An Empirical Study of TCP Vulnerabilities in Critical Power System Devices

David Formby, Sang Shin Jung, John Copeland, and Raheem Beyah
Communications Assurance and Performance (CAP) Group, School of Electrical and Computer Engineering, Georgia Institute of Technology
Atlanta, GA, USA
djformby@gatech.edu, sangsin@gatech.edu, john.copeland@ece.gatech.edu, raheem.beyah@ece.gatech.edu

ABSTRACT

Implementations of the TCP/IP protocol suite have been patched for decades to reduce the threat of TCP sequence number prediction attacks. TCP, in particular, has been adopted to many devices in the power grid as a transport layer for their applications since it provides reliability. Even though this threat has been well-known for almost three decades, this does not hold true in power grid networks; weak TCP sequence number generation can still be found in many devices used throughout the power grid. Although our analysis only covers one substation, we believe that this is without loss of generality given: 1) the pervasiveness of the flaws throughout the substation devices; and 2) the prominence of the vendors. In this paper, we show how much TCP initial sequence numbers (ISNs) are still predictable and how time is strongly correlated with TCP ISN generation. We collected power grid network traffic from a live substation for six months, and we measured TCP ISN differences and their time differences between TCP connection establishments. In the live substation, we found three unique vendors (135 devices, 68%) from a total of eight vendors (196 devices) running TCP that show strongly predictable patterns of TCP ISN generation.

Categories and Subject Descriptors

K.6.5 [**Security**]: Security

Keywords

TCP sequence number; TCP sequence prediction; power grid; SCADA; DNP3

1. INTRODUCTION

Power grid networks have been used for a long time to help utility providers manage power distribution during normal and abnormal (e.g., line outage) operations. The power grid SCADA network can be divided into categories by type of device: human machine interfaces (HMIs), historians, front-end processors (FEPs) (SCADA masters in general), remote terminal units (RTUs), and intelligent electronic devices (IEDs) or relays. Although some of the machines still run their application protocols over a serial or Ethernet link layer, some advanced machines have adopted TCP/IP protocol suites (e.g., DNP3/TCP), which increases their accessibility. However, the benefits provided by the TCP/IP protocol suite do not come without a cost. That is, now power grid devices must be concerned with traditional network threat vectors, including attacks against protocols in the TCP/IP protocol suite.

Previous guidelines, whitepapers, and reports on SCADA security requirements have pointed out weaknesses of security services that include lack of access controls, encryption of data, and security application deployment [1, 9, 11, 14, 15, 17]. They also provide suggestions for SCADA specific configurations of security applications (e.g., firewall rules for DNP3). In previous research, Zhu et al. provided a thorough survey and taxonomy of the security risks in SCADA [20,21]. The threats mentioned in previous works are mostly advanced attacks against TCP/IP protocols (e.g., TCP SYN flood or injecting malformed TCP packets) and well-known malware targeting the network.

However, according to our empirical observations, a weakness of predictable TCP ISN generation remains in devices in the power grid network. This fact is alarming given that Bellovin highlighted this security problem in 1989 [3]. Bellovin and others have also suggested better ways of generating TCP ISNs since the vulnerability was found. Modern operating systems (e.g., OSX, Windows, or Linux) have been updated and increased the randomness of TCP ISNs, but *most of* the machines' OSes in the power grid network that we observed did not have random TCP ISNs.

In this paper, we investigate the notable patterns of TCP ISN generation in the network traffic captures from a live substation. Our study aims to point out the weakness of TCP ISN generation found in a current power grid network. Our main contributions are the following:

- We collect network traffic from a live substation in a power grid network.
- We present clustered ISN distributions that use a fraction of the entire TCP sequence number space.
- We provide analysis that illustrates that the patterns of the TCP ISN generators of most of the observed

SEGS'14, November 7, 2014, Scottsdale, Arizona, USA.
Copyright 2014 ACM 978-1-4503-3154-8/14/11 ...$15.00.
http://dx.doi.org/10.1145/2667190.2667196.

devices are easily predictable and strongly depend on the local time.

