IoT Vulnerabilities in SCADA Systems

Jose Rivera Barbosa
Master in Computer Science
Jeffrey Duffany, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— The emerging technologies like Internet of Things (IoT) is an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react. With this possibility the Supervisory Control and Data Acquisition (SCADA) have been taken to this level. SCADA provides management with live data on production operations, implementing effective controls, and reduces costs of operation. Most consumers and vendors may or may not be aware or probably haven't realized the greater threats that are out there in the cyber world. By Applying security standards and best practices we may be able maintain and enhanced on minimizing the risk by using all available tools that are out there. The internet has grown a lot since the beginning and there are powerful tools out there that are accessible and resourceful from a novice level to experience Security Professional. This project will demonstrate how easy it's to find the vulnerabilities on IoT devices that are connected to SCADA systems. To produce this finding we will use the following search engines: SHODAN.io and CENSYS.io that search and extract worldwide data from devices that are currently connected to the internet. Ones identified a security issue; a security analyst can establish a corrective action plan to prevent future security flaws by applying security standards and best industries practices.*

Key Terms *— Internet of Things, IoT, SCADA, Vulnerabilities.*

INTRODUCTION

This project consists of the use of search engines that enables users to find specific types of computers (web cameras, routers, servers, etc.) connected to the internet using a variety of filters. It has been described as search engines of service banners, which are meta-data the server sends back to the client [1]. Also these search engines can allow computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, it lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed [2]. These are two similar search engines that can be used for data mining and research on devices connected to the internet. Since modern devices are being connected to the internet they land on the universe of Internet of Things. The IoT is an extension of the internet by integrating mobile networks, internet, social networks, and intelligent things to provide better services or applications to users.

HISTORY

Going back in time the term "Internet of Things" was eared more than 15 years ago by the founders of the original MIT Auto-ID Center (Kevin Ashton in 1999 and David L. Brock in 2001) [3]. But it has been evident that devices where being connected to the networks long before MIT Auto-ID for example, the famous Cambridge Computer Lab coffee pot back in 1993 was an early example [4]. But basically the concept started for them with the expression "Auto-ID" in which it refers to any broad class of identification technologies used in industry to reduce errors, automate and/or increase efficiency. In the climax of the Auto-ID Center reputation occurred around 2003, when the Electronic Product Code (EPC) Executive Symposium taking place in Chicago marked the official launch of the EPC Network an open technology infrastructure allowing computers to automatically identify man-made objects and track them as they flow from the plant to

distribution center to racks. The symposium supported then by more than 90 major companies from around the world come a key enabling technology for economic growth in the next fifty years. Many companies are developing products which are more and more connected in order to as we said reduce errors, automate or increase efficiency [3].

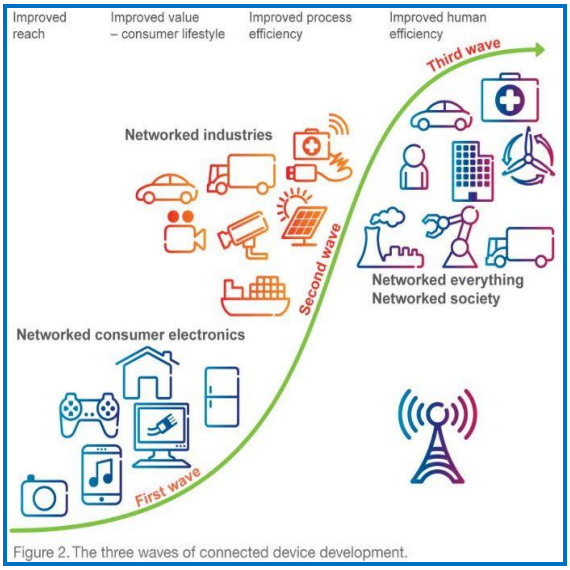

Figure 1
IoT Evolution

SCADA has evolved from its beginnings in the 1960s. The advent of low-cost minicomputers such as the Digital Equipment Corporation PDP-8 and PDP-11 made computer control of process and manufacturing operations feasible. Programmable logic controllers (PLCs) progressed simultaneously. These latter devices implemented traditional relay ladder logic to control industrial processes. PLCs appealed to traditional control engineers who were accustomed to programming relay logic and who did not want to learn programming languages and operating systems. When microcomputers were developed, they were programmed and packaged to emulate PLCs in function, programming, and operation.

