Exploiting SCADA vulnerabilities using a Human Interface Device

Grigoris Tzokatziou
School of Computer Science and Informatics
De Montfort University, Leicester, UK

Leandros A. Maglaras
School of Computer Science and Informatics
De Montfort University, Leicester, UK

Helge Janicke
School of Computer Science and Informatics
De Montfort University, Leicester, UK

Ying He
School of Computer Science and Informatics
De Montfort University, Leicester, UK

***Abstract*—SCADA (Supervisory Control and Data Acquisition) systems are used to control and monitor critical national infrastructure functions like electricity, gas, water and railways. Field devices such as PLC's (Programmable Logic Controllers) are one of the most critical components of a control system. Cyber-attacks usually target valuable infrastructures assets, taking advantage of architectural/technical vulnerabilities or even weaknesses in the defense systems. Even though novel intrusion detection systems are being implemented and used for defending cyber-attacks, certain vulnerabilities of SCADA systems can still be exploited. In this article we present an attack scenario based on a Human Interface Device (HID) device which is used as a means of communication/exploitation tool to compromise SCADA systems. The attack, which is a normal series of commands that are sent from the HID to the PLC cannot be detected through current intrusion detection mechanisms. Finaly we provide possible counter measures and defense mechanisms against this kind of cyber attacks.**

***Index Terms*—SCADA; Cyber Security; HID; PLC**

I. Introduction

One of the biggest issues that SCADA systems face is that they were designed to work solely in their environment segregated from inter-connected IT networks or ad-hoc systems. The primary reason for this is that there was no need for remote access at the time of their introduction. However, nowadays organizations want to establish local convenience or remote access, which will enable them to take decisions on production changes and apply them quickly from a centralized location rather than have to travel to different locations in order to make changes to their ICS systems. This interconnection of Industrial Control System (ICS) networks with organizational ICT network infrastructures, and even with the exterior has brought a new wave of security problems and attacks. In fact, the number of externally initiated attacks on ICS systems has increased much more rapidly than internal ones [1].

Moreover, SCADA communication protocols, which are responsible for the interaction between field devices, such as PLC (Programmable Logic Controller) or RTU (Remote Terminal Unit) components and the stations that control and monitor them, pose security concerns [2]. One such example is the Modbus protocol, originally developed by Modicon. Modbus messages are exchanged between entities by using TCP, which imposes more complexity with regard to managing the reliable delivery of packets in a control environment with strong real time constraints. In addition, it provides attackers with new avenues to target industrial systems [3]. Modbus is one of the most popular protocols for SCADA applications, but it suffers from security problems such as the lack of encryption or any other protection measures which thus exposes it to different vulnerabilities.

Serial communication has not been considered as an important or viable attack vector, but the researchers say breaching a power system through serial communication devices can be easier than attacking through the IP network since it does not require bypassing layers of firewalls [4]. Potential attackers use common vulnerabilities in order to put controlling servers into infinite loops. This case is not the same as not having access to the field network, but it could mean that the operators are not aware of the conditions on the ground. The worst of the vulnerabilities exposed so far enables a potential buffer-overflow attack, whereby code stored for one purpose overflows its container, and can end up being executed in different time instances than programmed to or in a different way. This allows for malicious code to be injected into control servers, giving access to attackers to the control system.

Modern intrusion detection systems (IDSs) focus mainly on analyzing the traffic that flows in the network. By capturing behaviour or traffic patterns in the network, misbehavior is detected and dedicated security events are reported. IDSs can be classified into centralized intrusion detection systems (CIDSs) and distributed intrusion detection systems (DIDSs), according to the way in which their components are distributed. Due to the rapid increase of sophisticated cyber threats with exponentially destructive effects, IDSs are systematically evolving [5], [6]. Among other approaches, neural networks, support vector machines, K-nearest neighbor (KNN) and the Hidden Markov model can be used for intrusion detection, while existing signature-based network IDS, such as Snort or Suricata can be effective in SCADA environments. However, most of the approaches that have been introduced recently cannot deal with attacks that come straight from serial communication devices.

In this article we investigate the vulnerabilities of a SCADA system and perform an attack directed to an ABB PM564 PLC, using a HID . The Teensy device used is an Arduino based one that allows the user to utilize onboard memory storage on a microcontroller and to emulate a keyboard/mouse. By using this HID device (see Figure 1) we can bypass any autorun protections on the system since it is shown as a keyboard that is connected to the workstation. By sniffing the packets that are exchanged between the HMI and the PLC we manage to extract the information of a STOP command, replicate it and store it in a web host. As the PLC has been set to run, we insert the Teensy HID device into the engineer's machine, or a machine connected to the same subnet. Once the Teensy USB has been plugged into the system, it waits for a specific amount of time in order to download the code and execute it. The attack, although primitive, cannot be detected by any current IDS as it involves the execution of a legitimate 'STOP' order from an authorized device.