The rest of this paper is organized as follows: We review related works in Section 2. In Section 3, we describe the dataset that we use in this study. Section 4 describes the methodology used to analyze the data. We present our results in Section 5 and discuss their implications in Section 6. Finally, we conclude our research and discuss future work in Section 7.

2. RELATED WORK

When the TCP/IP protocol suite was first developed, it was built on a foundation of trust among users. While reliability and robustness were the primary goals, security was not a consideration, resulting in inherent flaws that have required several patches and updates over the years as their significance has been discovered. Although these weaknesses and various defenses against them have been studied thoroughly, some industries (such as the power industry), have been slow to implement the defenses due to cost concerns, difficulty and risk of patching crucial equipment, or just a lack of understanding of the vulnerabilities and their possible consequences.

One of the first known discoveries of the vulnerabilities of the TCP/IP protocol suite was published by Robert Morris out of Bell Labs in 1985. Morris described how the 4.2BSD implementation of the protocol stack used predictable ISNs for its TCP connections, which allowed attackers to pose as legitimate hosts and remotely run commands on the victim machine. He then suggested defenses against these attacks including randomizing the ISNs and modifying the gateways to reject outside packets claiming to come from the internal network [10].

Building off of the work by Morris, but providing a much broader overview, Steven Bellovin published a widely known paper in 1989 where he analyzed the security problems found in the TCP/IP protocol suite as it was being used at the time. Two of the fundamental problems that he pointed out in the protocol stack was the use of IP address based authentication and the use of predictable sequence numbers. He explained how address spoofing was so easy that it rendered address-based authentication, used in services such as *rsh*, as virtually useless, and how using predictable sequence numbers provided means of attacking both the TCP and DNS protocols. To address these weaknesses, Bellovin recommended randomizing ISN generation and using cryptographically based authentication methods [3]. When he revisited his work in 2004, he reaffirmed his initial conclusions and was relieved to note that most networks were moving away from address-based authentication, plaintext passwords, and completely predictable ISNs [5]. However, as we found in our research, this statement does not necessarily hold true for possibly the most critical networks, those controlling the power grid. Realizing that predictable ISNs were a major problem with the TCP protocol, Bellovin provided specific recommendations on how to generate them in a 1996 RFC [4], and a revised version with the help of Fernando Gont in a 2012 RFC [6].

Attacks taking advantage of predictable sequence numbers have not only been discussed in theory, they have also been demonstrated and used in the real world. The most well known case was one where Kevin Mitnick was able to hijack Tsotuma Shimomura's X-terminal session by predicting the ISN to be used. Shimomura was able to capture the tcpdump for the entire attack and explained it step by step. In short, Mitnick filled up the login server's queue, probed X-terminal to understand the ISN generation algorithm, and was able to successfully pose as the login server and open up an X-terminal shell [13].

When the details of Mitnick's attack were released, the significance of having predictable ISNs was finally getting the attention it deserved and vendors began to address the problem. However, in 2001 Michal Zalewski published a whitepaper analyzing just how random or predictable ISN generators were for different operating systems, and found disappointing results. Zalewski discovered that although vendors had implemented various pseudo-random generators for their ISNs, most were very weak and could still be guessed by an attacker with reasonable resources [18]. When Zalewski performed this same analysis a year later, he found that only one vendor had properly addressed the issue while the rest had either done nothing, or implemented solutions that provided no significant improvement over the previous ones [19].

Hijacking a connection is also not the only concern that arises from using predictable ISNs, especially in the case of important long lived connections, such as those used in BGP and time-sensitive power system control networks. In 2003, Paul Watson published a whitepaper highlighting the feasibility of an attacker brute force guessing the sequence number to perform a TCP reset denial of service (DoS) attack. He pointed out that many implementations of the protocol stack accept and act on reset flags if they are simply in the TCP window, making a reset DoS attack feasible in a matter of minutes or even seconds. Proposed defenses against this kind of attack include firewall rules to check for internal address spoofing and the use of cryptographic authentication options in the TCP header [16]. Although this attack is not very feasible or useful for short-lived connections, a disruption in a long term TCP connection carrying time-sensitive control and measurement data in a power system could have much more dire consequences.

