University of Twente
The Netherlands

Economics of Security 2015/2016

Individual assignment

Ikram Ullah

S1737120

Abstract

SCADA that stands for Supervisory Control and Data acquisition, are systems that are responsible for controlling and monitoring industrial critical infrastructure functionalities. Internet connection of SCADA systems exposes them to external security threats. SCADA systems are the target of cyber attacks everyday at large scale, which results in devastating situation. The most common attack is DDoS (Distributed Denial of Service), disrupting productivity and as a result costing them time and money. In this report I will investigate into set of metrics in order to proof that only patching the vulnerabilities of SCADA devices is not the effective way to stop DDOS attack but instead it is the most costly, time consuming and ineffective approach. In alternative I will present a multi-layered security model for the problem owner (user) to make the industrial network infrastructure more secure at lesser price and time and would be the right approach to tackle DDOS attacks. I will present and support my model with standards related to SCADA system security and some real world metrics. Also I will present pros and cons of my model.

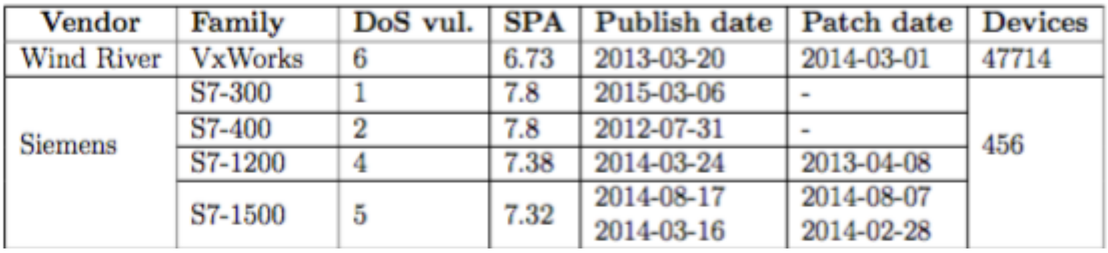
Keywords

DDOS, SCADA systems, IDS, IPS, IPSEC, honeypots.

Introduction

SCADA systems are the most attractive attack target for attackers, it is just because attackers make quite huge profit from it and also it is hard to manage the security infrastructure of SCADA systems. DDOS attack is an extended type of DoS attack. In DDoS attack a large number of slave machines are used against a target system. There are huge number of reasons that can illustrate that completely stopping DDOS attacks are hard if not impossible. The reasons can be using open source softwares, human faults, and insiders' attacks. Open source softwares are threat because they have known vulnerabilities, which are easy to exploit. Impact of Denial of service or distributed denial of service is so severe that it can shut down the whole network infrastructure. Such a shut down is completely unacceptable for industries like electricity gas and water. "Being victim of DDOS attack, as a owner of the scada systems which mitigation strategies to follow to limit the effect of DDOS attacks. " From the table below we can figure out that there are large number of Siemen OS that are still in used and are vulnerable to DoS attacks.

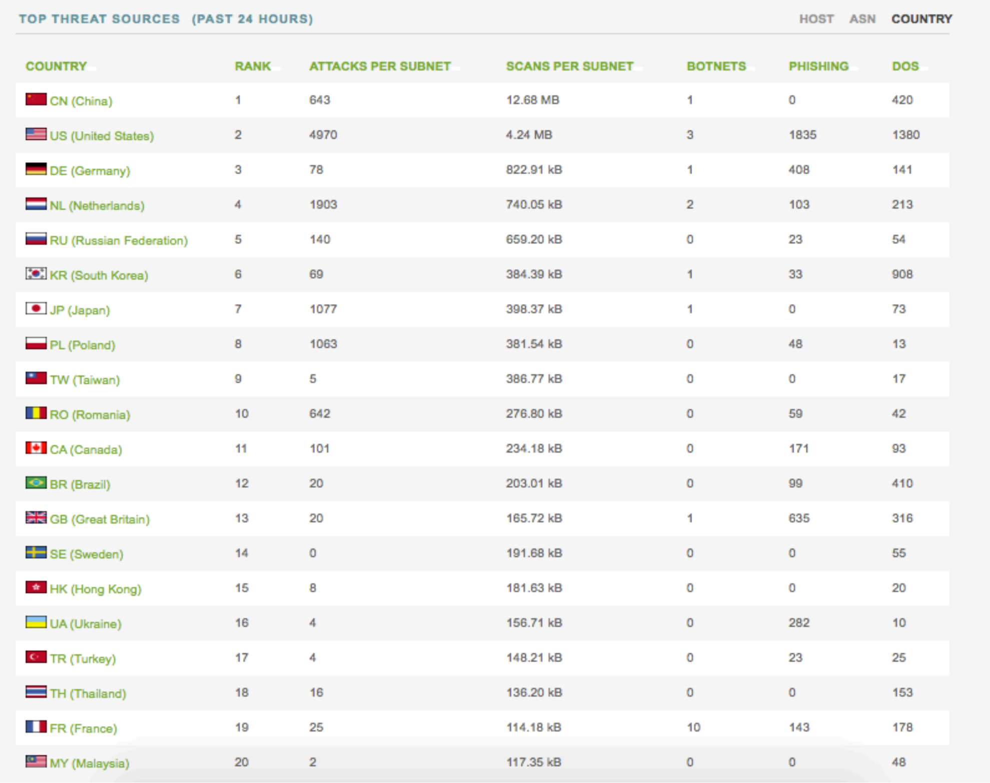
Figure 1: The collected dataset for different firmware/OS cases.