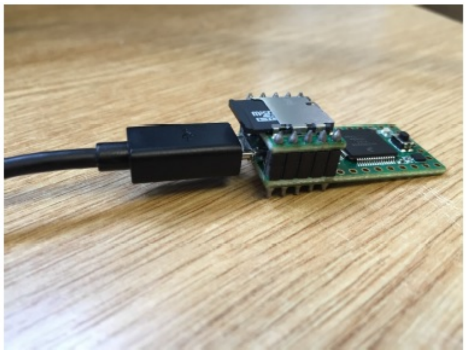

Fig. 1: Teensy HID

II. EXISTING SOLUTIONS

The current defense mechanisms that IT systems currently employ do not offer security to SCADA systems, this is primarily to the fact that SCADA systems were intended to be isolated from IT infrastructures. Using current IT security measures directly to SCADA systems does not solve the issue, with latency being one of the major concerns when using a firewall within SCADA systems.

A. Segregation and Perimeter Security

In order to create a secure network the perimeter needs to be fully identified and secured first. This traditionally is achieved, by firewalls but as this is not simply an IT system we take the perimeter as the wall that stands between the corporate network and also the external network (Internet). One of the best techniques to avoid unauthorized access from different devices/users of a network is to segregate the network. This way administrators can control the way traffic can flow and which part of the network can communicate with another part (i.e corporate network/management network)[9].

By segregating the network into different areas, the routing of information is controlled, policies can be created specific to the network, more security controls can be available in areas where it was not possible before, and from a monitoring prospective it is also easier to monitor specific parts of the network. ISA-SP99 Part 1-Terminology [10] concepts and models, recommend the use of ”Zones and conduit” model. This involves separating the networks by using groups. This model defines the assets that need to be inserted in each group, and when this is done, the groups containing assets that match based on some criteria, are put in the same zone, otherwise they are separated. From a security perspective it is also better to have a zoned approach, because if there is a breach on one part of the network it may be possible to protect the other sections.

B. Firewall/IPS

A Firewall/IPS is a system which can be configured to allow or deny traffic from location to location or from a host to a network e.t.c. This system has a rules database which is explicitly created for the specific organization; generic rules may still apply but may also leave important areas or parts of the networks unprotected. The general rule when using a firewall is to close all the ports, and only enable the ones that you need. Although generally firewalls are supplied with some well-known ports open by default. An IPS on th other hand has greater capabilities than a firewall. It is able to see anomalous traffic via signatures and it can take an action based on it's predefined rules, to either drop, alert, log or allow traffic to flow.

A firewall works more with protocols rather than just ports. It does this by inspecting the packet, looking at the destination port and the protocol, and if these do not match to a predefined rule it will drop the packet, or otherwise it will be let to pass. Deep packet inspection for encrypted traffic is not available to the general public and only government-based organizations will have access to such hardware in order to do some real-time analysis and decryption of data packets. Deep packet inspection can be very beneficial. MODBUS TCP protocol which is used by PLC's can be analyzed for behavioral changes; for example, the HMI should be able to read values from a PLC but not write, if this behavior occurs then a red flag should be raised.

C. Honeypots

The definition of a honeypot ”A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource” is given in [11]. The idea of the honeypot is to emulate a real network and attract attackers so that a company/business can predict how an attack evolved and the type of the actual attack. This way they can mitigate the risks and prevent them from occurring in real systems. There are different types of honeypot systems that could be used, the main types are low-interaction honeypots and high interaction honeypots. The major difference of the types of honeypots is described in the ability of an attacker to interact with the application or service.

D. IDS systems

The use of Intrusion Detection Systems in SCADA is recommended as they are able to scan the protocols which ICS systems use. Some of these protocols are MODBUS, DNP3, and TCP/IP (Ethernet). One of the best and well-known IDS system is SNORT. This IDS has SCADA preprocessors, which can sniff data packets and provide alerts or logs if there is an appropriate rule/signature for that type of packet. It is generally good practice to put IDS systems in between networks and not for example at the gateway, as threats may not necessary come directly from the outside. An IDS should be in front of the gateway which allows communications between two or more networks, and the IDS needs to be configured so that the alerts produce only relevant data and not false-positives. This system should be integrated in a Security Operations Environment (SOC) and a Security Information and Event Management (SIEM) system, so that data can be examined. It is important to state that an IDS will not block or drop any packet.