The application of these well known TCP hijacking and DoS attacks in the area of power system networks could pose much more significant problems than in other areas. For example, an attacker could theoretically insert packets into TCP connections to perform false data injection attacks as described by Liu et al. in their 2009 paper [8]. Even worse, if weak authentication mechanisms are used, an attacker could hijack a connection after the authentication window, pose as the control center or remote terminal unit (RTU) and begin issuing commands to operate generators and breakers throughout the grid causing serious physical damage. Additionally, if an attacker has no knowledge of the operation of the power system, he could still potentially implement coordinated reset DoS attacks that could delay the receipt of important control and measurement messages, interfering with the safe operation of the grid. Even though these vulnerabilities have been studied and known for almost *thirty years* now, this research has found that devices controlling the operation of the US power grid are still quite vulnerable to these attacks. In this paper, we use traffic captured from a live distribution substation to show just how predictable power system ISNs are in hopes of bringing about serious

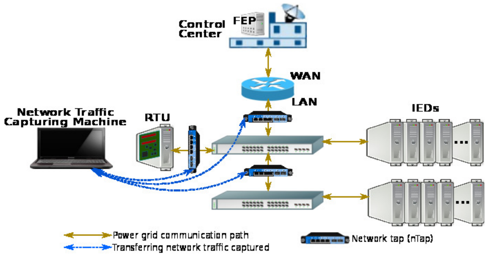

Control Center
FEP
WAN
LAN
Network Traffic Capturing Machine
RTU
IEDs
...
Power grid communication path
Transferring network traffic captured
Network tap (nTap)

Figure 1: Network capture environment in the live substation.

change in the design and implementation of critical power system devices.

3. DATASET

In this section, we present the dataset used in our study and describe an overview of the dataset from the live substation.

We installed our network traffic monitoring system in the live substation as shown in Figure 1. The network environment in which we capture network traffic consists mainly of an RTU and IEDs connected to network switches and a router. In the live substation, the RTU has frequent communication with IEDs and the FEP at the control center. IEDs have periodic communication with the RTU and sometimes have communication with the FEP at the control center as well, but not frequently.

In total, our dataset that we collected for six months (about 40 GB) consists of 210 devices including the RTU, IEDs and some devices (e.g., the FEP) from the WAN through the router. We categorize the devices in vendor types by media access control (MAC) addresses. Eight different vendors (VDs)[1], which are well-known in the power grid industry, provide most of the devices: VD1-3, VD5-6, and VD8 for IEDs, VD4 for the router, and VD7 for the RTU as shown in Table 1. We have analyzed only 196 (of the 210) devices that run TCP for their application protocols: most of them are DNP3 and others are HTTP and Telnet[2].

4. METHODOLOGY

After an initial characterization of the dataset [7] suggested that some devices had uneven distributions of TCP ISNs, the issue of TCP ISN generation was studied in more detail. Since the outdated original TCP specifications recommended the use of a clock-based generation algorithm [12], the dataset was first analyzed to see if there was any relationship between time and the ISNs generated. Specifically, the time between appearances of TCP ISNs was plotted against the difference between the two consecutive ISNs for every device. To avoid the complications of sequence number wrap-around, a sliding time window was used to limit the analysis to shorter times between ISN generation and heuristic thresholds were used to detect when the ISNs appeared to wrap around in a linear fashion. To test for linear relationships the sample Pearson Correlation coefficient [2] was used, given by Equation 1, where X and Y are two signals to be analyzed, $\bar{X}$ and $\bar{Y}$ are their respective means, and r is a measure of the linear relationship between the two. Pearson Correlation coefficients of *1* suggest a direct positive linear correlation, values of *-1* suggest direct negative linear correlation, and a value of *0* indicates that there is no linear relationship.

Table 1: The summary of power grid network traffic for six months (VD refers to vendor types).