Vendor	Family	DoS vul.	SPA	Publish date	Patch date	Devices
Wind River	VxWorks	6	6.73	2013-03-20	2014-03-01	47714
Siemens	S7-300	1	7.8	2015-03-06	-	456
	S7-400	2	7.8	2012-07-31	-	
	S7-1200	4	7.38	2014-03-24	2013-04-08	
	S7-1500	5	7.32	2014-08-17 2014-03-16	2014-08-07 2014-02-28	

One way to mitigate DOS vulnerabilities from the above SCADA devices would be to write different patches for almost each of the device. Because different devices might be used in different environments one device might be secure in one environment but not in the other environment. So the patches should explicitly consider the environment the device is used. Obviously writing patches will not be an easy and cheap task. For some large enterprise a DDOS attack against their SCADA systems cost them almost €22,000/minute. Also installing and updating devices in large networks is never considered a favorable option. This is because an update will require shutting down the whole network. Even if the patched are installed, in the present technological era there are online cheap service i.e. booters which for €10 can generate malicious traffic up to 25 Gbps against any SCADA device. SCADA device will not be able to tolerate such a high speed traffic so the device might go offline.

Figure below [21] show the real time attacks. From the figure it is obvious that majority attacks are of DoS attacks. So it is a huge issue because this sort of attacks are disrupting legal and crucial business.



TOP THREAT SOURCES (PAST 24 HOURS)

HOST ASN COUNTRY

COUNTRY	RANK	ATTACKS PER SUBNET	SCANS PER SUBNET	BOTNETS	PHISHING	DOS
CN (China)	1	643	12.68 MB	1	0	420
US (United States)	2	4970	4.24 MB	3	1835	1380
DE (Germany)	3	78	822.91 kB	1	408	141
NL (Netherlands)	4	1903	740.05 kB	2	103	213
RU (Russian Federation)	5	140	659.20 kB	0	23	54
KR (South Korea)	6	69	384.39 kB	1	33	908
JP (Japan)	7	1077	398.37 kB	1	0	73
PL (Poland)	8	1063	381.54 kB	0	48	13
TW (Taiwan)	9	5	386.77 kB	0	0	17
RO (Romania)	10	642	276.80 kB	0	59	42
CA (Canada)	11	101	234.18 kB	0	171	93
BR (Brazil)	12	20	203.01 kB	0	99	410
GB (Great Britain)	13	20	165.72 kB	1	635	316
SE (Sweden)	14	0	191.68 kB	0	0	55
HK (Hong Kong)	15	8	181.63 kB	0	0	20
UA (Ukraine)	16	4	156.71 kB	0	282	10
TR (Turkey)	17	4	148.21 kB	0	23	25
TH (Thailand)	18	16	136.20 kB	0	0	153
FR (France)	19	25	114.18 kB	10	143	178
MY (Malaysia)	20	2	117.35 kB	0	0	48

Having in mind all the above unacceptable issues, it can be justified to find a more suitable, effective, stable and cheap solution for DDOS attacks against SCADA systems. The solution be design in such a way that even if the SCADA systems are vulnerable, the malicious traffic will not reach these systems. The malicious traffic be stop and the source IPs be blocked far before reaching the critical system.

The assignment involves investigating and gathering of datasets on security vulnerabilities and relevant metadata, to be able to produce realistic, security model .

The goal it to be able to methodically use the gathered data and use this data in the support of the security of my model.

This approach involves the online metadata search engine, Shodan, as well as vulnerability databases, National Vulnerability Database (NVD) and CVE Details. Other useful resources will also be used if necessary. During the study, I looked into specific categories of online devices, namely SCADA systems. At the same time, on the aspect of vulnerabilities, our focus was Denial of Service attacks (DoS), i.e. although there might be many vulnerabilities in these devices, we only concentrate on vulnerabilities related to DoS and DDoS attacks. The focus on DoS is because of the fact that, these attacks are much more feasible for the perpetrator and much more frequent in the real world. Just as an example, if you search for known vulnerabilities for Siemens SIMATIC S7 (a type of industrial control hardware) in NVD, 14 out of 26 listed vulnerabilities are of the type DoS. The number of DoS vulnerabilities are 12 out of 24 for VxWorks, the most widely deployed real time embedded operating system in industrial setups. Avoiding vulnerabilities in SCADA devices is crucial but it is impossible to eliminate all the vulnerabilities. Even the most complex system doesn't need to be secure because complexity is its own type of vulnerability. It is not important that only attackers will use booters service, any unsatisfied employee can take advantage, or it can be any competitor. So therefore it is almost important to the make the SCADA devices as secure as possible and at the same time there should also be some external shields that can block the attack even before reaching the crucial SCADA systems. There is no standard way to tackle the vulnerabilities. The type of mitigation the owner implements heavily depends on the type of infrastructure, the amount of risk the owner can afford, the amount of cost for installing, if he is willing to sacrifice efficiency at the cost of security.