E. Air-gaps

This method is advisable but highly unrealistic in today's world. Disconnecting means simply un-plugging one network from the internet, in other words you need to separate and isolate the SCADA network from the corporate network making that way impossible to access remotely that network from the outside. This technique was used in SCADA before the idea of remote access. Although segregating and air-gaping primarily have the same concept, the main difference is that when apply air-gap policy you physically remove any links to and from the two networks, whereas segregating does involves mostly logically dividing a network.

F. DMZ

De-militarized zones is a good practice of increasing the security in a network. The idea is that you leave systems on a part of the network which you wish to allow the public to access. These systems can be viewed by the internal network but systems in the DMZ can not access the internal network, so it is a one-way system if it is configured appropriately.

G. VPN

virtual Private network connection can also be used in SCADA systems. These systems need to connect to a network which allows the IPSec protocol, as most SCADA systems mainly use MODBUS and TCP/IP this can be supported as an add-on. In terms of Firewall and IDS detection, using a VPN will not have a significant effect. Essentially more rules are added to the IDS firewall which are used in order to monitor connections coming to and from the VPN.

H. Network Access Control

The most important mechanism into creating a secure architecture is network access control policies. This policy is used in order to establish which devices are allowed to communicate with one another, what limitations these devices need, what type of access do they need i.e. read/write, which ports they can communicate with, what type of protocols do they use e.t.c. The types of authentication that can be used or are supported by the hardware already in place, are sometimes missed and can provide a pivotal point of access to intruders if omitted or miss-configured.

I. VLANs

VLAN's are local area networks that map workstations on different basis rather than geographical location. These are not suitable security mechanisms for segregation, due to the fact that there have been reported numerous VLAN hopping attacks. During these attacks communications which should not be accessible from one VLAN to another were possible reducing the security level of the system.

J. Redundancy

Redundancy is sometimes missed when creating a security architecture, but it can be catastrophic if it is not in place. When doing a security audit you need to asses which hardware or devices are critical to the ICS processes. Risk assessments provide such audit and point out the most critical components of the network. Redundancy allows a better up time if a critical component failed, as it would mean that the business will only be halted for a short period of time.

K. Host-Based Security

The weakest link to any security architecture are people, although it may be an un-intentional mistake or they might fall victims of a social engineering attack without their knowledge. A good example of an attack that originated from within the system is Stuxnet. This worm made subtle changes to the process of the ICS systems at the Nuclear Enrichment programme in Iran, and although it was very sophisticated, it could have been prevented if the company had white listing tools, that stop an unknown executable or DLL from running if it is not listed as a know process. This type of attack required an excellent knowledge of the systems in place and also the current security that the plant had in place.

Although the above mechanisms are useful for protecting a network from known attacks, they don't prevent attacks such as Zero-days attacks. Organizations can use a lot more techniques / methods in order to raise their security level. OS hardening is primarily seen as the security solution, essentially it indicates that the Operating system needs to have all the latest security updates in place and security policies. Periodic backup also is essential, since if a device or a O/S fail, the company can revert back to their backups and be up and running again. Device control, which can also be used as a security measure, means that no unauthorized external devices should be plugged into computers which are used to control field devices, or any other critical device. Software white listing is also recommended. The SANS Institute recommend the use of tools which will only allow application/process to run from the list created by an administrator, any file that is not on the allowed list will not be permitted to run. This typically prevents viruses from executing, since the virus process will not be on the white list tool and it simply will not execute.

User access control and authentication is one of the most important steps in securing the network. Knowing who to trust and which privileges to allow is a very important aspect. By limiting the ability of users on the operating system, even if they are compromised their account limitation may prevent the attacker to perform a task that requires Administrative privileges. In authentication, password policies should be hardened and the use of complex passwords must be introduced, as this will minimize any brute-force attempt on passwords.

Training is also an essential part of host based security, and employers need to be aware of certain risk which could compromise their systems. By providing security awareness training and applying best practice guides, the employees are aware of security issues and can help the organization stay on top of security threats by not using the system for any other reason apart from their task.

III. Possible Impacts

If there is not adequate security in place, then the impact of an attack or a disruption in the process of these critical infrastructures could prove hard to deal with, such impacts include :

- Physical Impacts - Loss of life, property and data, also potential damage to the environment i.e. oil spillage.
- Economic Impacts - Loss of income, revenue from attacks which cause the normal process of industrial systems to be halted.
- Social Impacts - If an attack compromises transportation networks or systems which will have a social impact i.e. water distribution systems the public will loose confidence in the Government.

