Flow-Based Security Issue Detection in Building Automation and Control Networks

Pavel Čeleda, Radek Krejčí, Vojtěch Krmíček

Flow-based Security Issue Detection in Building Automation and Control Networks

Pavel Čeleda[1], Radek Krejčí[2] and Vojtěch Krmíček[1]

[1] Institute of Computer Science, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic
{celeda|vojtec}@ics.muni.cz
[2] CESNET, z.s.p.o., Zikova 4, 160 00 Prague
Czech Republic, rkrejci@cesnet.cz

Abstract. The interconnection of building automation and control system networks to public networks has exposed them to a wide range of security problems. This paper provides an overview of the flow data usability to detect security issue in these networks. The flow-based monitoring inside automation and control networks is a novel approach. In this paper, we describe several use cases in which flow monitoring provides information on network activities in building automation and control systems. We demonstrate a detection of Telnet brute force attacks, access control validation and targeted attacks on building automation system network.

Keywords: network, security, attack, intrusion detection, entropy, flow, BACnetFlow, BACnet, building, automation.

1 Introduction

Internet and public networks in general have become a wild place. We have to protect our networks and connected devices against viruses, worms and hackers trying to compromise them. However, the network security is not just about these networks. We are facing similar security threats in sensor networks, Building Automation and Control Systems (BACS) networks or in Supervisory Control And Data Acquisition (SCADA) networks. The majority of new buildings or industrial facilities include intelligent networks, that are capable of controlling and monitoring the building's mechanical and electrical equipment. Although ordinary network provides hacker with a higher number of possible targets, industrial and automation networks become more and more interesting for some attackers [1]. These types of networks represent an interesting environment especially for more targeted attacks with possible high impact on basic functions of a company or a society. This type of attack is predicted to grow significantly in the near future [2].

Besides increasing passive security of the systems and networks, we need to detect intrusions and other security threats to minimize possible damages. In comparison to ordinary IP networks, security of the automation networks is still

underestimated. With experiences from high-speed IP networks we believe that detailed information about what is exactly happening in the network is crucial for the BACS network security.

The more and more BACS networks are being moved to the Ethernet/IP networks. It makes them possible to be operated using the existing network infrastructure. Today's BACS devices feature command-line and browser-based control allowing them to be accessed from anywhere in the world. The flow-based network security monitoring in BACS networks is still in an early stage. In this context, this paper investigates several use cases, answering the following research question:

What are the advantages of flow-based monitoring in BACS networks and how can it help to detect security issue in these networks?

The paper is organized as follows: After a short introduction and related work, we describe the flow-based monitoring system for BACS networks. Then we describe entropy based anomaly detection and BACS targeted attacks. We present detected issues from large BACS network deployment. Finally, we conclude by summarizing impacts of flow data on BACS network security and propose future work.

2 Related Work

First ideas of using network traffic flow information for monitoring BACS (namely SCADA) networks appeared in [3]. However, this work and its results published in [4] rely on the traditional IP flow measurement. In our work, we focus on the specific BACS networks based on Building Automation and Control Networking protocol (BACnet) [5]. The original IP flow definition was modified to follow specifics of the BACnet and we introduced the BACnetFlow in [6]. This approach enables to retrieve more accurate information about BACS network traffic.

Flow-based monitoring was originally proposed exclusively for IP networks. There is an extensive work in the area of network traffic monitoring in common IP networks. Today BACnet networks are monitored only by a Deep Packet Inspection (DPI) or by Simple Network Management Protocol (SNMP) queries to the network devices. DPI is used for example by BACnet Firewall Router (BFR) [7]. SNMP statistics are used for example in [8] as supplementary information to the resource (CPU, memory, etc.) usage statistics retrieved from the monitored devices.

The security of the BACnet protocol was underestimated in the first protocol specifications. In 2003, Holmberg provided a report [9] on possible security threats to BACnet networks. Based on this document, American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) prepared BACnet security update in a form of the protocol specification addendum 135-2008g [10].

3 Building Automation and Control Systems

BACS refer to systems providing services to achieve human comfort and safety, energy and economy savings and last, but not least, security of the controlled building. They interconnect all involved systems to form an *intelligent building*. BACS are currently deployed mainly as a part of large functional buildings as hospitals, office buildings or university campuses.