Literature Review

Being student of cyber security and an enthusiastic fan of network security, the solution I am going to present is solely my idea and independent of anyone's work, which according to my knowledge might be a best fit mitigation strategy against DDOS attacks. [3] Presents a very broad strategy starting from assessing the risk depends on the infrastructure and providing an appropriate mitigations that are cost effective. Mitigations suggested are firewalls and authentication methods, and peer-to-peer overly routing. But so far their work presents a test bed created using only software. The complete solution would be to incorporate actual hardware in the simulations. [4] propose an architecture of a modular SCADA testbed, and describe their tool which mimics a SCADA network, monitors and controls real sensors and actuators using Modbus/TCP protocol. Using DDoS scenarios they showed how attackers can disrupt the operation of a SCADA systems. But the limitation of this work is that it shows only the mimics of Scada systems not the real world scenario. And many argue that simulations do not represent real world scenarios accurately. [5] Also shows the simulation form of SCADA systems, to assess the security vulnerabilities. They argue that it is impractical to conduct security experiments on live systems. But again as it is just a simulation it is more likely that their results won't fit the real world scenario. [6] Shows run time infrastructure (RTI) software by implementing C2WindTunnel. It shows simulation of scada systems and shows how it handles time and event managements. In proof of concept implementation of SCADA system, C2WindTunnel facilitated interaction and data transfer between environments and monitoring response to attacks. But for a complicated system, calculating effects would require intensive analytical computations, could be intractable. [7] They have explored the implementation of peer-to-peer routing overly to improve the survivability of Scada system under DOS attack on a shared communications infrastructure. They found out that peer-to-peer overly enhances on-time message delivery during bandwidth consumption DoS attack on shared communication Scada system infrastructure. But they didn't discuss the choice of peer-to-peer routing protocol, and peer discovery protocol. [8] They state that IDS is one of the most know prevention strategy for attacks (i.e DOS) against SCADA systems. But IDS technology is not compatible in all environments. So they propose new IDS technologies like signature matching, flow analysis and data inconsistency detection that are tailored particularly for SCADA systems. But also only IDS won't help much.

Research Question, Objective and Hypothesis

As shown in the figure 1 the 48170 of SCADA devices that vulnerable to DDoS attack and but still in use which is almost half of the total 1 Million SCADA devices. So the question remains is it really hard to patch these devices or just patching is not enough. Means there should some other layers of mitigations that can shield the SCADA system infrastructure and block the attack even before reaching the critical infrastructure. In case of DDOS attacks patching software might only avoid 1/3 portion of the attack. Generally software patches are suggested only when the vulnerabilities are exploited and attackers successfully achieve their goal.
There are many contributing factors of DDOS attacks that always give attackers the upper hand. Some of the contributing factors that makes the attacker job easy are ANY, DNSKEY, NSEC, NSEC3 queries. They are contributing factors because the attacker sends a small request and the target machine receive a large response. In other words using anyone of the above mentioned queries will lead to high amplification thus the victim machine will be heavily flooded with traffic. This traffic is so intensive that even traffic monitoring device can't handle this traffic and they just simply goes down. Also the existence of million open resolvers are advantageous to the attackers. More the number of open resolvers, higher the number of slave machine available for the attacker so the victim machine will come under attack from larger number of devices that's why it is called distributed denial of service.

In theory many mitigation strategies are suggested. Very few owners implement some of the mitigations to their infrastructure, the rest of the mitigation strategies are having adverse effects on the efficiency. So they can never be put in practice. One of the effective mitigation strategies is the implementation of BCP 38 protocol also known as ingress filtering. The idea behind ingress filtering is that the network operators will only allow the traffic to exit the network if the source IP address is a legitimate address from their network. Thus avoiding the IP spoofing and limiting DDOS attack at larger extent. This strategy works very well but unfortunately very few operators implement it. And the actual fruit of BCP 38 will be if all the operators implement it. Because if one operator implements it he will only make the other operators safe but unfortunately not himself.

Domain Name System Security Extension (DNSSEC) is also a major contributing factor of DDOS attack because it causes much higher amplification factor. Elliptical Curve Digital Signature Algorithm (ECDSA) might be a better alternative for DNSSEC. But at the time being ECDSA is still under the research.

So the SCADA system owner can't wait until all the above vulnerabilities are fixed, countermeasures that are widely suggested including disconnecting of SCADA system from public internet, or just simply reducing the number of SCADA systems in use. So he is left with no other choice but to combine different mitigation strategies and form a multi layered security infrastructure. Long story short the scada system owner can't depend on one mitigation strategy. I suppose multilevel mitigation strategy will not only give attackers hard time to perform successful DDOS attacks but will also promote the SCADA system technology thus there will be an increase in number of SCADA systems in use rather than reducing the number.

After presenting the real world scenario of DDOS attacks the research question might be *"Will forming a multi layered security architecture can become so far better option to mitigate DDoS attacks against SCADA systems"*. This multi layered will be based on combination of different FIREWALLs, Intrusion detection system, intrusion prevention system, Internet protocol security (IPSEC) and honeypots.