The NIST Guide to ICS security also includes the following as potential consequences from an ICS incident:

- Impact on national security/facilitate an act of terrorism
- Reduction or loss of production at one site or multiple sites simultaneously
- Injury or death of employees
- Injury or death of persons in the community
- Damage to equipment
- Release, diversion, or theft of hazardous materials
- Environmental damage
- Violation of regulatory requirements
- Product contamination
- Criminal or civil legal liabilities
- Loss of proprietary or confidential information
- Loss of brand image or customer confidence.

IV. SCADA risks

One of the biggest issues that SCADA systems face is that they were designed to work solely in their environment segregated from inter-connected IT networks or ad- hoc systems. The primary reason for this is that there was no need for remote access at the time of their introduction, where as now organizations want to establish a local convenience or remote access, this enables them to take decisions on production changes and apply them quickly from a centralized location rather than have to travel to different locations in order to make changes to their ICS systems

As most ICS systems compromise significant legacy systems, it is difficult to add a security mechanism or firewall hardware as this will interrupt their normal process. If there is no redundancy in place a company may simply not afford their process to stop in order to add these devices. One of they key points is to understand the attack vectors and be able to deal with them. Companies need to prepare for the worst case scenario, there is no certainty that the end-point security solutions applied will ever be breached. There is a need to always prepare for the worst case , that is why it is advisable if possible to harden the security of the network. There are many ways this can be applied, one of which is to start by disabling all services/ports and only enabling what is needed. This will preserve attack cases were intruders were able to gain access to systems via ports that were open but not used by the company, hence there was no specific reason for the port to be open.

V. SCADA Attacks

There are a lot of threats to our National Critical Infrastructure systems (SCADA) which have a major effect not only on the public, but also the government and the economy of a country or nation. Most of the attacks have used sophisticated mechanisms to gain entry and exploit well-known vulnerabilities and ones that have yet to be discovered.

A. Stuxnet

Stuxnet is a computer worm which was built to attack and infiltrate previously unknown vulnerabilities which were present in Windows operating system, and also Siemens Simatic WinCC, PCS7 and the s7 products. These vulnerabilities are known as Zero-Day exploits, Zero-Day is the term used to define an attack/exploit on a previously unknown vulnerability. Stuxnet discovered by Kaspersky Labs2 in 2010 [12], and the main reason for its discovery was that Stuxnet infected except from the target system many others systems worldwide.

Stuxnet was of 500Kb size(KiloByte) which included two digital warhead; the file was transfered via a USB device; half of the file was intended for the Windows Exploits and the other for the Siemens specific PLC. Once the file was executed on the engineers laptop, Stuxnet would then start to look for specific versions of product files and software, once it found what it was looking for it then started to reconnaissance the normal day-to-day process of the PLC. This step would later come to be Stuxnets shield.

After a month Stuxnet started to alter the PLC's working logic to it's own version of the code and played back previous recorded months to the engineers screen so that the attack went unnoticed for over a year. Stuxnet managed to alter the Programmable logic controller language to it's own malicious version, it altered the Hz frequency of the drives outside of its normal working frequency; the normal working frequency was 807Hz and 1210Hz. Stuxnet altered the frequency to 2Hz and 1410Hz, to either spin slower or faster depending on its output.

B. Maroochy

The Maroochy shire water sewage system cyber attack is on of the most well known and publicized attacks. It infected a SCADA controlled system with 142 pumping stations over 1157 sq km, that was initialy installed in 1999. In 2000 the cyber attack took palce, which caused 800,000 litres of raw sewage to spill into local parks, rivers and the Hyatt regency hotel. Vitek Boden was an employee of Hunter Watertech who were responsible for the installation of the SCADA system for the Councils sewage system. After an unsuccessful attempt to gain employment at the council, Boden decided to take revenge on his previous employer and the council. He stole radio equipment from his job before leaving along with a computer and he began his attack by connecting to the wireless network of the command and control center which in turn connected to pumping stations via wireless link, which at that time were not passworded. The above example makes it very clear how attacks can occur and the consequences they have on the public, environment and national infrastructure. The actual cause of the problems that the attack caused are many, but the lack of monitoring and logging mechanisms, and the lack of an incident response plan in the Maroochy council made it difficult to deal with this attack.