Vendor types	# w/ TCP / # of all devices	Device types
VD1	1 / 1	IED
VD2	6 / 6	IED
VD3	39 / 43	IED
VD4	14 / 18	Router
VD5	1 / 1	IED
VD6	133 / 135	IED
VD7	1 / 1	RTU
VD8	1 / 5	IED
Total	196 / 210	-

$$r = \frac{\sum(X-\bar{X})(Y-\bar{Y})}{\sqrt{\sum(X-\bar{X})^2}\sqrt{\sum(Y-\bar{Y})^2}} \tag{1}$$

5. RESULTS

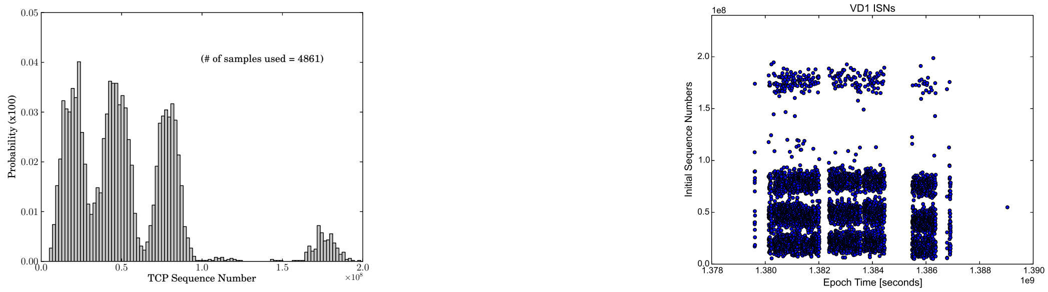
Clustered ISNs. When we ran our analysis again over a dataset with a longer duration (6 months vs 2 months) for the same device that was noted in previous research [7], the distribution of ISNs again showed very distinct clusters, as in Figure 2a. However, when we looked closer at the ISN generation shown in Figure 2b, there was no clear pattern or dependence on time, suggesting the use of a very weak pseudo random generator.

Predictable ISNs An ideal randomized ISN generator would equally use the entire sequence number space over a long period of time, resulting in a uniform distribution of ISNs. At first glance, the ISN distribution for the RTU over the course of six months, illustrated in Figure 3a, appears to show signs of a strongly random generator (i.e., there is an equal distribution of ISNs throughout the entire 32-bit space). However, when the ISNs are plotted against time over a short period (Figure 3b) it becomes obvious that they are strongly correlated with time and that they are far from random. Additionally, during this time window the RTU was initiating connections with various IEDs out in the field to poll for event data, suggesting that the same global ISN generator was used, no matter what device the RTU was talking to.

Our research found that the majority of the devices on the substation network, including both the RTU and IEDs in the field, still suffer from predictable ISN generation pat-

[1] We anonymized the vendors since they are critical information and are deployed in the live substation. Also, some of the vendors studied here are in process of filing and confirming ICS-CERT Vulnerability Reports.

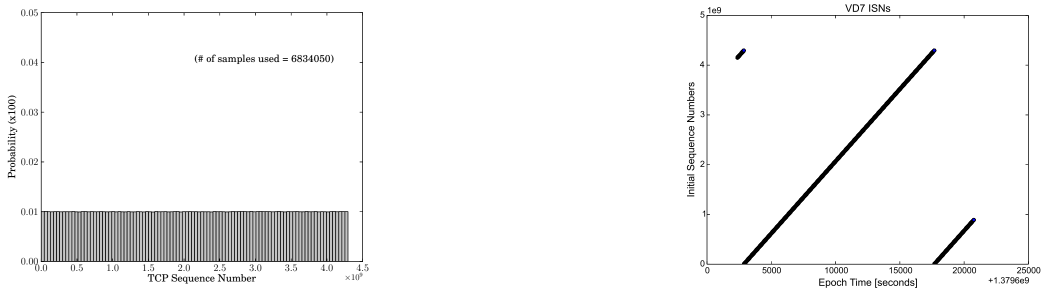
[2] We understand the implications of using this protocol, but our focus is on TCP sequence number predictability in this work.



(a) Distribution of ISNs for VD1 over six months

(b) Example ISN generation pattern for VD1

Figure 2: VD1 ISN Distribution and Pattern



(a) Distribution of ISNs for VD7 RTU over six months

(b) Example ISN generation pattern for VD7 RTU

Figure 3: VD7 ISN Distribution and Pattern

terns. In fact, most of the devices seen on the network increased their ISNs in a direct linear relationship with time and closely resembled the patterns of the RTU illustrated in Figure 3b.