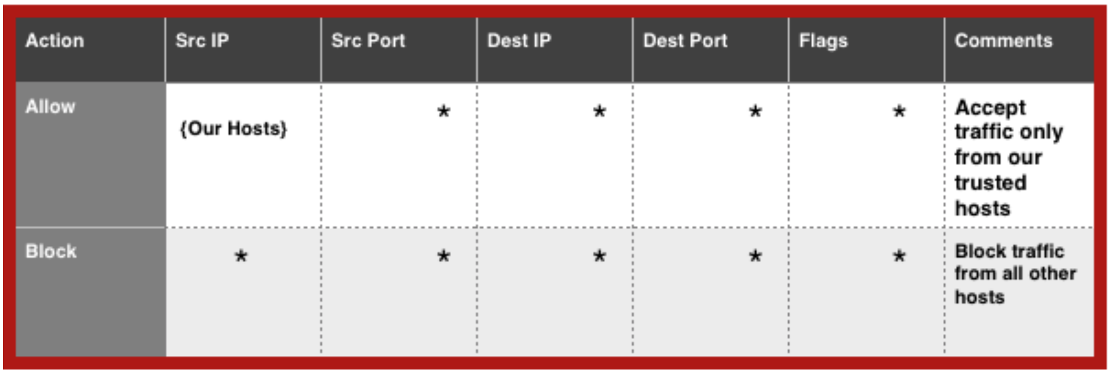
A substantive hypothesis would be considering our dataset the 48170 vulnerable SCADA systems in 2013, it would be hard and almost ineffective task to patch these vulnerable devices because of the difference in industry network architectures. Different network architecture might need different patches. Writing the patches is not the only hard task but installing patches is also tedious process. This is because during an update process the whole network will be down which is unacceptable for critical infrastructures. Therefore alternative mitigation approaches are required.

Security Model: Protecting SCADA Systems

As shown in the figure iv, that's how the security model will look like. At first firewall 1 is installed so that it will filter all the redundant and malicious traffic. After the first firewall the SCADA system owner is free to install honeypots or any other system where he can take risk and is not crucial part of the network. Afterwards IDS comes, it will look for both signatures based and anomalies based malicious traffic. Firewall 1 will make IDS job easy. In case any malicious traffic is received the IDS will make an alarm and IPS will take action against and prevent from such attack. Then comes firewall 2, it is because incase firewall 1 couldn't filter all the malicious traffic. So all the remaining malicious traffic will be block here. Next comes IPSEC VPN, which will allow traffic only from authenticated IP sources. So the SCADA system will not be only saved from malicious traffic but also from over flooded traffic.

The recommended security model is based on eight available SCADA security standards. Means that in these standards there are around 26 different recommended mitigation strategies. Some of these mitigation strategies are widely implemented while others are not. The idea behind this security model is that it will implement the top three most favorable mitigation approaches. That is Firewalls, Intrusion detection system, Intrusion prevention system, Internet protocol security, honeypot,

Firewall: When it comes to network protection against malicious and exhaustive traffic the first counter measure that comes to mind is the firewall. There are different types of firewalls like network level firewall, application level firewall, state-full firewall, stateless firewall. In case of stateless firewall each of the packet is processed independently, firewall rules are checked for each and every packet. This type of firewall is easy to implement and is very efficient. So the owner of the SCADA system can configure this type of firewall based on his own requirements. He can decide which sort of traffic to receive from which IP address on which port. Below figure shows the state-full firewall.



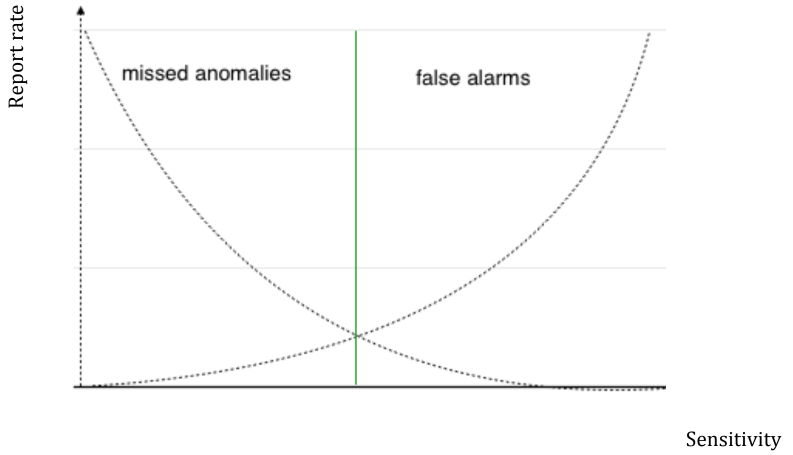
Action	Src IP	Src Port	Dest IP	Dest Port	Flags	Comments
Allow	{Our Hosts}	*	*	*	*	Accept traffic only from our trusted hosts
Block	*	*	*	*	*	Block traffic from all other hosts

So with the help of state-full firewall the malicious traffic is filtered and almost only trusted traffic is allowed access to the critical systems. At this stage it is also possible to configure the firewall policy in such a way that IP spoofing be avoided.

Even the firewalls have vulnerabilities. So lets take security mitigation one-step further.