C. Duqu

In 2011 there was another piece of malware that was detected named Duqu that targets Microsoft Windows computers. On its first analysis, the analysts at CrySys Labs discovered that Duqu was very similar to Stuxnet in terms of its design philosophy, structure and its various mechanisms [13]. In terms of the threat it is very identical to Stuxnet too, but it is completely built for a different purpose, it's aim is to gather intelligence data and assets from entities such as Industrial infrastructures and system vendors so that an attack could be more easy to be performed in the future. Information within documents which include a plants design, technical data and other relevant data which could help attackers to mount a future attack on various industries including those of ICS are stolen during a Duqu attack.

D. Flame

Flame is another piece of malware detected by Kapsersky Labs, and it has ben dubbed as an espionage toolkit, created by a state-run cyber-espionage operation [14]. It's main difference between Stuxnet and Duqu is that it is not only intended for Industrial infrastructures but also individuals and educational institutions. Although it may appear that this is not directly related to SCADA one may assume that the Mal aware was in fact looking to continue Stuxnets attack, since most of the infected machines have been in Iran since 2010 to until 2012.

E. Havex

Havex is a remote administration tool that was used to target Industrial Control systems (ICS) and SCADA used by energy companies in Europe and the United States. The way the attackers managed to get access to machines used by Command and Control centers was by using a technique called ”watering hole”, watering hole attacks that exploit vulnerabilities in websites. Once this was accomplished the cyber criminal could plant a compromised version of legitimate software to the compromised site. In this case they used PLC vendors website to upload their own version of the software, so that once the software was executed, it created a back-door connection to the attacker and they could have full control of the infected machine.

F. HID Related attacks

In reference to SCADA there have not been any attempts to attack their systems with a HID device, such as the Teensy 3.1 which falls under the HID category as this is how it is recognised by the system although it connects via USB. Further research showed that the primary use of the Teensy board was for personal projects which can all be found under the PJRC13 store. The teensy board itself has been used as a penetration testing tool kit.

VI. Experimental setup

Our earlier research showed that the commands sent from an engineer's machine to a PLC go through the TCP/IP protocol. We connected the machine and the PLC together (see Figure 2, Figure 3) via a switch so that we could confine any action to a safe environment without disrupting any other interconnected devices on the network.

By using the Codesys software to start and stop the PLC, while sniffing the connection between these two devices, we noticed that the commands sent between these devices were not encrypted, but rather, were in plain text (HEX). This characteristic is a vulnerability of the system that can be exploited. Since no authentication/encryption is used we can replicate this information without the need of the ABB suite of tools. The packets that are exchanged have a lot of raw data that do not perform any specific action on the PLC. One of the most important findings is the 3-way handshake being performed between the PLC and the computer. To attempt any sort of command execution we need to establish a connection using this 3-way handshake mechanism.

The packets also revealed that when an AA// was included in the raw data it meant that the following code was an attempt at communication. The above syntax was a key, as without

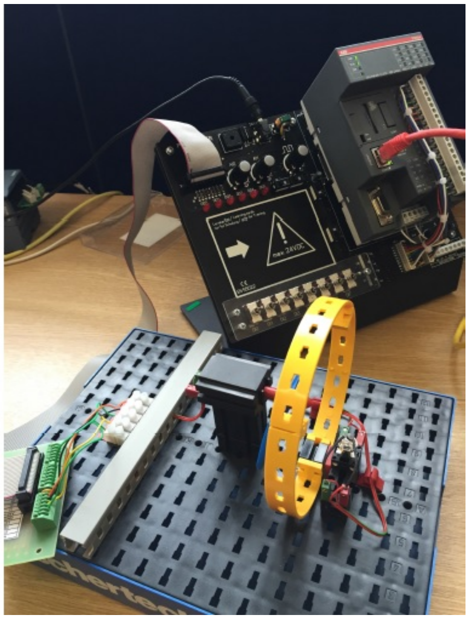

Fig. 2: Architecture of the PLC

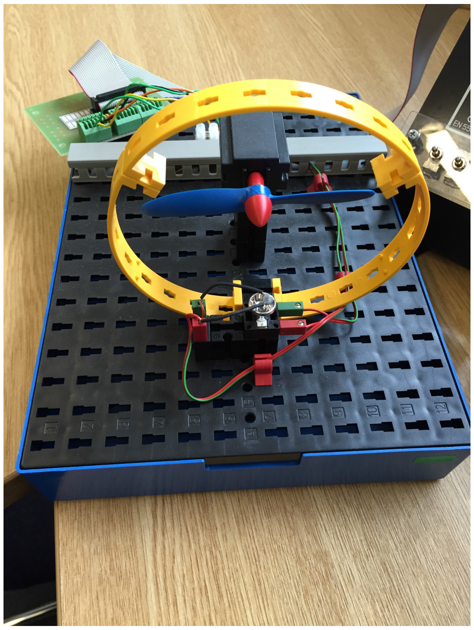

Fig. 3: FisherTechnics Propeller

this syntax we would have to go through every single piece of data and use a trial and error approach in order to interpret data to actual commands. In order to craft packets, we used a Linux tool which has been made available for Windows called Scapy, which is able to create a packet with a set of parameters specified by the user. Specifically, it is a packet manipulation tool developed by Phillipe Biondi with the ability to forge, decode packets from a different range of protocols and to send them or reply to a request.

