Cyber Security Relating to Touch Technology

A D Metro White Paper

A D Metro

1390 Star Top Road
Ottawa, Ontario, Canada K1B 4V7

Website: http://www.admetro.com/
Support: support@admetro.com
Sales: sales@admetro.com
Tel: +1 613 742 5545
1 800 463 2353 (US, Canada)
Fax: +1 613 742 5245

Table of Contents

Introduction

A D Metro was established in 1993 in Ottawa, Canada. The company's expertise is in touch screens and currently, it is one of the few remaining North American based touch sensor manufacturers. A D Metro is a world leader in the production of ULTRA, a patented glass/film/glass resistive touch screen. A D Metro has also advanced touch technologies with its recent development of Linear Correlating Infrared (LCIR), Multiplexed Projected Capacitive (MPC) and 2-Touch 5Wire Resistive technologies.

Cyber security has primarily focused on the software side of potential threats. Firewalls, antivirus and malware products typically tend to look for threats entering in through the internet or malicious programs running from memory or residing dormant on a hard drive. As these methods become better understood over time, it becomes more difficult for hackers to design a successful attack as system vulnerabilities all become identified and fixed. Some systems designers believe that isolating their local networks from the internet can provide an impenetrable level of security from external threats. That concept may be somewhat misplaced given how attacks with removable media (such as USB devices) have been seen to reach networks that are disconnected from the internet.

With software attacks becoming increasingly difficult, hackers are turning to hardware to provide a pathway to system intrusion. For example, we are all familiar with ongoing allegations of spyware in 5G cellular equipment. There have also been reports of spy chips compromising some Apple® and Amazon® server computers. Also, experts estimate vast numbers of computers being infected by removable media - around four million users worldwide in 2018 alone (Kapersky, 2018).

Financial, security and military customers are elevating their attention to hardware intrusion threats. All companies with sensitive intellectual property to protect need to increase their level of vigilance as well.

Infection and Attack Mechanisms

Electronic hardware, including USB devices, are a significant cyberthreat tool. Kaspersky Lab reports that about one in four users worldwide was affected by a ‘local’ (not introduced over the Internet) cyber incident in 2017 (Kapersky, 2018). Some of these ‘local’ attacks are caused by removable media like USB devices. Even a USB drive that starts out clean can become infected (and subsequently spread malicious software) after being inserted in an infected computer which loads malware onto the portable drive (Mills, 2008).

USB Infection Mechanisms

There are many ways that USB devices can infect computers with viruses, worms or other malicious software. These include:

- A USB drive that contains phishing HTML files. If the user clicks on such a file, a browser opens and requests sensitive information such as login and password text. Also, on this less elaborate end of the hacking scale, a USB drive can contain a malicious program that gets executed by the operating system AutoRun feature upon insertion.
- A virus can also be embedded in a benign looking file on the USB drive, and infect the computer when opened by the user through an operating system vulnerability (Mills, 2008). Files with the LNK extension are normally Windows shortcuts. These can be made to activate malicious programs. Among the most common viruses to act this way are the Windows LNK family of Trojanware. Typically, trojanware opens up an Internet browser to a predefined malicious web page (Wikipedia, 2017).
- A more complex malicious USB device might use Human Interface Device (HID) spoofing, fooling a computer into believing that the USB device is a keyboard. This fake keyboard might inject keystrokes perhaps as it is plugged into the computer. The keystrokes can be a set of commands that compromise the computer. The malicious device can ‘type’ anything that a user can type. In one known example, the harmful device spawns a process (a reverse TCP shell) to give full remote control of the attacked computer over the internet. USB devices with these damaging capabilities were demonstrated as far back as 2010 (Bursztein, 2016).

It is an unfortunate feature of the USB protocol that device firmware doesn’t have safeguards comparable to normal software such as ‘code-signing’ to ensure the unforgeable cryptographic signature of the manufacturer. There isn’t even standard trusted USB firmware against which to compare (Valcarcel, 2014).

Some Known USB Attacks

Almost any type of USB device (for example: lights, fans, speakers, toys, keyboards, mice and more) can spread malware. Even devices designed without malicious intent can be infected during fabrication or shipping unless these assembly processes are carefully monitored and controlled (Mills, 2008). Touch screen controllers are no exception. Like any other USB device, they can be designed or altered to have any of the malicious features found in these discovered, widespread attacks.