BACS networks usually combine a LAN infrastructure with some industrial network protocols. This approach allows utilisation of existing network infrastructure to interconnect BACS components. Furthermore, IP-based network makes remote control and maintenance easier. On the other hand, it increases the security risks.

In this paper we focus on BACS networks based on the BACnet protocol, especially BACnet over Ethernet and BACnet over IP variants. BACnet is an ASHRAE, ANSI, and ISO standard protocol developed to address specific needs of BACS networks.

The BACnet network topology consists of isolated BACnet networks interconnected by BACnet routers. Device addressing in such environment is provided by a combination of the BACnet network address and the local device address, which is specific to the link layer medium. BACnet defines several messages to discover the network or to share BACnet routing information. BACnet represents BACS functionality of each device as a set of objects with a collection of properties storing status or configuration data. The properties are available for other devices via BACnet service messages to read/write data from/to the property.

3.1 Flow-based BACnet Network Monitoring

BACnet is able to utilise various protocols (Ethernet, IP, LonTalk, PTP) as its data link layer. However, current network traffic flow monitoring tools are limited to IP networks. Furthermore, even if IP is used as BACnet's data link layer, the BACnet messages are often broadcasted across the whole IP network and it is not possible to identify communication participants. To identify and describe network traffic flows related to the BACnet protocol, we introduced the BACnetFlow [6]. If the BACnet traffic is detected in the monitored Ethernet/IP network, BACnet headers are parsed and stored in BACnetFlow record. BACnetFlow record is depicted in Figure 1. In this paper we extended the original BACnetFlow record to support *Application Layer Protocol Data Unit* (APDU) data, e.g., BACnet services.

Our monitoring system is deployed at the Masaryk University Campus BACS network. The system passively observes network traffic passing through the main switches of the BACS network and its management servers. Another part of our monitoring system observes network traffic at the university network border. We generate and analyse non-sampled NetFlow and BACnetFlow statistics.

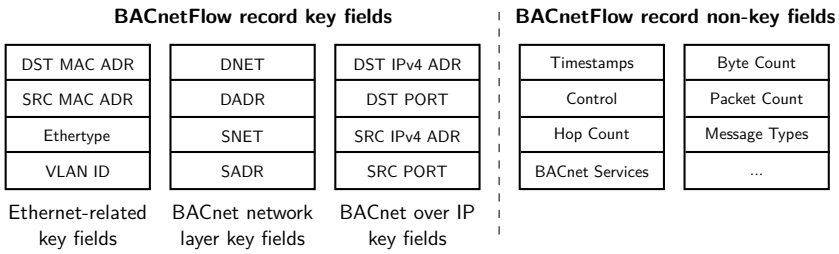

Fig. 1: BACnetFlow record consists of key fields extracted from the protocol headers and non-key fields with additional information.

4 BACS Anomaly Detection

There is a wide spectrum of flow based anomaly detection methods targeted to IP networks [11]. In this paper, we decided to compare simple volume based approaches to detection of network anomalies with an entropy based approach, providing another way how to analyse and disclose possible anomalies in network traffic. We applied this approach used in IP networks to the BACS networks environment.

Entropy represents a measure of the randomness of data. In this context, the term usually refers to the Shannon entropy [12], which quantifies the expected value of the information contained in a message, usually in units such as bits. Entropy $H(X)$ according to Shannon and used in our measurements is estimated as follows: Let's have an empirical histogram $X = \{n_i, i = 1, ..., N\}$ meaning that feature i occurs n_i times in the data. Then the entropy is defined as:

$$H(X) = -\sum_{i=1}^{N} \left(\frac{n_i}{S}\right) \cdot \log_2 \left(\frac{n_i}{S}\right) \tag{1}$$

where $S = \sum_{i=1}^{N} n_i$ is the total number of feature observations in the histogram.