In order to be certain that this data did not change per every single connection attempt, we captured the data many times and compared these values. We concluded that the data exchanged in order to perform specific actions on the PLC are exactly the same every time. This finding lead us to the view that ABB PLCs with the specific firmware version use the same set of data to communicate with a workstation. This is very beneficial for our research since it means the attack can work for the same model of PLC without the need to alter the code. Using the same strategy we managed to sniff the 'STOP' command that is sent from a workstation to the PLC. The series of commands was crafted into a packet and was correctly sent from our device to the PLC, since no authentication or encryption was demanded from the PLC. The script was converted to a simple executable program and the file is hosted on local internet host; ready to download.

VII. Results and Analysis

The attack script starts by accessing the Scapy library and importing the time which is important because without this the PLC and engineer's machine could not talk to each other in different times, i.e. they have to be synced. We create a connection socket specifying the IP and port of the PLC. We then define four variables that include the RAW Hex data, send the request, and wait (sleep) 0.1s before sending the second request. After the second request is sent we dispatch the third, which is the ACK and the fourth request is the STOP command. Finally the last raw data that we sent is to close the socket (See Figure 4). We have to mention here that the full information cannot be disclosed in this article for security reasons.

Based on the research and experimental work that we conducted we found that a ready malicious executable file can cause a PLC to STOP running. The executable file can be downloaded from the internet and executed from the workstation that controls the PLC. It can be copied to the startup location of the workstation so that the payload will run with every restart.

VIII. Discussion

A. Current ICS security practices

IT systems security practices have provided rich experience in defending against systems attacks. However these practices can hardly be applied directly as ICS is fundamentally different from IT systems. IT systems values confidentiality, integrity and availability (CIA), whereas ICS values reliability, maintainability and availability (RMA) [15]. This has resulted in different security defense mechanisms in terms of performance requirements, availability requirements, risk management requirements, physical interaction, time-critical responses, system operation, resource constraints, communications, architecture security focus, change management, managed support, component lifetime and access to components [15]. Moreover, attack can be performed as different levels including RTUs and edge devices, SCADA protocols and Network topology [16]. Existing IT system defense mechanism

```
def pkt_send():
    mysocket = socket.socket()
    mysocket.connect
        (('192.168.0.10',1201))
    myStream = StreamSocket(mysocket)
    req = Raw(load=”\xbb\xbb\x00\x00
        ......”)
    req1 = Raw(load=”\xbb\xbb\x00\x00
        .....”)
    req2 = Raw(load=”\xbb\xbb\x00\x00
        .....”)
    req3 = Raw(load=”\xbb\xbb\x00\x00
        .....”)
    myStream.send(req)
    time.sleep(0.1)
    myStream.send(req1)
    time.sleep(0.1)
    myStream.send(req2)
    time.sleep(1)
    myStream.send(req3)
    time.sleep(0.1)
    mysocket.close()
pkt_send()
```

Fig. 4: Attack code

has to be tailored to address the above-mentioned aspects in ICS security defense.

There have been some existing researches on adapting existing IT system security to satisfy the needs of ICS security. Snort, a signature-based intrusion detection open source solution have been widely used. Yang et al. [17] proposed a rule-based Intrusion Detection System (IDS), which is a signature-based and model-based approach specifically designed for SCADA networks. The proposed rules were implemented and validated using Snort rules. Cheung et al. also used Snort implementation for a model-based intrusion detection approach for SCADA Networks [18]. Artificial intelligence has also been applied into ICS security defending. Tsang and Kwong [19] proposed multi-agent intrusion detection systems and distributed the operational process into multiple agents. Jiang and Yasakethu [20] applied support vector machines (SVMs) for automated anomaly detection in SCADA. The results showed that the proposed algorithm achieves high detection rates. Maglaras [5] extended this work and applied OCSVM (One-Class Support Vector Machine) for detecting intrusions.