- The ProjectSauron and Strider cyberespionage tools used partitioned USB data storage that left hidden, unused space. This hidden storage helped with removal of data from computers and networks isolated from the Internet (Kapersky, 2018) (GReAT, ProjectSauron, 2016).
- The attack known as Dark Tequila illustrated a higher level of sophistication. This malware acted for five years before it was detected, perhaps because it included features to evade detection. For example, the multi-stage attack payload avoided spreading infection when security (anti-virus) software was present or when it detected that it was running in an analysis environment (GReAT, Dark Tequila Añejo, 2018). The attackers even uninstalled the malware from computers that were not of interest. This malware contained a variety of different modules. Its operation was strictly monitored and controlled by the attacker at a remote server who decrypted and activated particular modules to receive stolen data. (Kapersky, 2018).
- Perhaps the most sophisticated widely known USB attack was the Stuxnetworm in 2010. In this attack, USB devices containing shortcut and LNK files were used to infect an Iranian nuclear facility. (Kapersky, 2018). Remarkably, this attack employed six separate Windows vulnerabilities, four of which were previously unknown. It included a system to hide its own presence, a worm to spread widely and highly specialized malware to target only very specific systems (Wikipedia, 2019). Designers of the Stuxnetworm are not the only sophisticated group in existence. Some of the same vulnerabilities used in this attack have also been exploited by "other advanced threat actors, including Equation Group, Flame, Regin and HackingTeam" (Kapersky, 2018).
- The leading edge of USB espionage might have been revealed through Edward Snowden's leaks. These detailed a 2009 NSA spying device known as Cottonmouth. Reportedly, the tiny device was capable of hiding in practically any USB plug and infecting a connected computer with malware then subsequently communicating covertly with that malware. It is said to have its own RF link to communicate with the attacker, even allowing reprogramming to change its behavior and the malware behavior (Cottonmouth-I Product Data, 2007).
- There have been reports of manufacturers altering product designs and hiding malicious microchips on circuit boards. The microchips were reportedly very small, shaped to resemble harmless capacitors rather than microchips and colored gray or off-white, again to resemble capacitors instead of integrated circuits. Malicious microchips have even reportedly been assembled and connected in between the layers of fiberglass circuit board material itself (Riley, 2018).

The many ways that USB devices can be altered to compromise computers highlights the importance of carefully selecting and monitoring the supply chain for any USB devices that you put into service.

Specific Touch Screen Concerns

Touch screens are uniquely positioned to have direct access to sensitive information. For example, as users enter pin codes, IDs, user names and passwords, those touch locations are handled by the touch screen controller. Touch screens are therefore a potential security risk regardless of how they interface to a system electrically (USB, I^2C, TTL, RS-232 or other). A malicious touch screen might attempt system attacks through the electrical interface. Alternatively, a touch screen controller might compromise a system by incorporating (or being modified to include) malicious extra hardware such as a radio transceiver.

While a piece of software can be certified and this certified code can be electronically verified, this same level of protection is not possible with electronic hardware such as a touch screen controller. There is no general way to electronically confirm that an electronic assembly has not been altered.

It is easy to imagine a malicious touch screen (or a normal touch screen with malicious modification) containing a hidden radio transceiver that is able to communicate a long distance. There are many readily available, compact radio transceivers able to communicate over 1 km in the 400 MHz to 5 GHz range. The invisible conductive traces of the touch sensor itself might be used as the radio antenna, making protection by shielding of radio signals impossible. The radio could either respond to inquiry from a nearby hacker's device or occasionally attempt to link up with, or send information to such a device. Aside from walking away with sensitive information, a hacker could conceivably even remotely enter touches to a system.

Clearly, thoughtful security decisions need to be made before incorporating any hardware into a system design - especially those that need to be secure.

At A D Metro, we pay careful attention to our product components and keep tight control over our North American manufacturing facility to ensure no malicious hardware or software hacks invade your system through any of our products. Know your source of hardware supply. It should be treated with the same threat level consideration as any other aspect of your security system. Always buy from known and trusted sources. Cheap cost should never be a determining factor in these instances. Indeed, cheap pricing is a tool that bad actors may employ to entice you to buy compromised product.