Intrusion detection system (IDS):

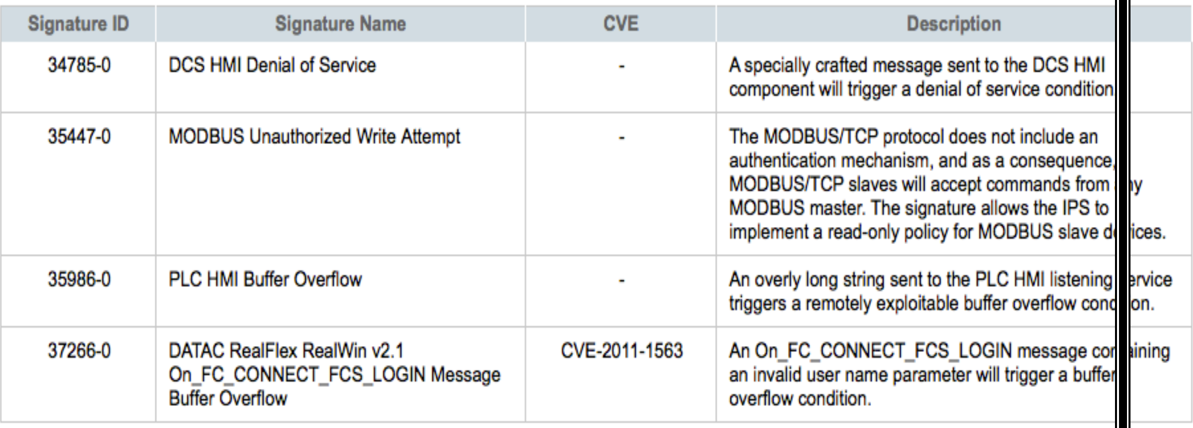
IDS monitors network traffic for any malicious activities or anomalies. So it identifies intrusions and reports them to the management station. They are of two types; knowledge based (aka signature based) and behavior based (aka anomaly based) IDS. It is good industrial practice to implement both types of IDS in SCADA systems. This is because of the fact that signature based IDS are embedded with know types of attacks/exploits signatures so as soon it detects any matching signature it will identify intrusion and anomaly based IDS detects unknown attacks and any irregularities in the network infrastructure. Anomaly based IDS is tuned according to requirements of SCADA system owner. Depends on how the parameters are selected but there will always tradeoff between detecting all the anomalies but it will raise many false alarms and missing anomalies with no false alarms. As shown in the figure below



The best feature of such strategy is that the owner has the authority to define his parameters based on his requirements.

Intrusion prevention system (IPS)

IPS will monitor the industrial network traffic for malicious activities or traffic and if any malicious activity or traffic is identified IPS will respond with prevention techniques that can be blocking the malicious IP address, dropping the malicious packets, resetting the connection. The most appropriate IPS would be Network-bases intrusion prevention system that will monitor the whole industrial network traffic looking for chary traffic. Based on the requirements of the problem owner he can install SNORT, OSSEC, or Suricata IPS. Each system has advantages and disadvantages. Following are examples of Cisco IPS signatures [20].



Signature ID	Signature Name	CVE	Description
34785-0	DCS HMI Denial of Service	-	A specially crafted message sent to the DCS HMI component will trigger a denial of service condition
35447-0	MODBUS Unauthorized Write Attempt	-	The MODBUS/TCP protocol does not include an authentication mechanism, and as a consequence, MODBUS/TCP slaves will accept commands from any MODBUS master. The signature allows the IPS to implement a read-only policy for MODBUS slave devices.
35986-0	PLC HMI Buffer Overflow	-	An overly long string sent to the PLC HMI listening service triggers a remotely exploitable buffer overflow condition.
37266-0	DATAC RealFlex RealWin v2.1 On_FC_CONNECT_FCS_LOGIN Message Buffer Overflow	CVE-2011-1563	An On_FC_CONNECT_FCS_LOGIN message containing an invalid user name parameter will trigger a buffer overflow condition.

The above two mitigation strategies purely based on statistical characteristics of the attack. There might be situation in which the attacker trick and bypass both the protection borders so therefore we need the third protection border that is responsible for authentication and confidentiality of the traffic and IPSEC will do that.

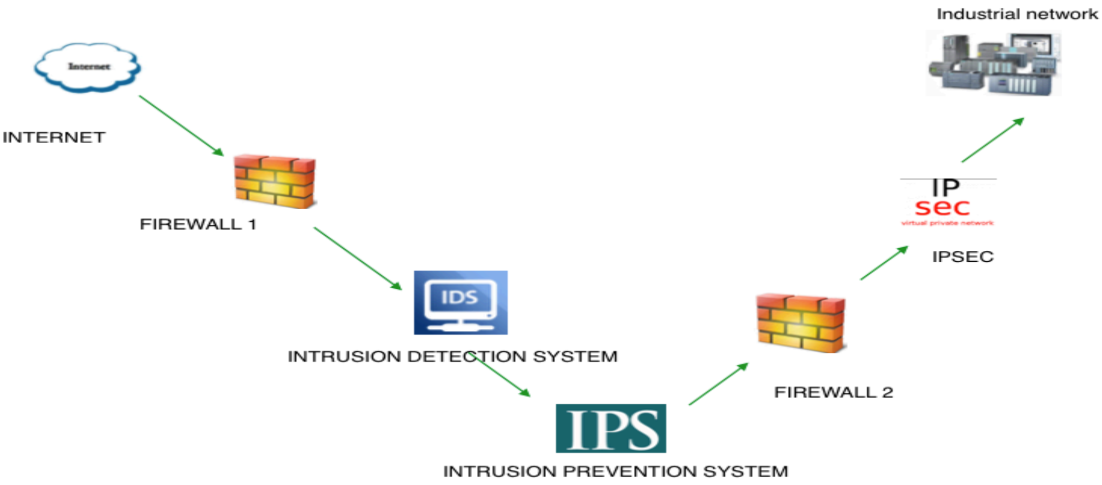
Internet protocol security (PSEC)

IPSEC comprise of set of protocols that provides secure IP communications by establishing mutual authenticating between the source and destination. IPSEC can be deploy to implement VPNs. IPSEC with transport mode and Encapsulating security payload (ESP) protocol will most appropriately fit the industrial network. IPSEC will not only block unauthenticated malicious traffic but will also provide confidentiality to SCADA system traffic by encrypting the traffic so that no one can spoof or alter the traffic.