5 BACnet Targeted Attacks

IP network is widely used as a backbone network that interconnects isolated BACnet networks. This backbone network can be the corporate LAN or even the Internet. BACnet traffic transported through the public networks can be an easy subject of eavesdropping or disruptions. To avoid this issue, the BACnet routers connecting BACnet network to the backbone network should add a security layer (VPN, IPsec, etc.) to the transported data.

Following list of threats presumes a physical break-in or a remotely accessible compromised device inside the BACnet network. BACnet provides addendum 135-2008g [10] to secure the protocol. These security extensions can prevent the

following attacks, originally described in [9]. However, the extensions are optional and not widely implemented and deployed.

BACnet spoofing is equivalent to the similar attack in Address Resolution Protocol (ARP) [13] or to an advertisement spoofing in IPv6 [14, sec. 4.1.1]. Compromised device generates BACnets' *I-Am-Router-To-Network* messages with the fake content and forces other devices to send their messages via the attacker's device. Furthermore, compromised device can claim to be any other device using the *I-Am* service messages.

Denial of Service attack by flooding the BACnet network. Attacker (repeatedly) broadcasts *Who-Is* service requests without specifying device instance range limits. Then, all devices across all available BACnet networks respond with the *I-Am* message and flood the network. Another approach is to broadcast a confirmed service request with the source address set to the network broadcast address. The receiving device will broadcast a response.

Write-Property attack changing present value of the BACnet object's property. Result of such action can vary according to meanings of the affected object and its property. It can cause switching off/on the equipment, allowing access into the restricted area or disrupting the whole BACS.

Disabling network connection can be done using several BACnet services. BACnet network routing tables can be broken by the compromised device which shares defective routing information. Furthermore, communication can be disrupted by fake *Router-Busy-To-Network* messages.

6 BACS Security Use-Cases

In this section, we evaluate detected issues to demonstrate the capabilities of flow-based monitoring in BACS network. The results are organized in three categories. First, we present remote attacks from BACnet over IP devices carried over Internet against Masaryk University network. The second category of results shows how the devices behave in BACS network with strict access control and how strict it is. Last, we look for attacks specific for the BACnet devices.

6.1 Intrusion Detection

Massive Telnet scans were detected against university computers on December 4th, 2011. Tracing back to a source, we have identified infected devices world wide. The first remote device we were able to analyse [15] was a Modular automation station with BACnet over IP and web server. Other infected devices ranged from firewalls, routers, modems, VoIP appliances to consumer electronics, including satellite receivers, IPTV boxes, etc. This confirmed utmost importance of network security monitoring of any network and any device.

The source of attacks was a new Aidra botnet. The Aidra botnet is an open source IRC-based mass router scanner/exploiter publicly available for download from Internet [16]. The novelty of this botnet lies in supporting multiple hardware platforms of vulnerable devices. Equivalent versions for six different

hardware architectures (ARM, MIPS, MIPSEL, PPC, SH4, x86) were observed until now. Aidra includes several types of scanners searching for other vulnerable devices using the Telnet protocol. According to attacker's commands, the bots are able to perform *Denial of Service* (DoS) attacks against specified targets. We noticed DoS attack against `www.whitehouse.gov`. Attacker is also able to execute any system command on infected devices. Aidra bots can be automatically upgraded and new functions can be added.

Figure 2 shows Telnet traffic observed on Tuesday 6th and Wednesday 7th December. We can see four graphs representing the Telnet traffic as the amount of *kilobits/s*, *packets/s*, *flows/s* and *entropy* of destination IP addresses.

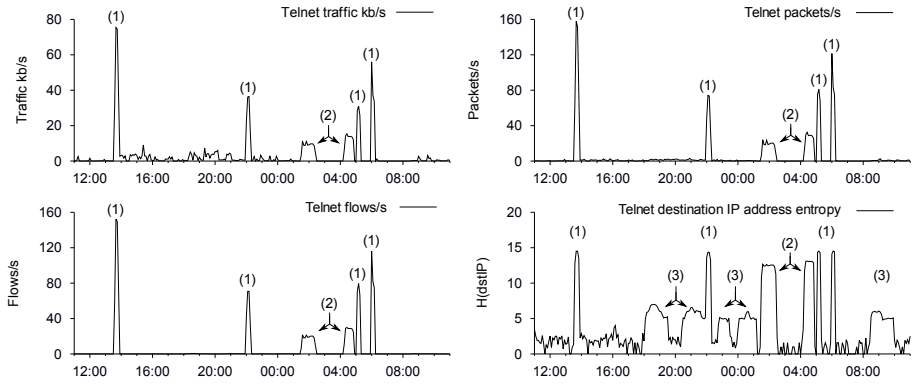

Fig. 2: Telnet attacks against Masaryk University network.

