I Can Show You the World: How Shodan is Used to Exploit Vulnerable SCADA Systems

Matt Long
matthew.long@tufts.edu
Mentor: Ming Chow

Abstract

In an effort to make life easier through automation, more and more technologies feature internet connectivity to facilitate more efficient use by users, whether built in by design or hastily thrown together on an older device. Unfortunately, many of these technologies neglect sufficient security practice, with many users entirely unaware that by simply connecting their devices to the internet, they can expose not only their device but their whole network, and possibly the public at large, to malicious attackers. This paper explores how many of these devices grew to live on the internet without efficient security measures, how a tool called Shodan can be used to find and expose these vulnerable technologies on the internet, and how this could spell trouble if left unchecked in the future.

Introduction

What are these devices and technologies?

Today, more and more devices are connected to the internet in the name of automation. Nest thermostats use the internet to communicate and learn a user's habits, while other devices like refrigerators and lights connect to the internet to allow a user to do what they want at the click of a button (or touchscreen). This practice of connecting more and more devices to the internet is leading to what is known as the "Internet of Things". The Internet of Things is not exclusive to new technology - many old existing technologies are now connected to the internet, including public infrastructure. Many devices, such as power plants, dams, and a particle accelerator, have been hooked up to the internet to provide more efficient interaction between the devices and workers [1]. These large scale devices and systems are referred to as SCADA systems, or supervisory control and data acquisition systems. SCADA systems are digital systems used to run critical infrastructure systems, such as the electrical grid systems, sewage and water systems, and air traffic control systems [4]. In years before the internet, these devices required physical interaction to operate. Now, internet connectivity and computer interfaces allow for remote monitoring and operation, creating a double-edged sword that promotes efficiency as well as exposure.

What is Shodan?

Shodan is a service that crawls the internet, returning devices whose banners match information given in the query, like search engines return pages whose content matches the given query. Information returned includes IP address, City and Country of origin, open ports and services, organization name, and Internet Service Provider name. Anyone is able to use and explore Shodan at www.shodan.io. Limited functionality is available for anybody, basic functionality requires an account with the website, and advanced functionality requires paid credits. The scope of this paper is focused on Shodan’s basic functionality.

One thing that should not be lost in the contents of this paper is the idea that Shodan is a helpful tool, not a malicious one. Shodan will almost exclusively be mentioned in the context of being a tool that exposes vulnerabilities in critical infrastructure, and as a result may appear as a malicious means of discovering attack vectors. Shodan was created with the intent of letting companies track the usage of their software out in the world [1]. In reality, Shodan is used primarily by security experts to identify at-risk networks so that they can be fixed or taken down. As Dan Tentler, a San Diego-based security consultant puts it:

> The fact that somebody is basically shining a flashlight into a dark room shouldn't be the part people are afraid of. The part people should be afraid of is the fact that some genius decided to take, for example, a five-megawatt hydroelectric plant in France, put its control computer on the Internet and allowed everybody that knew about the IP address to connect to it and make changes to this dam, with no encryption or authentication to speak of [5].

Shodan also is not an anonymous service - if users want more than 50 results (and anybody looking to do something malicious wants more than 50 results), then users are required to enter personal and payment information. There also exists a large gap between the knowledge required to find vulnerable sites with Shodan and the knowledge required to exploit them, and most people with the knowledge to exploit them have their own anonymous means to find them [1].

To The Community

Most people have daily interactions with technology other than their phones or computers that use the internet. Things previously mentioned, like Nest or smart appliances are usually connected, but so are the traffic lights and electrical construction signs motorists drive past daily. Many people have an insufficient knowledge regarding what it means to be connected to the internet, especially outside their personal computers or phones. It is important to understand the consequences as well as the benefits of creating the Internet of Things, and these lessons scale from the large SCADA systems discussed in this paper down to the webcam in your bedroom, and everything in between. Proper security measures need to be taken with all devices connected to the internet, both present and future. Interconnectivity and automation are great advancements that increase the quality of life, but many people are completely unaware of the reckless path being taken towards innovation.

Evolution of SCADA Systems on the Internet

Many of these industrial systems were developed in isolation, primarily as hardware systems [3]. These systems required an engineer on-site to interact with and operate them. With an advance in technology and a regression in the number of engineers on the market, tele-control of these machines became the go-to method of interaction, giving birth to the SCADA industry. Over time, this technique began employing modems to connect. While this technique still originally offered point-to-point connectivity, further attempts at saving costs resulted in the use of communications networks for tele-control. Company-specific protocols began causing conflicts with desired interoperability between devices, and the simultaneous push for firmware and software led to the abandonment of point-to-point connectivity in favor of IP technology [3].