Honeypots

Installing honeypot would be an excellent choice to understand malicious activities against the network, at the same time tracking the attacker and not being effected by the attack. It is optional if the owner is interested he can add it otherwise he can just ignore it. But it is good practice to add it.

Figure iv shows how the defense architecture will look like



Results

I am quite confident that my recommended security model for SCADA system would definitely take DDOS attack to its least limits. I will defend my findings with Standards and policies related to SCADA system security. The secure network infrastructure I recommend to counter DDOS attacks comprise the most recommended mitigation strategies in all the eight standards. Figure ii shows eight standards and guidelines that comply with SCADA system security and 26 different mitigation strategies are recommended in all the eight standards.

From [9] the keywords and phrases associated with the 26 groups of countermeasures occurred in total 8222 times in the eight SCADA standards. Figure iii shows the number of occurrences for each group normalized with the total number of occurrences in all standards. Based on the following figures I can justify my findings, absolutely follows all the best industry standards and recommendations.

Document(s)	Publisher
Good practice guide, process control and SCADA security [10]	Centre for the Protection of National infrastructure (CPNI)
Cyber security procurement language for control systems [11]	Department of Homeland Security (DHS)
21 Steps to improve Cyber security of SCADA Networks [12]	U.S Department of Energy (DOE)
CPI-0021-1-CIP-009-1 [13]	North American Electric Reliability Corporation (NERC)
Guide to industrial control systems (ICS) Security [14]	National institute of standards and technology (NIST)
System protection profile industrial control systems [15]	National institute of standards and technology (NIST)
ANSI/ISA-99.00-01-2007 part 1-3 [16][17][18]	The International society of Automation (ISA)

Cyber security for critical infrastructure protection [19]	U.S Government Accountability office (U.S GAO)

Figure ii [9]

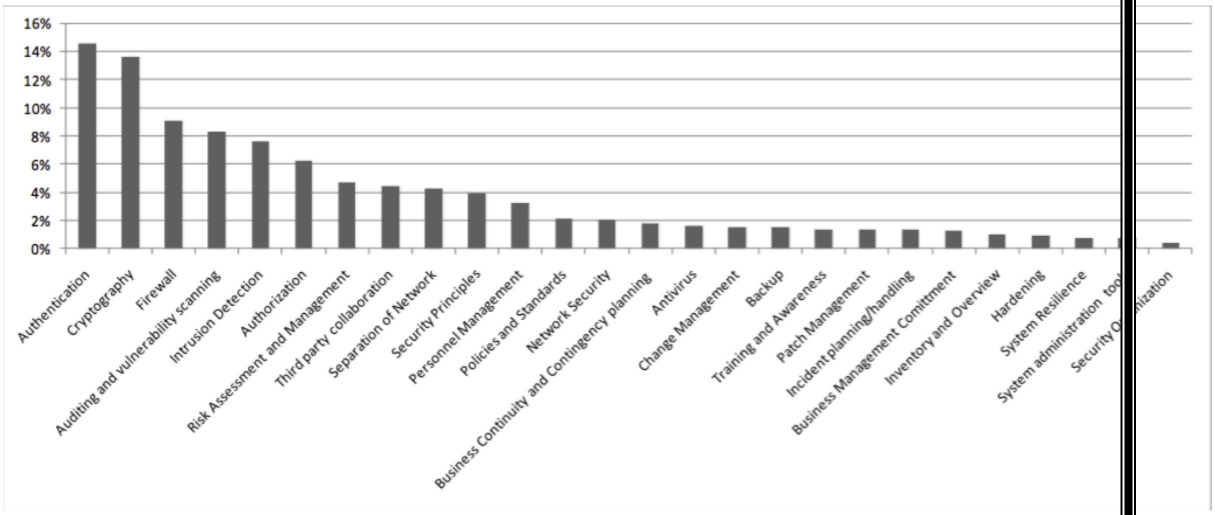
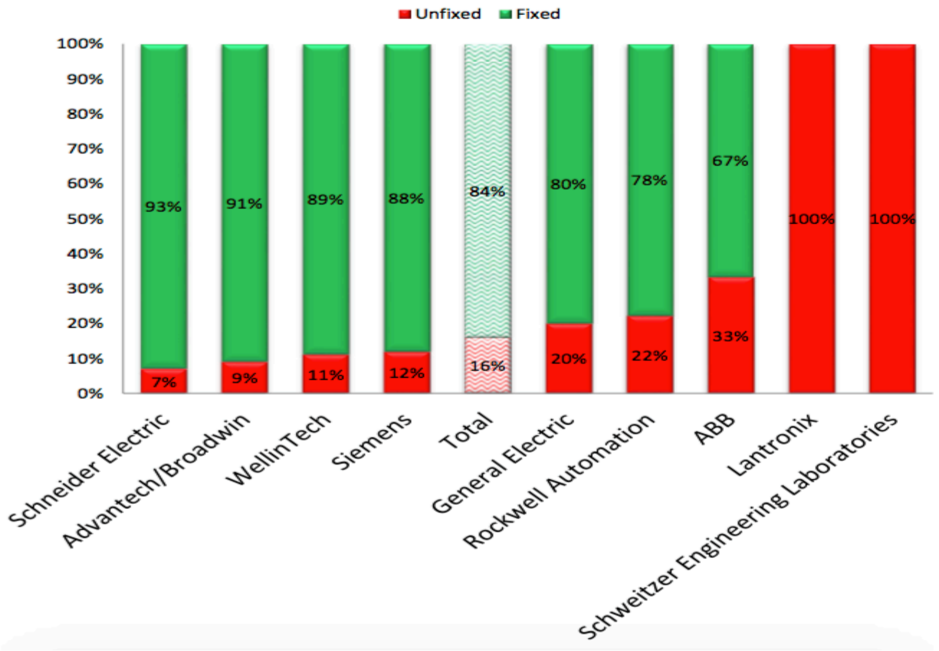
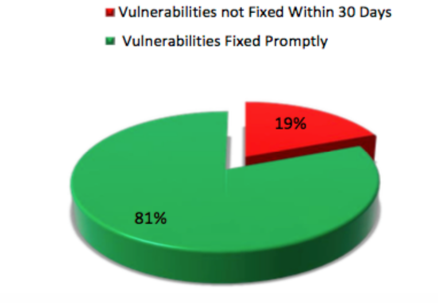