Initially, control systems were confined to a particular plant. The associated control devices were local to the plant and not connected to an external network. The early control systems consisted of a central minicomputer or PLC that communicated with local controllers that interfaced with motors, pumps, valves, switches, sensors, and so on.

This architecture is sometimes referred to as a distributed control system. Such systems are generally confined to locations close to each other, normally use a high-speed local network, and usually involve closed loop control. As a necessary requirement for the operation of these systems, companies and vendors developed their own communication protocols, many of which were proprietary.

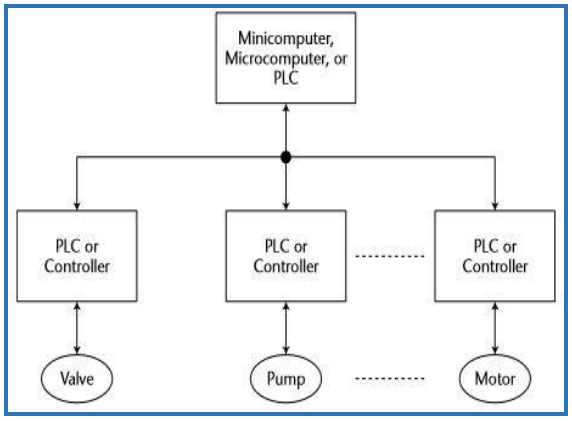

Figure 2
SCADA Local Control System

The Supervisory control and data acquisition (SCADA) systems are vital components of most nations' critical infrastructures. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations. SCADA provides management with real-time data on production operations, implements more efficient control paradigms, improves plant and personnel safety, and reduces costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. However, these benefits are acquired at the price of increased vulnerability to attacks or erroneous actions from a variety of external and internal sources [5].

PURPOSE

Demonstrate the vulnerability challenges that face the IoT devices in SCADA system and present security standard solution that can be applied from the manufacture to the client who's acquiring the device.

REQUIREMENTS

Since both search engines are accessible through the internet you can use basically any web browser to perform the analysis. With SHODAN.io you create a free account to perform searches and buy credits through the website to download reports generated from the searches. In the CENSYS.io site you need to create an account to have access to the rest of the search engine features.

PROCEDURE

To perform these searches we have to use customized queries to generate and narrow down results for both SHODAN.io and CENSYS.io. The data is generated of all IoT devices around the world. Mostly searches consists of keywords/tags related to SCADA, device manufacture or ports.

Here are some basic filters for the SHODAN.io search engine [6]:

- **City:** find devices in a particular city
- **Country:** find devices in a particular country
- **Geo:** you can pass it coordinates
- **Hostname:** find values that match the hostname
- **Net:** search based on an IP or /x CIDR
- **OS:** search based on operating system
- **Port:** find particular ports that are open
- **Before/After:** find results within a timeframe

SHODAN searches used during the research:

- SCADA port:"80"
- country:"PR" energia
- port:"23" country:"CN"
- server:SQ-WEBCAM
- linux: upnp avtech

CENSYS using the following filters [7]:

- **Specifying fields:** Searches for all hosts with a specific HTTP status code with the following query:
  (e.g., *80.http.get.status_code: 200)*
- **Boolean Logic:** You can compose multiple statements using the terms **and**, **or**, **not**, and parentheses.
  (e.g.,"Schneider Electric" or Dell) and 23.20.0.0/14.)
- **Networks, Host Names, and Protocols:** You can search for IP addresses using CIDR notation *(e.g., ip:23.20.0.0/14)* or by specifying a range of addresses ip:[23.20.0.0 TO 23.20.5.34]. Another query is the search for hosts that serve a particular protocol by searching the protocols field. (*e.g., protocols: "102/s7"*).
- **Ranges:** You can search for ranges of numbers using [and] for inclusive ranges and { and } for exclusive ranges.
  (e.g.,"80.http.get.status_code:[200 TO 300].)
- **Wildcards and Regular Expressions:** Censys searches by default for complete words but you can use wildcards like "?" to replace single characters or "*" to replace zero or more characters.
  (*e.g., SCAD*)*

CENSYS searches used during the research:

- SCADA
- RUT500
- ip:[IP TO IP]

VULNERABILITY FINDINGS

At this point we have to think on possible security vulnerabilities that are out there that affects companies and industries from physical to systematical. For instance, ports that are very vulnerable to existing penetration tools, devices that have default credentials, SCADA logging screens that support brute force attacks.

