Advancing the Micro-CI Testbed for IoT Cyber-Security Research and Education

Conference Paper · February 2017

CITATIONS
0

READS
10

6 authors, including:

William Hurst
Liverpool John Moores University
41 PUBLICATIONS **68** CITATIONS
SEE PROFILE

Nathan Shone
Liverpool John Moores University
13 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Ben Kotze
Central University of Technology
4 PUBLICATIONS **1** CITATION
SEE PROFILE

Bob Duncan
University of Aberdeen
25 PUBLICATIONS **99** CITATIONS
SEE PROFILE

Advancing the Micro-CI Testbed for IoT Cyber-Security Research and Education

William Hurst, Nathan Shone & Abdennour El Rhalibi,
Department of Computer Science
Liverpool John Moores University
Byrom Street
Liverpool, L3 3AF, UK
{W.Hurst, N.Shone, A.Elrhalibi}@ljmu.ac.uk

Andreas Happe
AIT Austrian Institute of Technology,
Austria
andreas.happe@ait.ac.at

Ben Kotze
Department of Electrical, Electronic and Computer Engineering,
Central University of Technology, Free State,
South Africa
bkotze@cut.ac.za

Bob Duncan
Computer Science
University of Aberdeen
Aberdeen, UK
Email:
bobduncan@abdn.ac.uk

***Abstract*— Physical testbeds offer the ability to test out cyber-security practices, which may be dangerous to implement in a real-life scenario. They also provide a means to educate students and researchers on effective cyber-defence practices. However, the majority of existing non-virtualised physical testbeds are costly, inaccessible, and are often location constrained. As such, modern education and research for control system security is becoming increasingly reliant on virtualised labs and tools. Any learning or research undertaken using these tools, however, is based around the limitations and characteristics of such tools, as well as any assumptions made by their developers. Virtual testbeds are not perfect. Additionally, the accuracy of data resulting from emulations and models may be further decreased if used outside of their intended usage scenario. As such, this paper presents a discussion on the effectiveness of physical testbeds over simulation approaches. In addition, an approach for the design and construction of a replicable, cost-effective testbed for cyber-security education and training is presented.**

Keywords—Testbed, Cyber-Security, Education

I. INTRODUCTION

Simulation-based testbeds are used to construct data for cyber-security experimentation, testing and education purposes [1]. A virtualised approach offers significant cost savings and a self-paced and active approach to learning. However, it has several key limitations including: no hands-on experience, no real-world training with specific equipment and no experience in identifying and interpreting incorrect or uncharacteristic data. Simulation is effective at representing '*correct'* behaviour. However, critical infrastructure systems need to be protected against situations where they are exposed to extreme abnormal events. Unfortunately, in such circumstances, systems do not always behave in the way expected or respond in the same consistent manner. Similarly, it is therefore difficult to accurately model how a system's erratic behaviour might cascade and impact other parts of the infrastructure.

Additionally, a simulation testbed approach is constructed through the developer's mental model of how the system functions. In result, the data generated is constructed. Whereas, in a physical approach, data is, instead, captured. This can be for example, communication, control and physical system characteristics in a unified environment [2]. Both simulation data and captured data are used for research purposes [3]. Captured, also known as observational data, is generally irreplaceable and tends to offer further realistic analysis over simulation approaches. Yet, simulation is mainly used, as testing in '*real*' scenarios has the potential to impact human well-being [4]. For that reason, testbed projects are often presented to bridge the cyber-physical divide and offer a safe environment for cyber-security testing and training [5]. However, many existing approaches, as outlined in the related research section, are either costly, not-replicable or involve an element of simulation in their design.

The research presented in this paper provides an ideal solution. The practical element involved in the Micro-CI project introduces a level of realism that is difficult to match through simulation alone. As such, this project provides innovative research opportunities for the testing and development of security enhancements in a real-life scenario. This is evaluated through a cyber-attack case study, to demonstrate the capability to construct different data set types. As such, the aim of the research is to have a practical output; a fully working critical infrastructure testbed named Micro-CI. The goal is to demonstrate the suitability of the datasets generated by the Micro-CI testbed for the following advantages.

- Pedagogical benefits: Research has shown that practical learning opportunities are vital to students becoming comfortable with cyber-security concepts. In addition, users will learn the functioning of infrastructures and their security systems through reverse engineering. A lack of experience produces immaturity for systems understanding, in an era where cyber-security experts are in high demand [6];
- Cost effectiveness: Project has been designed to be as cost effective as possible. We estimate that at the time of writing the paper, replicating the experiments can be achieved for under £100;
- Portability and Dataset: As the project components are on a miniaturised bench-top scale, it enables them to be packed away, stored and transported with ease. Projects can still be moved and/or stored whilst partially assembled. We envision that the testbed can be purchased

and assembled by other researchers in the future. In addition, as outlined later in the paper, the amount of real data which can be generated in a relatively short time period offers advantages over larger testbed constructions.