The ISN generation pattern for the RTU was then analyzed using a more generalized method by plotting the time between connection initiations versus the difference between the sequence numbers used in the two consecutive initiations. Therefore, if the change in time results in a linearly proportional change in ISN, the scatter plot should be a line with a constant slope. Figure 4 shows the results when the first 1000 such data points were collected from the RTU in the dataset. As the graph suggests, the two quantities have a direct linear relationship and the Pearson correlation coefficient was found to be 0.995. The scatter plot also shows signs of being a piece-wise step function, which could be caused by incrementing the ISN by a large constant for a given time interval. In fact, after closer inspection, it was found that each ISN increment was always a multiple of 64000, and that for a given time increment, there were always only a small number of possibilities for the ISN increment.

After plotting the same type of graphs for all of the VD6 IEDs, it was found that ones in the field behaved differently from ones in the substation. The IEDs in the field, referred to as Type 1, all displayed a linear relationship between time and ISNs generated, whereas the IEDs in the substation, Type 2, appeared to be much less predictable. As of now it is not clear whether this difference was caused by different firmware versions, or possibly due to the nature of the connections. The Type 2 devices in the substations appeared to have much longer lived connections and transmit more data per connection, so it is possible that the algorithm operates slightly differently in those cases. To create Figure 5, the first 100 data points were collected from each of the 128 VD6 Type 1 devices, resulting in a strong linear relationship that was found to have a Pearson correlation of approximately 1 when rounded to three significant digits.

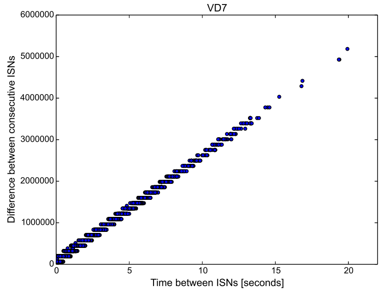


Figure 4: Scatter plot of time between ISNs and changes in ISNs for VD7 RTU (1 device)

The VD6 Type 2 devices had much longer lived connections and longer time periods between ISNs, which resulted in fewer data points in the small sliding time window, and only totaled 30 for the five devices. While Figure 6 shows some of the same signs of the ISNs having a linear relationship with time, it is much less predictable and more data in this time window would be needed to perform stronger analysis. Due to the sporadic placement of the points on the scatter plot, the Pearson coefficient for this smaller dataset was found to be -0.296, suggesting that there is not a clear linear relationship.

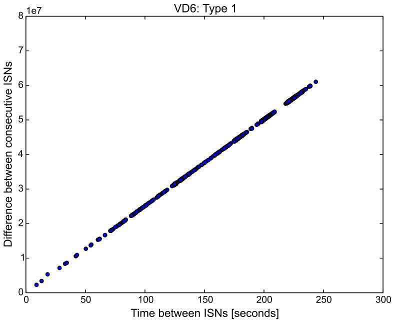


Figure 5: Scatter plot of time between ISNs and changes in ISNs for VD6 Type 1 (128 devices)

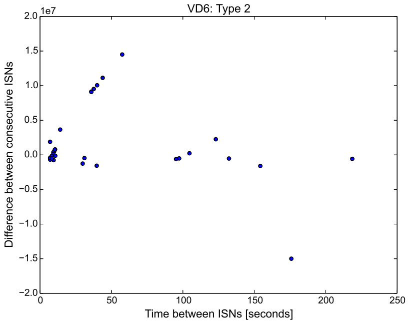


Figure 6: Scatter plot of time between ISNs and changes in ISNs for VD6 Type 2 (5 devices)

The VD2 devices, found both in the substation and in the field, also had very long-lived connections and long time periods between connection initiations, making it hard to form any concrete conclusions about the ISN generation. However, as Figure 7 illustrates, the 14 data points collected from a total of 6 devices suggest that this vendor's ISN generator also has a strong linear relationship with time. Even though more data needs to be collected to verify these results and perform more accurate calculations, the Pearson coefficient for this data was also found to be approximately 1 when rounded to three significant digits.