Existing work also provide control system security standards, guidelines and best practices. IEC/ISA-62443 [21] is an internationally recognised industrial control system security standard. The content is organized into four categories, which are General, Policy & Procedures, Systems and Component. NIST SP 800-82 [15] provides cross-industry guidance for establishing secure industrial control systems (ICS). The U.K. CPNI has produced a good practice guide for ICS security. It includes seven parts encompassing both technical aspect (implementation [22] of security techniques) and managerial aspects (governance [25] and security awareness [24]). The U.S. Department of Homeland Security [26] produced guidance on the enhancement of ICS security. It provides a general structure of ICS security management and rich links to other industrial guidelines. The Swedish Civil Contingencies Agency (SEMA) has also produced guidelines to increase security and people's awareness of industrial control system security [27]. It provides 15 recommendations and these recommendations were integrated into Deming Cycle, also known as the PDCA (plan, do, check and act) [28].

B. Future directions for ICS security

Although security standards, guidelines, best practices and security mechanisms are available for ICS, limited researches can be found in the change management and interdependencies between IT and ICS systems.

1) Change management: unlike IT systems, ICS system availability is a primary concern and ICS processes are always continuous in nature. Frequent software patching and updates are not suitable for ICS. Future research should focus on developing new security mechanisms to allow patching and updating equipment without affecting the main operation of ICS systems. The impact of patches and system updates needs to be thoroughly measured and tested.

2) Complex interdependencies: ICS has complex integration with IT systems and physical system. Future research should investigate interdependencies on communication networks and ICT components, develop new tools and processes for security defense.

Future research should focus on these directions and retrofit IT security into existing ICS components. This is consistent with H2020 call in the protection of critical infrastructure [22]. Future research should consider developing security solutions for the next generation ICS and integrating security measure in the ICS product lifecycle.

C. Proposed defense mechanisms

The Teensy HID device appears on the system under the Universal Serial Bus. Traditionally, Windows does not require any privileges for the installation of this device as these drivers are already part of the O/S and by default are automatically installed. A way to stop any input from a certain HID device is to blacklist it by vendor and product ID, but this is not very reliable as the vendor can change the identifiers which then" can by-pass the blacklist enabled within Windows [7]. Another option would be to create a policy within Windows to allow only one keyboard and mouse to be present at any one time. Another available option is to allow the administrator to specify a list of device set-up GUIDs (global unique identifiers) for device drivers that windows is allowed to install. Cryptographic solutions are incomplete without effective key management which remains an open problem in SCADA networks.

The security properties of ICS can be improved by using many of the current cryptographic methods. Although SCADA protocols typically do not support any sort of cryptography, this capability would be useful in securing these networks. The unique characteristics of SCADA networks, on the other hand, make it difficult to adapt existing cryptographic techniques for these systems. Except from strict policies and maintenance issues, security technologies and procedures that are applied on a SCADA network must be audited and updated in a regular basis. Regarding which, more research is needed to develop proper metrics to assess the security of SCADA networks. The integration of new technologies introduce new threats to the security of the ICS. In the ICS network there are three crucial aspects of security that must be protected: Confidentiality, Integrity, and Availability [8].

IX. Conclusion

This article has investigated the vulnerabilities of a SCADA system and performed an attack directed at an ABB PM564 PLC, using a HID (Human Interface Device). This PLC uses the Codesys programming software as its SCADA programming interface. The HID device is inserted into the workstation and is recognized as a keyboard. Once the Teensy USB has been plugged into the system it will wait for a specific amount of time (set in the code) in order to download the code and execute it. The attack, although primitive, cannot be detected by any current IDS, since it involves the execution of a legitimate 'STOP' order from an authorized device. The malicious packet which alters the behaviour of the PLC can be executed in random time periods and in different PLCs, thus making the situation harder to be controlled.

The article then reviewed current security counter measures and ICS defense mechanisms from both technical and managerial perspectives. It also provided possible counter measures and defense mechanisms against this kind of cyber attack. As future work, more sophisticated attacks are going to be performed with real time defense systems tested against them in order to assess their detection capabilities.

References

[1] Igure, Vinay M., Sean A. Laughter, and Ronald D. Williams. ”Security issues in SCADA networks.” Computers & Security 25.7 (2006): 498-506.