There is some basic level of a regular Telnet traffic observable all the time (very low amount, about 0 to 5 kb/s). Beside this, we can see three types of attacks using the Telnet protocol. The most significant attacks are marked as *(1)*, representing massive horizontal scans against B class subnet of campus network and probing all machines in this subnet for open Telnet ports. These attacks are very intensive, about 60 to 130 thousand flows and last only very short period, 15 minutes at maximum. Source of these attacks are Linux network devices (SYN packet size is 60 B) infected by Aidra botnet. We can notice attack spikes very well in all four graphs.

Second type *(2)* of attacks is similar – it is again a massive horizontal scan against B class subnet, caused by hosts infected by Aidra botnet. The difference is the intensity of the attacks – they are performed during longer time window (60 minutes). Again, we can notice them in all types of graphs, although the spikes in first three graphs are not so significant as in the graph with entropy.

Third type of Telnet attacks *(3)* represents a different class of attackers. In this case, the attackers are not infected devices like modems and routers, but ordinary computers with Microsoft Windows (SYN packet size is 48, 52 B). These attacks were performed with much slower rate, against C class subnet only.

Therefore, we are not able to notice them in the case of *traffic/packets/flows* graphs, where they are hidden inside regular traffic. The role of the *entropy* (destination IP address entropy) is crucial for revealing such kind of attacks. This measure is able to distinguish attack scans from regular traffic due to the different amount of randomness in the data. Therefore we can see clear spikes (marked as *(3)*) in last graph.

Beyond common botnets' activities, we identified mass Telnet scan from a large-scale embedded device vulnerability scanner[1] on November 14th, 2011. In that way Cui et al. [17] found over 540,000 publicly accessible devices, configured with factory default root passwords.

6.2 Access Control

The first task in securing any network is to ensure that unauthorised entities do not gain entry into the network. Most BACS networks are connected to the outside corporate/university network or the Internet through a gateway (see Figure 3). The previously held belief that the control networks are protected by an "air gap" is no longer true [18].

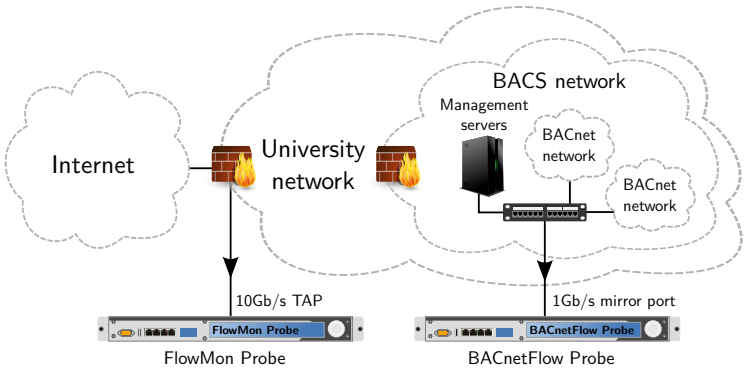

Fig. 3: University LAN infrastructure with dedicated BACS network. Deployed monitoring system provides flow information from *(a)* entire university network and *(b)* building automation and control systems network.

We present week-long access control validation results for the BACS network. Week-long statistics were chosen in order to take into account time-of-day and day-of-week variations. Figure 4 shows worldwide attempts to establish a connection to monitored BACS network. We use SURFmap [19], a network monitoring tool based on the Google Maps API, to visualize IP connections.