The results of this research are summarized in Table 2 with 135, approximately 68%, of the total 196 devices seen on the network suffering from easily predictable ISNs.

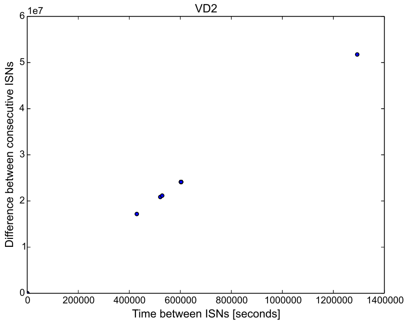


Figure 7: Scatter plot of time between ISNs and changes in ISNs for VD2 (6 devices)

Table 2: Table of Pearson Correlation coefficients

Device	Coefficient	Number of Data Points	Number of Devices
VD7	0.995	1000	1
VD6 Type 1	≈1	12800	128
VD6 Type 2	-0.296	30	5
VD2	≈1	14	6

6. DISCUSSION

Although TCP ISN prediction attacks are actually quite an old concept, the fact that these vulnerabilities are still found in devices today that control the US power grid is rather alarming. To protect against these attacks, most other OSes have adopted more randomized ISN generators and the applications running on them use stronger types of authentication (such as digital signatures) when security is important. However, our results show that a large number of power system devices still use predictable ISNs and all of the devices seen used either no authentication or sent passwords in clear-text. These weaknesses allow for a variety of attacks that could potentially lead to catastrophic results.

To briefly illustrate the types of attacks that exploit these weaknesses, we consider two threat models based on the predictability of the ISN generation algorithm.

Exploiting Clustered ISN Distributions. The first model we consider is one illustrated by the example VD1 ISN generation pattern in Figure 2b. In this model, the ISN generation algorithm has no clear relationship to time and appears to be pseudo-randomly distributed over short time periods. However, when analyzed over long time periods, Figure 2a shows that certain ranges of numbers are used much more frequently than others, effectively reducing the 2^{32} sequence space to a much smaller one. After closer inspection, the distribution shows that roughly 70% of the ISNs fall within the range of 0 to 100 million, covering only 2% of the entire sequence space of 4 billion. Additionally, there are clusters within this smaller range that are also more likely to appear than others. This aids an attacker in a TCP hijacking attempt by allowing him to make intelligent guesses at likely ISNs, thereby increasing his chances at guessing a valid ISN within a feasible amount of time.

Under this threat model, an attacker could know the distribution of a certain vendor's ISNs beforehand and never have to probe or sniff the target network, which means he could even launch the attack from thousands of miles away if the devices were connected to the Internet. A determined adversary can then launch millions of hijacking attempts, while guessing the most likely ISNs, and have a significant chance of finding a valid ISN in a reasonable amount of time. In the case where an attacker is located too far away to be able to forge responses to time-sensitive requests, it is still possible for him to cause damage by forging unsolicited responses, control commands, and maliciously crafted configuration files.

Exploiting Predictable ISN Algorithms. The second model attacks the time-based sequence number predictability illustrated by most of the devices studied in this paper. In this case, the devices use easily predictable ISN generation algorithms based on some deterministic signal, such as the local time. In order for an attacker to fully take advantage of this, he would have to obtain an ISN and time-stamp from which he could then predict all future ISNs. While this creates a stronger adversarial model, practical methods of doing so include sniffing the network in a weakly guarded substation, or as in Mitnick's case, probing a server with SYN requests. Once an ISN is obtained, the attacker would only require a trivial number of guesses before finding a valid ISN and almost instantly be able to hijack a connection.

As in the previous attack model, once the attacker has hijacked a connection, he may begin to inject false data or dangerous commands into the power grid while posing as the RTU or Control Center.

7. CONCLUSIONS AND FUTURE WORK

The inherent security flaws in power system equipment today pose an alarming threat to the modern world. This research found that devices used to control the distribution of power to keep our hospitals, transportation, and commerce operating smoothly show signs of being vulnerable to attacks that have been studied for almost thirty years. These types of attacks, which could theoretically be used to cause physical harm to the power grid resulting in significant economic damage, must be avoided by patching important devices and implementing strong authentication methods.