The remainder of this paper is organised as follows. Section 2 presents an insight into the motivation behind this work and a discussion on related projects. Section 3 details the approach taken for the Micro-CI testbed development. Section 4 presents an evaluation and the paper is concluded in Section 5.

II. BACKGROUND

Internet of Things (IoT) is growing as a new model for the expansion of the Internet, and can be held as the next revolution in distributed systems and pervasive computing technologies. It is predicted that in the next decade, it will transform everything in people's everyday lives due its major influence on so many areas of the industry: critical infrastructure, education, healthcare, city management, business, innovation, community, cultural heritage and many more. In this new emerging technology, IoT would be effortlessly assimilated within data science infrastructures, producing data and generating knowledge. Traditionally, data was stored upon few centralised hosts. All connections to them were protected by perimeter security, connected clients themselves were input/output devices with very limited capabilities. Security mostly focused upon the few centralised components.

A. *The Cyber-Threat*

As technology moved onwards, things became decentralised. Desktop computers, with their myriad of installed software systems and applications, and often lacking professional administrative care, became a new battle ground. In hindsight, this was an evolutionary step that led to even more decentralised networks; the current manifestation being the internet of things (IoT) and connected industrial control systems (ICS). Initially, these were attacked too, e.g., Stuxnet [15] or reports of attacks against honeypots posing as nuclear power plants. However, recently, they have also become weapons that endanger other systems too – they are now commonly part of large distributed high-bandwidth distributed denial of service (DDoS) attack botnets [16]. There's an abundance of insecure IoT and ICS devices, fitting to a common cloud-theme. For example, one can currently buy a botnet-as-a-sevice for around $7500 for a 100000 device botnet.

While decentralisation is still the best hope in the face of state-based offensive actors, its security implications still need further analysis. With the rise of desktop computers, attackers started to pivot between captured desktops, utilising retrieved credentials to move between networks and gain further data. To prevent these attacks, security on and between desktops was improved. Personal firewalls and malware detection tools were deployed on desktops; network segregation and traffic scanning was performed between them. This reduced the available attack surface.

IoT and ICS now introduce even more communication paths, while the IoT/ICS devices themselves are sometimes lacking resources for essential security tasks. This allows attackers to traverse more freely between devices while the devices themselves are worse protected when compared to traditional computers and servers. The latter is not just due to reduced performance; IoT devices employ different hardware architectures, some of the most commonly used architectures lack hardware support for basic hardware security techniques such as memory protection. This is related to the monetary and power consumption related requirements. While desktop computers are always connected to a power outlet and may (now) cost a substantial amount of money, IoT devices are power limited or run on battery-power and must not cost more than a couple of dollars. Power utilisation might be of higher importance than security.

Another distinction is their usage pattern. Desktops are personal computers, named due to their direct usage through human users. IoT/ICS devices are often not directly monitored by users. While security problems can ultimately be of the highest consequences, they might not be detected immediately. Even if faults are detected, end users might not have the means of easily updating those systems. While a desktop computer is built by commodity hardware and runs (mostly) standard software, IoT and ICS devices are often build for a special purpose and employ special software. If the vendor ceases product support, the device will gain additional security problems that might not be solvable over time.

Educational material must adapt to this new reality. In particular, they should focus on the distributed nature of deployed systems and not on a single high-value target. The interaction between the control system and distributed "*cheap*" and insecure sensors should be part of any testbed. Simulation of update mechanisms and transport mechanisms that are not standard Ethernet cables should be included to resemble the real world. We fear, that without an adequate testbed the next generation of defensive IT professionals will have an even harder task as the current generation already has.

The growing cyber-threat has led to a switch in research focus from physical protection to digital infrastructure security measures. However, this cyber-security research is hampered by a lack of realistic experimental data and opportunities to test new theories in a real-world environment.

B. *Related Projects*

For that reason, projects such as SCADAVT, have developed simulation-based testbeds, which builds upon the CORE emulator, for building realistic SCADA models [7]. In their approach, Almalawi *et al.*, develop a framework to construct a water distribution system [7]. The testbed consists of SCADA components, including the Modbus/TPC slave and master, and the Modbus/TPC HNI server. Functioning together, the testbed employs the use of the dynamic link library (DLL) of EPANET to simulate the water flow within the system. The testbed combines the use of existing techniques to produce a novel testbed application. The system

tested through a case study involving a DDoS attack to demonstrate that convincing data-construction is possible. Software-based simulation data, such as this approach, is often used to test theoretical cyber-security systems; however, the data is constructed through emulators.

Examples of simulation approaches include a SCADA-testbed constructed using TrueTime, and Matblab Simulink. In their research, