of an infected USB pen drive.

Cyber protection for USB ports can be enforced, however, it is often cost prohibitive and is not one hundred percent effective. There is no essential requirement for using a USB instead of other standard and more secure interfaces such as Ethernet and serial ports.

Some of the common methods to protect the USB ports are:

- Disabling (via software) the physical ports
- Prominent physical port usage discouragement such as a port cover plate or tamper tape
- Physical port obstruction using removable locks

These measures are examples of defense-in-depth methods, but the CIP guidelines acknowledge that these control approaches can be easily circumvented. It is also not uncommon for an employee or authorized contractor to inadvertently compromise a device simply by plugging in an infected smart phone to charge the battery.

USB flash drives pose two major challenges to critical infrastructure cybersecurity: ease of data theft owing to their small size and transportability, and system compromise through infections from computer viruses, malware and spyware. It is well documented that a seemingly harmless USB supported portable peripheral device can trigger a massive cyberattack, even when the computer system targeted is, in theory, isolated and protected from the outside with firewalls and other types of security devices.

According to a SanDisk Corporation commissioned study [4], data files that are copied to USB flash drives represents a significant risk of data loss. The study revealed that corporate data files on flash drives includes: customer records (25%); business plans (15%); employee data (13%); intellectual property (6%) and source code (6%). The survey also indicated that 40% of the companies lacked a policy forbidding corporate data on portable devices.

What a US Power Grid Attack Could Mean

Lloyd's Emerging Risk Reports are a well-known and reputable industry reference for quantifying risks in strategic sectors. One of these reports, "Business Blackout" [5], is an impressive study of the hypothetical impact of cyberattack which causes a widespread blackout, plunging 15 US states into darkness and leaving 93 million people without power.

In the scenario, a piece of malware (the 'Erebos' trojan) infects electricity generation control rooms in parts of the Northeastern United States. The malware goes undetected until it is triggered on a particular day when it releases its payload which tries to take control of generators with specific vulnerabilities. It identifies 50 generators it can control, and forces them to overload and burn out. This temporarily destabilizes the Northeastern United States regional grid and causes some sustained outages. While power is restored to some areas within 24 hours, other parts of the region remain without electricity for few weeks.

Economic impacts include direct damage to assets and infrastructure, decline in sales revenue to electricity supply companies, loss of sales revenue to business and disruption to the supply chain. The total impact to the US economy is estimated at $243B, rising to more than $1T in the most extreme version of the scenario with insurance payouts reaching at least $71B.

Cybersecurity Threats – Real Life Examples

The prevalence of malware infection by means of a USB flash drive was documented in a 2011 Microsoft study [6] analyzing data from more than 600 million systems worldwide in the first half of 2011. The study found that 26 percent of all malware infections of Windows systems were due to USB flash drives exploiting the AutoRun feature in Microsoft Windows.

As USBs have become a common method in easily sharing information locally between devices, they have become a common source of information system cyber compromise.

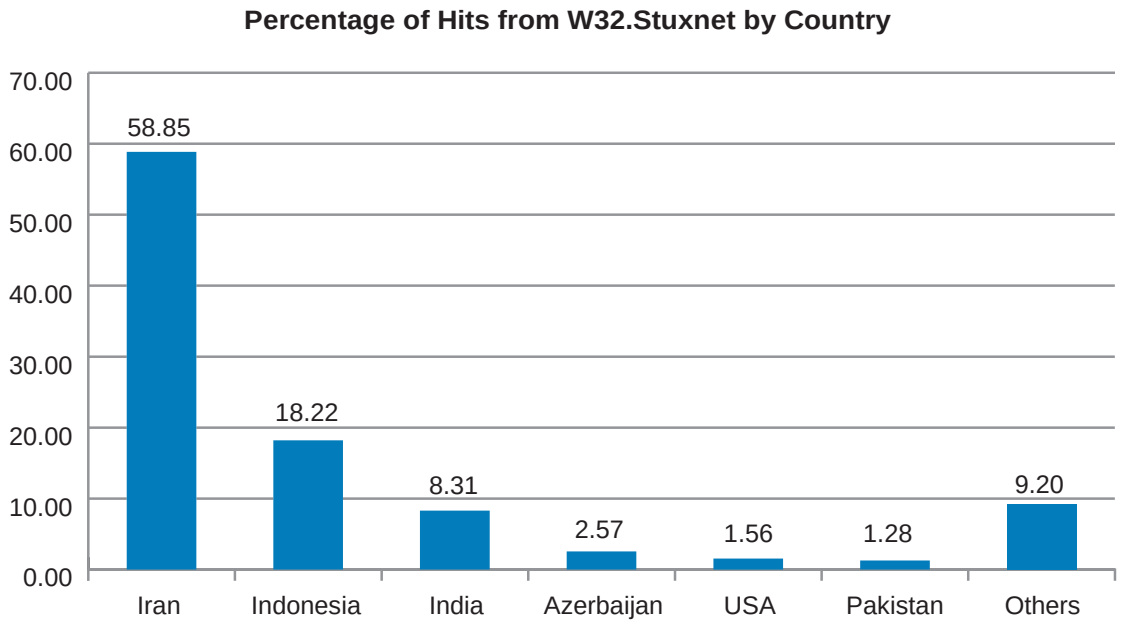
Struxnet Worm

A classic example of how a USB port can be used to spread a cyberattack is the well documented Struxnet worm that specifically targeted SCADA systems. It was responsible for causing significant damage to Iran's Natanz nuclear facility, destroying a fifth of the nuclear centrifuges by causing them to spin out of control.