An ICS-CERT Vulnerability Report has been filed and confirmed regarding the clustered ISNs for VD1. We are now working with the vendor to generate a patch. Additionally, we are in the process of filing ICS-CERT vulnerability reports for the devices that showed predictable sequence numbers (i.e., VD2, VD6, and VD7).

For future work, the ISN generation data will be studied in more detail to look for more complex, but still predictable, patterns. The research could also be extended by obtaining devices to test in a controlled environment to record more ISN data as well as to demonstrate an attack that exploits these weaknesses.

8. ACKNOWLEDGMENTS

This work was partly supported by DARPA-N10AP20022 and NEETRAC.

9. REFERENCES

[1] 21 Steps to Improve Cyber Security of SCADA Networks. `http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf`.

[2] The pearson correlation coefficient. `http://forrest.psych.unc.edu/research/vista-frames/help/lecturenotes/lecture11/pearson.html`.

[3] S. M. Bellovin. Security Problems in the TCP/IP Protocol Suite. *SIGCOMM Comput. Commun. Rev.*, 19:32–48, 1989.

[4] S. M. Bellovin. RFC 1948 - Defending Against Sequence Number Attacks. 1996.

[5] S. M. Bellovin. A Look Back at "Security Problems in the TCP/IP Protocol Suite". In *Proceedings of the 20th Annual Computer Security Applications Conference*, ACSAC '04, pages 229–249, Washington, DC, USA, 2004. IEEE Computer Society.

[6] F. Gont and S. M. Bellovin. RFC 6528 - Defending against Sequence Number Attacks. Technical report, Feb. 2012.

[7] S. S. Jung, D. Formby, C. Day, and R. Beyah. A First Look at Machine-to-Machine Power Grid Network Traffic. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, 2014.

[8] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 21–32, New York, NY, USA, 2009. ACM.

[9] R. E. Mahan, J. R. Burnette, J. D. Fluckiger, C. A. Goranson, S. L. Clements, H. Kirkham, and C. Tews. Secure Data Transfer Guidance for Industrial Control and SCADA Systems. Technical Report PNNL-20776, Pacific Northwest National Laboratory, Richland, Washington, September 2011.

[10] R. T. Morris. A weakness in the 4.2bsd unix tcp/ip software, 1985.

[11] L. Piètre-Cambacéd, M. Tritschler, and G. Ericsson. Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs. *Power Delivery, IEEE Transactions on*, 26(1):161–172, jan. 2011.

[12] J. Postel. RFC 793 - TRANSMISSION CONTROL PROTOCOL. Technical report, September 1981.

[13] T. Shimomura. Technical details of the attack described by markoff in nyt. `http://www.gont.com.ar/docs/post-shimomura-usenet.txt`, 1995.

[14] K. Stouffer, J. Falco, and K. Scarfone. Guide to Industrial Control Systems (ICS) Security. Technical Report Special Publication 800-82, NIST, June 2011.

[15] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn. Guide to Industrial Control Systems (ICS) Security. Technical Report Special Publication 800-82, Rev2, NIST, May 2014.

[16] P. A. Watson. Slipping in the window: Tcp reset attacks. `http://packetstormsecurity.com/files/author/3245/`, 2003.

[17] T. Yardley. SCADA: Issues, Vulnerabilities, and Future Directions. *;login:*, 33(6):14–20, Dec. 2008.

[18] M. Zalewski. Strange attractors and tcp/ip sequence number analysis. `http://lcamtuf.coredump.cx/oldtcp/tcpseq.html`, 2001.

[19] M. Zalewski. Strange attractors and tcp/ip sequence number analysis - one year later. `http://lcamtuf.coredump.cx/newtcp/`, 2002.

[20] B. Zhu, A. Joseph, and S. Sastry. A Taxonomy of Cyber Attacks on SCADA Systems. In *Proceedings of the 4th International Conference on Cyber, Physical and Social Computing*, pages 380–388, oct. 2011.

[21] B. Zhu and S. Sastry. Scada-specific intrusion detection/prevention systems: A survey and taxonomy. In *Proceedings of the First Workshop on Secure Control Systems*, SCS'10, Stockholm, Sweden, 2010.