University Internet gateways have liberal access policies and the most traffic can pass through. We observed attempts to establish connections to hosts

[1] http://www.hacktory.cs.columbia.edu

Fig. 4: Worldwide attempts to establish a connection to BACS network.

in the address range of BACS network. Attackers' primary interests were following services - SSH(22), Telnet(23), HTTP(80), HTTPS(443), MS-SMB(445), MSSQL(1433), MSRDP(3389) and RADMIN(4899). All these unauthorized connections were denied by the BACS firewall and were not observed in the BACS network.

Table 1 shows foreign traffic observed inside BACS network. Incoming UDP and TCP connections are denied by default. ICMP messages are permitted. However, we did not observe any malicious or abnormal ICMP traffic.

PROTO	DIR	Bytes	Packets	Flows	DIR	Bytes	Packets	Flows
TCP		2217553	23122	323		15248736	33267	287
UDP	**In**	0	0	0	**Out**	2068299	27396	13113
ICMP		6812	100	96		4202	65	65

Table 1: Week-long remote communication statistics to/from BACS network.

We found out that the outgoing UDP traffic was caused by incorrectly set DNS servers. Some of the devices used preconfigured foreign or public DNS servers as Google Public DNS[2] (IP address 8.8.8.8).

Foreign TCP traffic was caused by the BACS management servers placed in "demilitarized zone" (DMZ). Some of these servers are allowed to establish remote connections, e.g., to download Microsoft Windows updates. Furthermore, we detected a feature called *Network Connectivity Status Indicator* (NCSI) [20] present in Windows Vista and later versions. This service enables network-interacting programs to change their behavior based on how the computer is

[2] http://code.google.com/speed/public-dns/

connected to the network. Windows machine tries to *(i)* download `http://www.msftncsi.com/ncsi.txt` file and *(ii)* resolve DNS name `dns.msftncsi.com`.

6.3 BACnet Attacks

We verified the occurrence of the security threats described in Section 5 in the Masaryk University Campus BACS network. To be able to detect BACnet targeted attacks we added support for the BACnet application data to the BACnetFlow record.

Firstly, we analyzed the presence of BACnet router spoofing attack. We selected flows with the *I-Am-Router-To-Network* and *I-Could-Be-Router-To-Network* messages. In that way we could filter out the traffic from the legitimate routers and detect spoofing device. We did not detect such rogue device in our network. Figure 5 shows the BACnet over IP routers announcing their routing capabilities every 30 minutes. This kind of automatically generated traffic is prevalent in BACS networks [4], but it is not the only type, as shown in Figures 6 and 7. The same approach can be used to detect fake *Router-Busy-To-Network* messages.

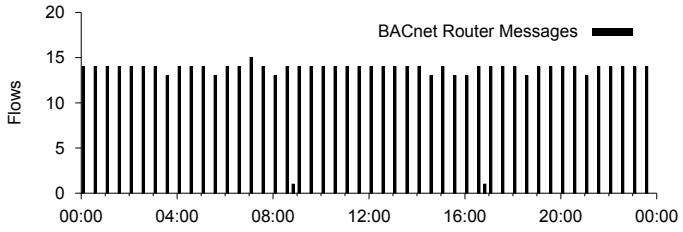

Fig. 5: BACnet over IP routers broadcasting *I-Am-Router-To-Network* and *I-Could-Be-Router-To-Network* messages to the campus BACS network.

Secondly, we analyzed the BACnet device discovery DoS attack. This attack is based on flooding the network by *I-Am* messages generated by *Who-Is* requests without limited device range. Figure 6a shows amount of *I-Am* responses related to the *Who-Is* requests. While level of the *Who-Is* requests is constant, there are several spikes of *I-Am* responses. In this case, they are caused by *Who-Is* requests broadcasted to all BACnet networks. However, all these requests contain device range limits so the *I-Am* responses are sent only by requested devices. DoS attack would generate even higher spikes of *I-Am* messages and would be seen in this type of graph even more clearly. We did not detect other kinds of BACnet flooding attacks that use broadcasted confirmed service requests without a source address.