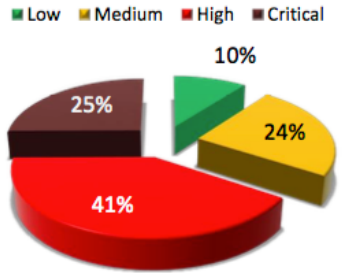
Figure iii [9]

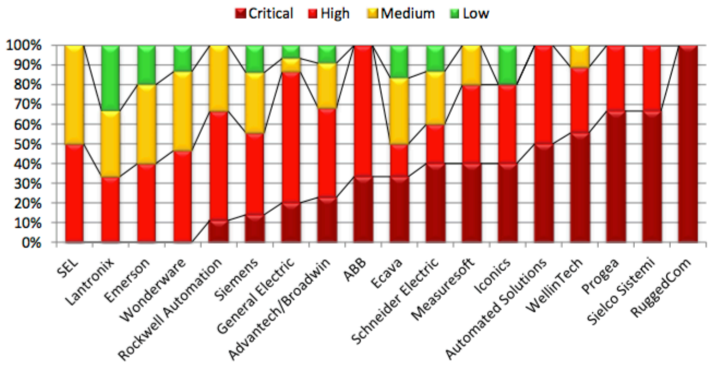
All the protocols I recommended are widely used in real world scenarios and are quite effective against existing DDOS threats.

Lets consider the security scenario of SCADA system and the security model I recommended. First lets consider SCADA systems. As I said before it is almost impossible to fix all the vulnerabilities of SCDA devices and on average it almost takes a month to fix the vulnerabilities during that time the attacker is free to take advantages of such vulnerable devices. And most of these vulnerabilities are of high or critical level. Below are some of the figures [21], which will support this claim.

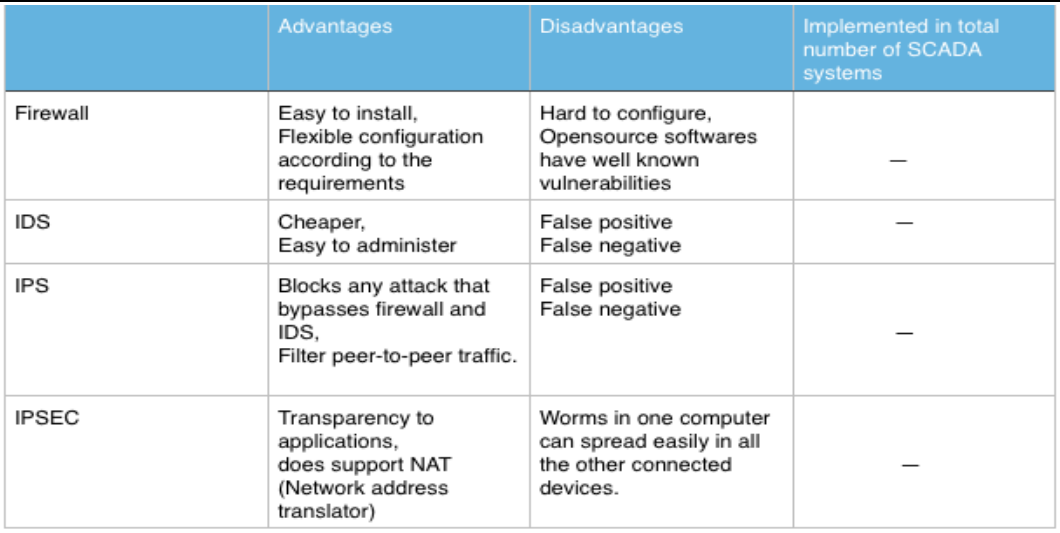








Approximately 1,000,000 SCADA devices are used. In the following table I will elaborate the number of scada devices comprising any of the suggested protocols (firewall, IDS, IPS, IPSEC VPN) and advantages and disadvantages of these protocols implementation but in most cases the advantages outweigh the disadvantages.