Struxnet was introduced tothetarget environment via an infected USB flash drive. Itthen proceeded to infect all computers running Microsoft Windows OS and remained dormant and hidden as it made copies of itself. By using a digital certificate that implied it came from a reliable source, the worm circumvented virus scanning systems. After propagating across compromised networks, it scanned for computers that were part of the industrial control system made by Siemens. Upon a successful scan, the worm attempted to access the Internet and download a more updated version of the worm. The worm targeted logic controllers exploiting zero day vulnerability software weaknesses. Initially, Struxnet monitors operations of the targeted system and then uses that information to take control. In the instance at the Iran nuclear facility, it modified the control system and generated unexpected commands to the PLC while returning a loop of normal operations system values feedback to the command center. Since the operational feedback from the PLC was programmed by the malevolent agent as normal conditions, no alerts were triggered until its programmed destruction cycle was executed and the damage had been done.

Significantly, according to a paper presented at the 37th Annual Conference of the IEEE Industrial Electronics Society, Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern Supervisory Control And Data Acquisition (SCADA) and PLC-like systems.

According to public domain data and Symantec information, multiple countries were targeted by Struxnet.



Source: Symantec [7]

According to papers presented as recently as Oct 2017 in the 4th Annual Industrial Control Cyber Security Europe, USB are and continue to remain the number one source for Malware. Even International Space Stations (ISSs) [8] have fallen victim to malware introduced by a compromised device brought on board and connected to the main system.

The fact that even an ISS, with its safety protocols and limited number of visitors and strong access controls has been subject to infection via USB devices, should clearly illustrate the risk any utility could confront and experience.

BadUSB

A USB, in addition to disk space, includes firmware since it is inherently a microcontroller with writable storage memory registers. This firmware however can be embedded with executable codes which cannot be verified by third party security software applications since the firmware is not open source. This flaw in USBs opens the door to modification USB firmware, which can easily be done from inside the operating system, and hide the malware in a way that it becomes almost impossible to detect. The flaw is even more potent because complete formatting or deleting the content of a USB device won't eliminate the malicious code, since its embedded in the firmware.

Cyber Activists (researchers Adam Caudill and Brandon Wilson) have already loaded complete source code of BadUSB in popular software sharing site, Github, to nudge USB manufacturers to open up remedial counter measures *("We really hope that releasing this will push device manufactures to insist on signed firmware updates")*.

According to Wired, a leading emerging technology magazine, the vulnerability is "practically unpatchable" and undetectable by Anti Virus Software because it exploits "the very way that USB is designed." Once infected, each USB device will infect anything it's connected to, or any new USB stick coming into it. It also made Wired's list of top five dangerous software bugs of 2014 [9].

Once compromised, the USB devices can reportedly:

- enter keystrokes
- alter files
- affect Internet activity
- infect other systems and then spread to additional USB devices
- spoof a network card and change the computer's DNS setting to redirect traffic
- emulate a keyboard and issue commands on behalf of the logged-in user, for example to infiltrate files or install malware

Patches made for BadUSB have been largely ineffective [10] and a fix is years away.

Conclusion

For all critical energy infrastructure entities, Kalkitech strongly suggests that devices be protected against vulnerability to malicious agents like the ones illustrated above. Complete elimination of the need for a USB port is advised and recommended in the interest of reliable and safe operations. Kalkitech is committed to helping ensure a secure and intelligent grid and strives to fulfill its responsibility to customers worldwide.

About Us

Kalkitech offers a line of products and services that securely bridge the data communications gap between legacy and intelligent power utility field devices and head-end systems, transparently across multiple vendors. By transforming and accelerating accessibility to real-time data and analytics, our solutions help utilities improve system reliability and operational efficiencies while extending the life of legacy SCADA systems.

WHITE PAPER

References

[1] http://www.nerc.com/Pages/default.aspx
[2] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
[3] http://www.cercind.gov.in/
[4] https://www.sandisk.in/about/media-center/press-releases/2008/2008-04-09-sandisk-survey-shows-organizations-at-risk-from-unsecured-usb-flash-drivesusage-is-more-than-double-corporate-it-expectations
[5] https://www.lloyds.com/search?q=The%20insurance%20implications%20of%20a%20cyber%20attack%20on%20the%20US%20power%20grid&spell=1&
[6] http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf
[7] https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
[8] http://www.dailymail.co.uk/sciencetech/article-2503352/Russian-cosmonaut-accidentally-infected-International-Space-Station-USB-stick.html
[9] https://www.wired.com/2014/12/most-dangerous-software-bugs-2014/
[10] https://www.wired.com/2014/10/unpatchable-usb-malware-now-patchsort/

Kalkitech

Corporate Headquarters: **Bangalore, India**

U.S. Headquarters: **Campbell, California**

Sales Office: **United Arab Emirates**

www.kalkitech.com

sales@kalkitech.com

Version: 1.01.122017