Figure 6b shows *Who-Is*/*I-Am* statistics during one week. We observed diurnal pattern of the *I-Am* responses to *Who-Is* requests broadcasted to all net-

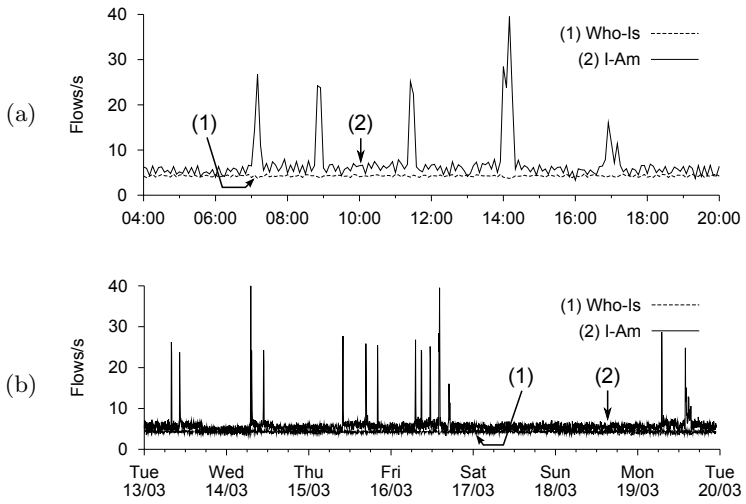

Fig. 6: BACnet device discovery - relation between *Who-Is* and *I-Am* messages during *(a)* a single day - March 16, 2012, *(b)* a week - March 13 - 20, 2012.

works during busy hours. This traffic is probably related to some operational staff activities in the university campus.

Thirdly, we analyzed the BACnet write-property attack. This attack uses *Write-Property* service to harmfully change any property, e.g. turn off/on equipment. Figure 7 shows the statistics of *Read-Property* and *Write-Property* services. We observed distinct diurnal and weekly pattern for *Read-Property* service. The *Write-Property* service does not exhibit a clear pattern. Figure 7a shows very low number of write flows. We observed between 1 and 2 long-pending flows exported every 5 minutes (flow cache active timeout). This corresponds to constant *Write-Property* traffic shown in Figure 7b. The write-property attack can even succeed by using only one or a few well-targeted packets. The design of a single flow/packet detection method is subject of our further research.

7 Summary

On the three use-cases described in Section 6, we demonstrated advantages of using flow monitoring to detect security threats in the BACnet network.

The first use-case reported on Aidra botnet infected devices. Beyond standard small office/home office (SoHo) devices we detected foreign BACnet over IP devices scanning entire university network. There does not exist an anti-virus or an anti-malware for these devices. Most users would not suspect that any embedded device can threaten their computers. Flow information is essential to reveal such rogue activities.

The second use-case showed how the BACS gateway prevents unauthorised access to automation and control devices. BACS firewall misconfiguration can

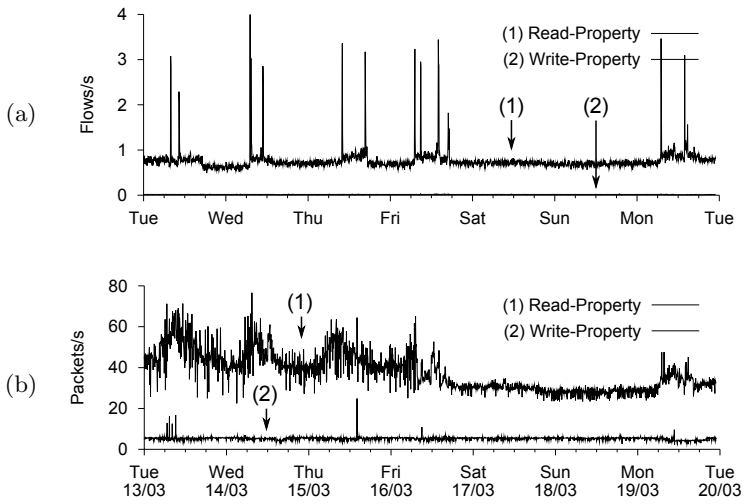

Fig. 7: BACnet data sharing - *Read-Property* and *Write-Property* services.

facilitate an attack against BACnet devices as mentioned in the first use-case (publicly accessible BACnet devices using default credentials). We presented extrusion detection results using the flow representation of outbound traffic to highlight this security threat.