We can analyze these devices by using search engines like SHODAN.io and CENSYS.io to

analyze IoT devices related to SCADA systems in order to find the vulnerability to generate an attack.

- **Default credentials** – Most manufactures develop device with default credentials where you can easily look them up on the manufactures guide. Clients fail to change them after being setup.

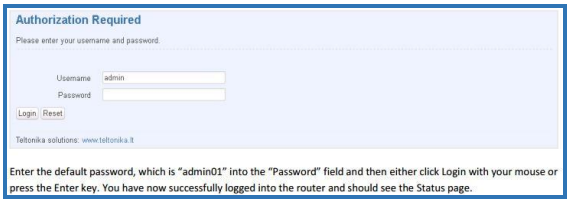

Image 1
Teltonika RUT500 Manual

- **Remote Access** – We all want flexibility on our jobs but we must make sure that the connection and devices that are in between are properly secured. Connection can be intercepted, tampered, rerouted, etc.

Image 2
Login Screen of Security Webcam

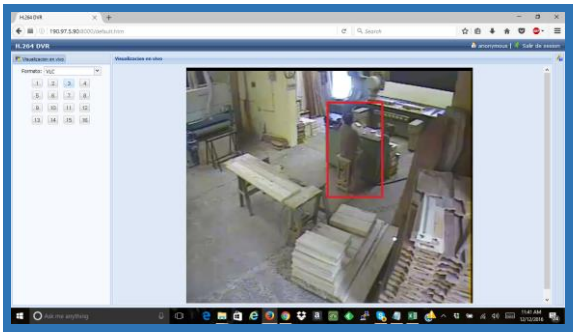

Image 3
Webcam – Factory in Argentina

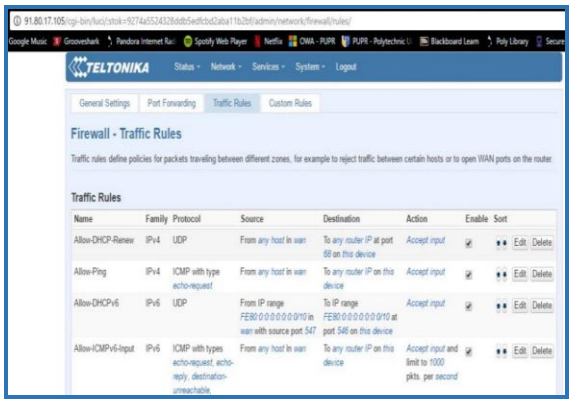

Image 4
RUT500 Firewall Traffic Rules

- **Unencrypted ports or Open Ports** – Setting up a network infrastructure is no easy task but when you're enabling ports you've got to secure or close ports. Having open ports may allow unwanted traffic to flow in or out.

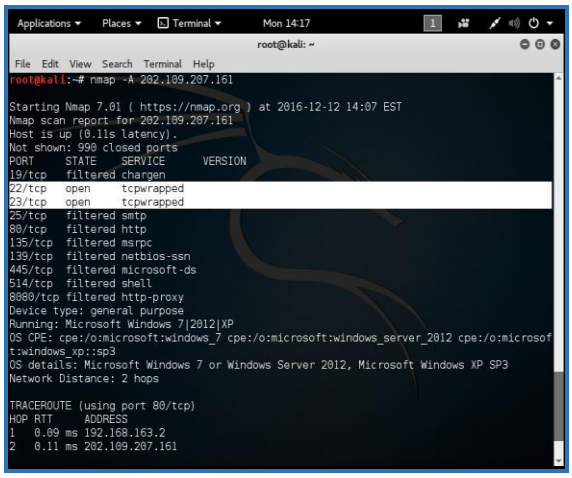

Image 5
Scan on a SCADA Device

- **Hardcoded Credentials** – Some WebGUI or application interface contains hard-coded credentials, such as a password or cryptographic key in which it is used for its own inbound authentication, outbound communication to external components, or encryption of internal data. In this specific case the device WebGUI has plaint text username credentials integrated on the code in which allows hackers to generate an attack.

Image 5
Teltonika WebGUI Source Code

- **Manufactures flaws** – Devices and applications might have vulnerabilities on their devices in which are later installed on client's infrastructure.