Security was an afterthought with the evolution of these SCADA systems. These systems were not designed to handle internet-like traffic, and as a result were rife with security vulnerabilities. Despite the knowledge of these vulnerabilities, many infrastructure software vendors maintained that their products were safe, claiming they were “air-gapped” from the internet, meaning that while the systems were all internally connected on a network, none of the system components provided a link to the internet [8]. While that may have held sufficient at one point in time, we know directly through results from Shodan, as well as indirectly from the research done by Éireann Leverett - his dissertation has been and will be referenced throughout this paper - that no air gap exists between these networks and the internet.

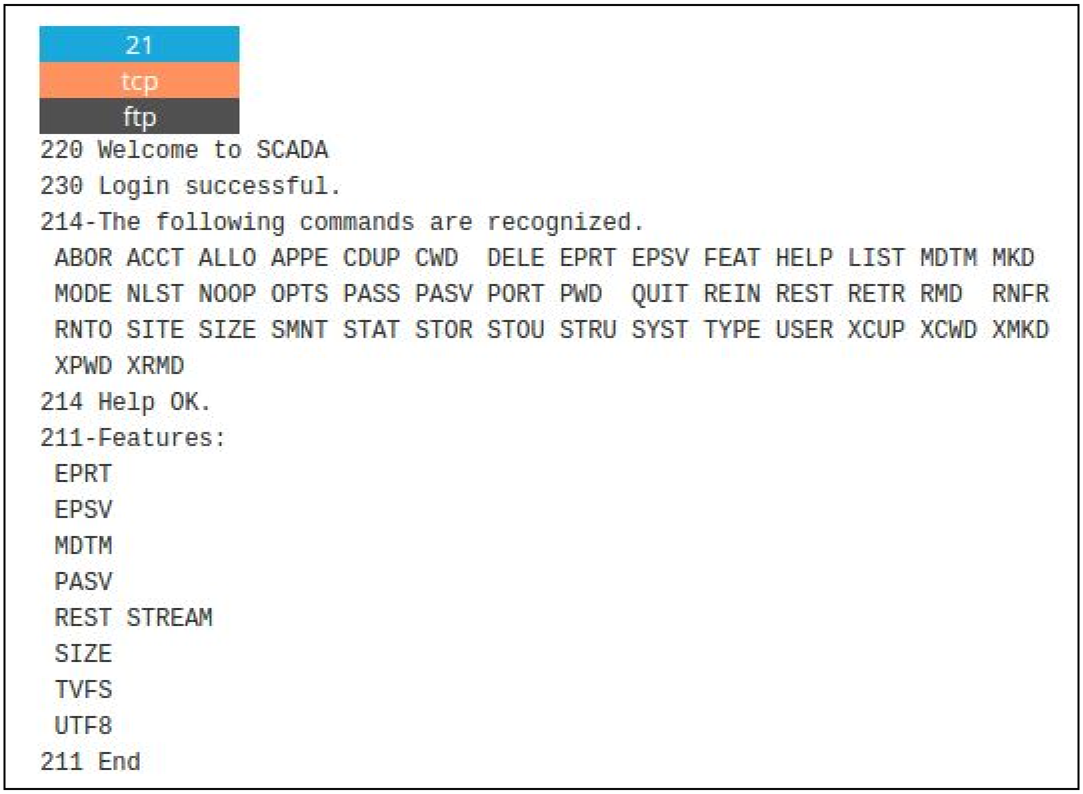
Accessing SCADA Systems using Shodan

A quick search on Shodan can reveal many of these systems connected to the internet. A query of ‘SCADA’ returns a couple hundred IP addresses of internet-connected services whose banners indicate that those computers are various SCADA systems - all potential targets for exploitation. The banners also contain information, such as what server is being run, introducing more information about the system that can be exploited by an attacker. Note that this is one of the simplest, out-in-the-open queries available - Leverett’s research turned up 10,358 vulnerable systems [8].