The third use-case showed a novel approach to detection of BACnet targetted attacks. We added support for BACnet application data into the BACnetFlow to be able to detect these attacks. We analyzed the traffic to detect router spoofing attack, device discovery DoS attack and application service attack. According to our best knowledge, we provided the first flow-based detection results for BACnet targetted attacks.

As future work, we intend to extend our detection towards a malfunction and a security misconfiguration detection of BACnet devices. We consider to investigate the attacks launched from within the BACS network and trusted internal networks.

Acknowledgments. This material is based upon work supported by the Czech Ministry of Defence under Contract No. SMO02008PR980-OVMASUN200801 and also supported by the "CESNET Large Infrastructure" project LM2010005 funded by the Ministry of Education, Youth and Sports of the Czech Republic.

References

1. Byres, E., Lowe, J.: The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems. In: Proceedings of the VDE Congress (2004).
2. Security Predictions 2012&2013 – The Emerging Security Threat, `http://www.sans.edu/research/security-laboratory/article/security-predict2011`

3. Barbosa, R.R.R., Pras, A.: Intrusion detection in SCADA networks. In Proceedings of conference on Autonomous Infrastructure, Management and Security (2010).
4. Barbosa, R.R.R., Sadre, R., Pras, A.: Difficulties in Modeling SCADA Traffic: A Comparative Analysis. In Proceedings of PAM Conference (2012).
5. American Society of Heating, Refrigerating and Air-Conditioning Engineers: Standard 135-2010 – BACnet A Data Communication Protocol for Building Automation and Control Networks. ASHRAE (2010).
6. Krejčí, R., Čeleda, P., Dobrovolný, J.: Traffic Measurement and Analysis of Building Automation and Control Networks. In Proceedings of conference on Autonomous Infrastructure, Management and Security (2012).
7. Holmberg, D. G., Bender, J., Galler, M.: Using the BACnet Firewall Router. http://www.bacnet.org/Bibliography/BACnet-Today-06/28884-Holmberg.pdf
8. Yang, D., Usynin, A., Hines, J. W.: Anomaly-Based Intrusion Detection for SCADA Systems, in Proc. of 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (2006).
9. Holmberg, D. G.: BACnet wide area network security threat assessment, U.S. Dept. of Commerce, National Institute of Standards and Technology (2003), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=860911.
10. ANSI/ASHRAE: Addendum g to BACnet Standard 135-2008, http://www.bacnet.org/Addenda/Add-135-2008g.pdf
11. Sperotto, A., Schaffrath, G.,Sadre, R., Morariu, C., Pras, A., Stiller, B.: An Overview of IP Flow-based Intrusion Detection. In: IEEE Communications Surveys & Tutorials, 12 (3). pp. 343-356.
12. Shannon, C.E.: A Mathematical Theory of Communication. In: Bell System Technical Journal, vol. 27, pp. 379423, 623-656, July, October, 1948.
13. Whalen, S.: An Introduction to ARP Spoofing (2001), http://www.rootsecure.net/content/downloads/pdf/arp_spoofing_intro.pdf.
14. Nikander, P., Kempf, J., Nordmark, E.: IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756 (Informational), IETF (2004), http://tools.ietf.org/html/rfc3756.
15. Čeleda, P., Krejčí, R., Krmíček, V.: Revealing and Analysing Modem Malware. In Proceedings of the IEEE International Conference on Communications (2012).
16. Fazzi, F.: Lightaidra – IRC-based mass router scanner/exploiter. http://packetstormsecurity.org/files/109244.
17. Cui, A., Stolfo, S.: A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan. In Proceedings of the 26th Annual Computer Security Applications Conference (2010).
18. Byres, E.: #1 ICS and SCADA Security Myth: Protection by Air Gap. Tofino Security, http://www.tofinosecurity.com/blog/1-ics-and-scada-security-myth-protection-air-gap.
19. Hofstede, R., Fioreze, T.: SURFmap: A Network Monitoring Tool Based on the Google Maps API. In Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (2009).
20. Microsoft Corporation: Network Connectivity Status Indicator. http://technet.microsoft.com/en-us/library/cc766017%28WS.10%29.aspx.