Glossary

2-Touch 5Wire Resistive technology – Resistive touch screen technology with enhanced control capability to provide 2-touch capability, invented by A D Metro (patent pending).

5G – The fifth generation of cellular network technology.

Attack Payload – The component(s) of a virus or malware responsible for executing the malicious activity. The activity may be unauthorized data acquisition or data modification or opening of unauthorized external access, for example.

AutoRun – Component of the Windows Operating System that dictates what action the system takes when a drive is connected.

Code-Signing – The process of digitally signing executable files to confirm the author and guarantee that the code has not been altered since it was signed.

HID - Human Interface Device – A category of USB device for those devices that accept input from humans or present output to humans.

HTML files – Files that contain HyperText Markup Language – the standard language for documents intended to be displayed using a web browser.

I^{2}C – 'Inter-Integrated Circuit' serial bus communication protocol.

LCIR - Linear Correlating Infrared – Fully sun-tolerant, dual-touch infrared touch screen technology invented by A D Metro (patent pending).

LNK Extension – The computer filename extension ".LNK" – used in the Windows operating system to indicate a file that is a Windows shortcut.

Malware – Any Software intentionally designed to cause damage to any computer or computer network.

MPC - Multiplexed Projected Capacitive – An advanced form of projected capacitive (PCAP) touch technology that has robust interference tolerance and simple cable connection, invented by A D Metro (patent pending).

NSA – National Security Agency of the United States.

Phishing – Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.

Removable Media – A form of computer storage designed to be inserted and removed from a system.

Reverse TCP Shell – An Internet communication link opened by a computer to accept commands or code from a remote computer. Having the link opened by the local computer often bypasses firewall restrictions.

RS-232 – Recommended Standard 232 – A longstanding standard for electrical communication using serial transmission of data.

Spawning – Loading and executing a new computing process.

Spoofing – A program masquerades as another by falsifying information.

TCP – Transmission Control Protocol – one of the main communication protocols used for Internet communication.

Trojanware – Any malware which misleads users of its true intent. It is common for such malware to open up an Internet browser to a predefined page.

TTL – Transistor-transistor logic. A current-sinking based logic standard for communication (typically) at the integrated circuit level.

ULTRA - Glass/film/glass resistive touch screen technology invented and patented by A D Metro.

USB – Universal Serial Bus – An industry standard for communication between computers, peripheral devices and other computers.

Virus – A type of malware capable of replicating itself by modifying other computer programs and inserting its own code.

Windows Shortcut – Typically a small computer file that represents an executable computer program that is located in a different directory or folder.

Worm – A standalone malware computer program that replicates itself to spread to other computers.

Bibliography

Bursztein, E. (2016, August). *Understanding malicious USB attack vectors - What are malicious usb keys and how to create a realistic one?* Retrieved from elie.net: https://elie.net/blog/security/what-are-malicious-usb-keys-and-how-to-create-a-realistic-one/

Cottonmouth-I Product Data. (2007, January 8). Retrieved from Electronic Frontier Foundation: https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf

GReAT. (2016, August 8). *ProjectSauron*. Retrieved from SecureList: https://securelist.com/faq-the-projectsauron-apt/75533/

GReAT. (2018, August 21). *Dark Tequila Añejo*. Retrieved from SecureList: https://securelist.com/dark-tequila-anejo/87528/

Kapersky. (2018, September 25). *USB threats from malware to miners*. Retrieved from SecureList: https://securelist.com/usb-threats-from-malware-to-miners/87989/

Mills, E. (2008, November 20). *USB devices spreading viruses*. Retrieved from CNET: https://www.cnet.com/news/usb-devices-spreading-viruses/

Riley, J. R. (2018, October 4). *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*. Retrieved from Bloomberg Businessweek: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Valcarcel, J. (2014, July 31). *Why the Security of USB Is Fundamentally Broken*. Retrieved from Wired: https://www.wired.com/2014/07/usb-security/

Wikipedia. (2017, May 27). *Trojan.WinLNK.Agent*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Trojan.WinLNK.Agent

Wikipedia. (2019, July 20). *Stuxnet*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Stuxnet