Attempting to visit these IP Addresses produces mixed results. Some of the web-interfacing computers provide an HTTP 401 response, indicating authorization is needed to access the site. Out of all the results returned by Shodan, this is the most secure (although by no means is it entirely secure, nor is it the most common). No access to any part of the site is granted without proper login; however often times lazy system administrators leave the default login, such as ‘admin/admin’ or ‘admin/1234’ as the login credentials for the machine, assuming that their system will never be accessed by outside users. Often times these defaults can be looked up, or even exist inside the banner that Shodan returns to the user. Even if the login information is changed and unique, Shodan returns information about the system that can be used to help identify the system and plan more targeted attacks against it. Along with the IP address, Shodan returns information like City, Country, Organization, and ISP for the IP address - information that could be found using programs like ‘whois’, but is nicely parsed and consolidated on the screen. An attacker can use that information to gain more knowledge about the system found by Shodan to orient their own targeted attacks against the system.

Other systems provide a HTTP 200 response, meaning a user can go directly to the site. Often times the user is then presented with a secondary authentication screen, but using this secondary authentication is already less secure than sites returning a 401. All the vulnerabilities listed for the 401-returning sites still apply here, including the prevalence of default usernames and passwords, but in this instance the secondary login screen can provide an attacker with even more information. The name of the system or architecture may be present in the header of the website, informing the potential attacker what system exactly they are trying to infiltrate. The system is no longer a black box, and the attacker can look up more information to aid them in their attack [3]. Also, internal authentication may be vulnerable to SQL-Injection attacks or Cross-site scripting attacks.

Some of these devices have no web interface, and cannot be visited by a browser. Despite that, they still have TCP or SSH ports open. One computer responded with the following:



```
220 Welcome to SCADA
230 Login successful.
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
 UTF8
211 End
```

Shodan was granted access on port 21 of this machine, potentially allowing Shodan or a malicious user to poke around and access content that should be hidden.

It should be noted that banners can be modified to display false content as a defensive measure. A banner can advertise that they are running an Apache web server, when in reality they are running a Microsoft server. An attacker may spend hours attempting fruitless Apache exploits on a different server. Other servers may be honeypots, and determining what percentage are legitimate vulnerable systems is outside the scope of this paper, both in terms of time and ethics. However, through anecdotal evidence[1] and the fact that some sites found require no authentication to access critical infrastructure, it can be determined that the number of legitimately vulnerable sites returned by Shodan is non-zero.

Future Implications

As it stands today, many systems remain vulnerable. These systems can make up the critical infrastructure for a population, and often times there is no overarching architecture for, let alone understanding of, these systems and their interactions [6]. As a result, many systems have security vulnerabilities baked into the construction. The ever-expanding Internet of Things is continuing to add devices to the internet, typically with insufficient thought for security. New reports of hacked cars, Nest thermostats, and fitness bands arise constantly. As the Internet of Things grows, so does the information stored with it. The list of devices that can be found with Shodan expands way beyond SCADA systems - things like baby monitors, traffic lights, Caterpillar trucks, medical devices, heating units, and crematoriums have been found by Shodan and subsequently accessed [2]. The healthcare industry specifically has been shown to be incredibly lax when it comes to security. An independent examination by the Washington Post found that healthcare is “among the most vulnerable industries in the

[1] The Stuxnet Worm and incidents in Maroochyshire, Australia detail two cases of attackers exploiting vulnerabilities in SCADA systems - Leverett’s paper outlines a few more in its introduction.

country” [7]. Passwords are often foregone in the name of efficiency, and there used to be a general apathy when it comes to fixing known flaws (although, that seems to be disappearing lately). Originally, belief existed that the healthcare industry was not a lucrative target, and that it was too obscure for attackers to target. Now, there is a growing concern that hacktivists or terrorists may begin targeting medical information, which spells trouble considering multiple medical devices, including an implantable defibrillator and insulin pump were recently found to be vulnerable, and a glucose monitor was found using Shodan [7].

Separate from lone hackers, these vulnerable systems could be exploited by nation-states in a large-scale attack [4]. A nation at war would not stand long if its water system or electricity system was knocked out. If the nation’s transportation or communication system was compromised, that could lead to serious and immediate tragic consequences. Some experts, such as James Lewis from the Center for Strategic and International Studies, believe that infrastructure attacks now and in the near future will only appeal to “pranksters”, but there’s no denial of the existence of these vulnerabilities, both in the systems and the architecture surrounding them. It may only be a matter of time until someone discovers a much more critical vulnerability or develops a stronger attack that can do lasting damage [6].