[2] Robinson, Michael, Kevin Jones, and Helge Janicke, ”Cyber warfare: Issues and challenges”, Computers & Security 49 (2015): 70-94

[3] A. Carcano, I. Nai Fovino, M. Masera and A. Trombetta, ”SCADA malware: A proof of concept”, in *Third International Workshop on Critical Information Infrastructure Security, 2008.*

[4] Ashford, W, ”US Researchers Find 25 Security Vulnerabilities in SCADA Systems”, ComputerWeekly.com, 2013, October 18, http://www.computerweekly.com/news/2240207488/USresearchers-find-25-security-vulnerabilities-in-SCADA-systems

[5] L. Maglaras, J. Jiang, T. Cruz, ”Integrated OCSVM Mechanism for intrusion detection in SCADA systems”,in *Electronics Letters 50.25(2014):1935-1936*

[6] M. Gil Perez, F. Gomez Marmol, G. Martinez Perez, A. Skarmeta Gomez, ”Repcidn: A reputation-based collaborative intrusion detection network to lessen the impact of malicious alarms”, in *Journal of Network and Systems 730 Management 21 (1) (2013) 128-167*

[7] Crenshaw, Adrian. ”Plug and prey: Malicious USB devices.” URL: http://www.irongeek.com/downloads/Malicious%20USB%20Devices.pdf (2011).

[8] Khurana, Himanshu, et al. ”Smart-grid security issues.” IEEE Security & Privacy 1 (2010): 81-85.

[9] CPNI. PROCESS CONTROL AND SCADA SECURITY GUIDE 2. IMPLEMENT SECURE ARCHITECTURE. In Good Practice Guide, 2008.

[10] Digital Bond. ISA99 Part 1, 2011. URL http://www.digitalbond.com/scadapedia/standards/isa99-part-1/.

[11] Spitzner, Lance. ”The honeynet project: Trapping the hackers.” IEEE Security & Privacy 1.2 (2003): 15-23.

[12] Kushner, David. ”The real story of stuxnet.” IEEE Spectrum 50.3 (2013): 48-53.

[13] Bencsth, Boldizsr, et al. ”Duqu: Analysis, detection, and lessons learned.” ACM European Workshop on System Security (EuroSec). Vol. 2012. 2012.

[14] Zetter, Kim. ”Meet FlameThe Massive Spy Malware Infiltrating Iranian Computers.” Wired, 28th May,Online resource Available at: https://www. securelist. com/en/blog/208193522/The_Flame_Questions_and_Answers,[Accessed 20/11/2012] (2012).

[15] Stouffer, K., Falco, J., Scarfone, K.*Guide to industrial control systems (ICS) security*. NIST special publication, 800-82, 2011.

[16] Alcaraz, C., Fernandez, G., Carvajal, F. *Security aspects of SCADA and DCS environments*. In Critical Infrastructure Protection (pp. 120-149). Springer Berlin Heidelberg. 2012.

[17] Yang, Yi, et al. ”Intrusion Detection System for IEC 60870-5-104 based SCADA networks.” Power and Energy Society General Meeting (PES), 2013 IEEE. IEEE, 2013.

[18] Cheung, Steven, et al. ”Using model-based intrusion detection for SCADA networks.” Proceedings of the SCADA security scientific symposium. Vol. 46. 2007.

[19] Tsang, Chi-Ho, and Sam Kwong. ”Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction.” Industrial Technology, 2005. ICIT 2005. IEEE International Conference on. IEEE, 2005.

[20] Jiang, Jianmin, and Lasith Yasakethu. ”Anomaly detection via one class svm for protection of scada systems.” Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2013 International Conference on. IEEE, 2013.

[21] International Electrotechnical Commission, Industrial Communication Networks Network and System Security Part 1-1: Terminology, Concepts and Models, IEC/TS 62443- 1-1 ed1.0, Geneva, Switzerland, 2009.

[22] European Commission. *Digital Security: Cybersecurity, Privacy and Trust - The role of ICT in Critical Infrastructure Protection*. 2015. URL http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1052-ds-03-2015.html.

[23] Centre for the Protection of National Infrastructure, Good Practice Guide, Process Control and SCADA Security, Guide 2: Implement Secure Architecture, London, United Kingdom, 2008.

[24] Centre for the Protection of National Infrastructure, Good Practice Guide, Process Control and SCADA Security, Guide 4: Improve Awareness and Skills, London, United Kingdom, 2008.

[25] Centre for the Protection of National Infrastructure, Good Practice Guide, Process Control and SCADA Security, Guide 7: Establish Ongoing Governance, London, United Kingdom, 2008.

[26] Technical Support Working Group, Securing Your SCADA and Industrial Control Systems, Department of Defense, Washington, DC, 2005.

[27] Swedish Emergency Management Agency, Guide to Increased Security in Process Control Systems for Critical Societal Functions, Stockholm, Sweden, 2008.

[28] Deming, William Edwards. The new economics: for industry, government, education. MIT press, 2000.