	Advantages	Disadvantages	Implemented in total number of SCADA systems
Firewall	Easy to install, Flexible configuration according to the requirements	Hard to configure, Opensource softwares have well known vulnerabilities	—
IDS	Cheaper, Easy to administer	False positive False negative	—
IPS	Blocks any attack that bypasses firewall and IDS, Filter peer-to-peer traffic.	False positive False negative	—
IPSEC	Transparency to applications, does support NAT (Network address translator)	Worms in one computer can spread easily in all the other connected devices.	—

Table below shows the time difference between the SCADA system to fix the vulnerability and firewalls/IDS/IPS. The time to fix vulnerabilities in firewalls/IDS/IPS is less than just a day because of the fact that these protocols mostly have misconfiguration faults which is easy and quick to fix. While of SCADA systems it almost takes a month.

	Time to fix vulnerabilities (Days)
SCADA systems	=>30
Firewalls/IDS/IPS	=>1

Finding and fixing vulnerabilities during the development phase is quite cheap but once the system is deployed it too expensive to fix. For SCADA systems it almost take around €10,000 to only find the vulnerability not fixing it. It can take up to €1Million to fix a vulnerability.

	Cost to fix vulnerabilities (€)
SCADA systems	Up to 1 Million
Firewalls/IDS/IPS	30,000/Year to manage

Considering all the above facts and figures, Firewall/IDS/IPS/IPSEC might be the secure, cost effective and time efficient solution for all SCADA system.
Hence we can conclude that the security model I recommend is cheaper to maintain, easy to install, and much more secure than existing security models.

Limitations

Considering the limitations of my work, I won't say its limitation rather I would say a challenging task be to properly configure all these protocols and test the design in real world scenario. Because it is almost impractical to test new designs in real infrastructure. Also maintaining such a complex system would a tiresome task. From a security prospective, complexity is a type of vulnerability itself. But as we are living in much faster and sophisticated technology era such a model won't be consider as too complex and would be compatible with existing technologies.

Designing, configuring, testing and implementing this model might be chellenging. But for companies who are losing €22,000/min because of DDOS attack, such system might be an attractive remedy.

Conclusion

As DDOS attacks against SCADA systems are quite serious so there are huge number of mitigation strategies. But it is obvious that no system can be 100% secure and security always comes with the cost of losing efficiency. Based on my experience in network security and architecture the recommended security model well fits the requirements of SCADA systems security and might show surprising results. The best feature of multi level security architecture is that it requires the attacker to pass through many obstacles and having honeypot software in the network might be a better way to trace back the attacker and give him a taste of justice. The other good feature of this security model is that it can be implemented in any industrial network infrastructure and also the owner has the flexibility to set the requirements of the network and this model will fully suit his requirements. The owner of the SCADA system wants secure and functioning network, this model will fulfill both of his wishes at a lower price.

References

[2] James M Buchanan and W Craig Stubblebine. “Externality”. In: Economica 29.116 (1962), pp. 371–384.

[3] http://tcipgwebpro.web.engr.illinois.edu/sites/default/files/papers/NAPS06.pdf

[4] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5319283

[5] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6009221

[6] http://mr-modi.chabukswar.in/projects/scspresentation.pdf

[7] http://delivery.acm.org/10.1145/1170000/1161796/p300-farris.pdf?ip=130.89.237.67&id=1161796&acc=ACTIVE%20SERVICE&key=0C390721DC3021FF%2E7DEDEACE9AC2380A%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=728183650&CFTOKEN=11566521&__acm__=1446904282_9e709e8531c38d61be113b580a61b272

[8] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6162722

[9]http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.172.630&rep=rep1&type=pdf

[10] CPNI, “Good Practice Guide, Process Control and SCADA Security,” Centre for the Protection of National Infrastructure (CPNI), 2005.

[11] DHS, “Cyber Security Procurement Language for Control Systems,” DHS, August 2008.

[12] DOE, “21 steps to Improve Cyber Security of SCADA Networks,” Office of Energy Assurance, U.S. Department of Energy, 2002

[13] NERC, “CIP-001-1 - CIP-009-1,” North American Electric Reliability Corporation

(NERC), 2006

. [14] K. Stouffer, J. Falco, K. Scarfone, “Guide to Industrial Control Systems (ICS) Security Special Publication 800-82,” Second public draft, National Institute of Standards and Technology, September 2007

. [15] NIST, “System Protection Profile - Industrial Control Systems,” Version 1.0, National Institute of Standards and Technology (NIST), April 2004

. [16] ISA, “ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models,” International Society of Automation (ISA), October 2007

. [17] ISA, “ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems,” International Society of Automation (ISA), October 2007

. [18] ISA, “ANSI/ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment,” International Society of Automation (ISA), October 2004

. [19] GAO, “Technology Assessment - Cybersecurity for Critical Infrastructure Protection,” U.S. Government Accountability Office, May 2004

. [20] http://www.cisco.com/web/about/security/intelligence/protecting_ics_networks_with_cisco_ips.html

[21] http://www.ptsecurity.com/upload/ptcom/SCADA_WP_A4.ENG.0018.01.DEC.29.pdf