Action Items

The average American or reader of this paper likely does not have the controls of their city’s nuclear power plant at their fingertips, and likely cannot do much to patch up some of the vulnerabilities as a result. In fact, even if the admin of a vulnerable power plant was reading this paper, there still likely is not much she or he could do. Many of these systems were implemented years ago, and as a result were implemented on vulnerable systems like Windows XP or Windows 2000. These systems may be so critical to a process that they cannot be shut down in order to upgrade, or they cannot run the risk of a critical error arising post-upgrade [4]. As a result, they often remain running on their vulnerable distributions. Many other SCADA systems resist network testing with tools like Nmap or netcat out of fear that an issue could arise during testing that affects production. In one instance, a ping sweep was performed on an industrial control system merely to identify hosts on the network. One machine hung and as a result caused $50,000 worth of damage to wafers [3].

While much of the system architecture may be too deeply ingrained in its vulnerable, offline-intended structure[2], there are steps that can be taken to secure these systems as much as possible. Perhaps the most important, as well as the most widely applicable, is setting up authentication - not just instituting it in the system, but removing the default user. Most default accounts can be looked up, and aren't hard to guess on their own. Setting up a unique username and password, as well as setting up users with least privilege, can help protect your systems. Another step to limit intrusion instances are to set up firewalls and utilize IP whitelisting. Most of these systems shouldn't be accessed from outside one or two IP addresses anyway, so using IP whitelisting is an effective method to limit traffic to your system [3].

[2] Leverett refers to focusing on device vulnerabilities as a "red herring", considering many weren't intended to face the internet at all [3].

Conclusion/Summary

The internet is a tool that many users take for granted. Typical users assume that security is either taken care of for them, or simply that they won't be targeted when it comes to attacks. In reality, security is often put by the wayside in the name of automation and innovation, and has been way before the expansion of the Internet of Things. Tools designed for isolated interaction were forced onto the internet, and a host of vulnerabilities followed. Some of these tools may be innocuous, like CCTV outside a warehouse, but others involve much more important systems - particularly SCADA systems. Developers knew about many of these vulnerabilities, yet dismissed them, thinking their systems were not lucrative targets and the "air gap" between their networks and the internet would protect them. Evidence has shown, however, that that simply is not the case. A tool called Shodan can crawl the web, finding these exposed, vulnerable devices and presenting them to anyone with access to a computer. Despite the many inherent security vulnerabilities of these devices, many lack simple security measures. Some devices or systems still use the default login to access them, while others forgo authentication entirely. There have been a few notable attacks on these vulnerable systems in the past, but the insecure nature of these devices on the internet opens itself up to much more. As the Internet of Things grows, we need to keep security in mind. While some systems may be beyond salvation, we can implement basic security measures like strong passwords, firewalls, and IP whitelisting while we work to reform the tangled, chaotic architecture currently being built upon.

References

[1] Clements, Sam. "Is Shodan Really the World's Most Dangerous Search Engine? | VICE | United Kingdom." VICE. 26 Apr. 2013. Web. 14 Dec. 2015.

[2] Hill, Kashmir. "The Crazy Things A Savvy Shodan Searcher Can Find Exposed On The Internet." Forbes. Forbes Magazine, 5 Sept. 2013. Web. 14 Dec. 2015.

[3] Leverett, Éireann P. "Quantitatively Assessing and Visualising Industrial System Attack Surfaces." Diss. U of Cambridge, 2011. Darwin College, June 2011. Web. 14 Dec. 2015.

[4] occupytheweb. "Hacking SCADA." Null Byte RSS. Wonderhowto.com, 23 May 2015. Web. 14 Dec. 2015.

[5] Peterson, Andrea. "The 'Scariest Search Engine On The Internet' Has Been Around For 3 Years And Is Used For Good." ThinkProgress. 9 Apr. 2013. Web. 14 Dec. 2015.

[6] Peterson, Andrea. "Could Hackers Take down a City?" Washington Post. The Washington Post, 18 Aug. 2015. Web. 14 Dec. 2015.

[7] Robert, O'Harrow Jr. "Health-care Sector Vulnerable to Hackers, Researchers Say." Washington Post. The Washington Post, 25 Dec. 2012. Web. 14 Dec. 2015.

[8] Zetter, Kim. "10K Reasons to Worry About Critical Infrastructure."Wired.com. Conde Nast Digital, 24 Jan. 2012. Web. 14 Dec. 2015.