Table 1
Devices with Vulnerabilities

Devices	Names
Wifi Router	Teltonika RUT500, RUT950
Webcam/DVR	AVTech AVC 787 DVR
Webcam/DVR	H.264 DVR
CIRCONTROL	Charge Station

Image 6
Teltonika RUT500

- **Malware** – Basic and advance scripts are generated based on the flaws of common vulnerabilities.

Here's is an example of the data base that uses the Mirai malware. Mirai uses default credentials to gain access to IoT devices on the network. This malware has the potential of shutting down networks.

Image 7
Mirai Source Code

Image 8
SCADA System Logging Screen

COUNTERMEASURES

These common IOT vulnerabilities that affect SCADA system have been proofed to be very effective. But there are existing standards that can mitigate these vulnerabilities and risk if they are followed by the book such as; the Security International Organization Standards ISO/IEC 27002, ISO/IEC JTC 1 for IoT, ISO/IEC for programming languages and of course enhance and maintain company's security standards [8][9].

SCADA systems can be also enforce by Isolating the SCADA network using encryption, strong authentication, segmented network topologies, biometrics, and by disconnecting the network from unnecessary external connections. We can also conduct vulnerability analyses and risk assessment on the network and on each connection point to the enterprise network. Develop and implement an incident response and remediation

plan in case of a network breach. Remove or disable all unnecessary services that may not be need for applications. Apply firewalls that are compatible with requirements of SCADA systems to protect traffic leaving or entering the network. Install and operate intrusion detection systems that would raise a flag if unknown behavior is detected on the network. Be sure to perform backup of critical software and data in case data has been corrupted or destroyed. Apply configuration management to SCADA and network software and hardware. Incorporate patch management to SCADA network software and hardware to maintain systems with the latest version. Conduct security audits. Implement an enterprise-wide security awareness program, including handouts, slogans, login banners, briefings, and training classes. Also develop and test business continuity and disaster recovery plans [10].

By combining strategies, we can significantly improve security posture of real-time data acquisition and control systems and allow both environments to perform their designated critical functions and operations.

CONCLUSION

As evident these vulnerabilities strategies are at the reach of any individual and may seem alarming. If the device is available, it can be analyzed and exploited. Take it as a small beacon on the cyber world. But if we embrace this knowledge and countermeasures we can definitely put them in practice in our daily jobs, industries and of course add them to the security tools methods.

ACKNOWLEDGEMENTS

I would like to acknowledge Dr. Jeffrey Duffany for his contribution and guidance during the project and classes.

REFERENCES

[1] J. Matherly, "All about the data", *Complete Guide to Shodan -Collect. Analyze. Visualize. Make Internet Intelligence Work for You*, Lean Publishing, 2016, pp 6 - 7

[2] *Censys*, University of Michigan, Z. Durumeric, D. Adrian, A. Mirian, M. Bailey & J. A. Halderman (n.d.)., Search Syntax [Online]. Available: http://censys.io/. [Accessed: January 22, 2017].

[3] *Origin & Definition. (n.d.)., para 1 - 2.* [Online]. Available: http://iotomorrow.wordpress.com/origin-definition/. [Accessed: December 5, 2016].

[4] D. McFarlane. (2015, June 26). *The Origin of the Internet of Things* [Online]. Available: http://www.redbite.com/the-origin-of-the-internet-of-things/. [Accessed: December 5, 2016].

[5] R. L. Krutz PhD, "SCADA Evolution", *Securing SCADA Systems*, Wiley Publishing Inc., IN, 2006, pp. 5 - 6.

[6] J. Matherly, "Introducing filters", *Complete Guide to Shodan -Collect. Analyze. Visualize. Make Internet Intelligence Work for You*, Lean Publishing, 2016, pp 12 - 17.

[7] *Censys*, University of Michigan, Z. Durumeric, D. Adrian, A. Mirian, M. Bailey & J. A. Halderman (n.d.)., Search Syntax [Online]. Available: http://censys.io/overview#. [Accessed: January 22, 2017].

[8] *ISO/IEC 27002(2013, October)* International Organization Standard (n.d.)., Search Syntax [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=54533. [Accessed: January 5, 2017].

[9] *ISO/IEC JTC1* International Organization Standard (2015)., Search Syntax [Online]. Available: http://www.iso.org/iso/internet_of_things_report-jtc.pdf. [Accessed: January 5, 2017].

[10] R. L. Krutz PhD, "SCADA Security methods and techniques", *Securing SCADA Systems*, Wiley Publishing Inc., IN, 2006, pp. 89 - 108.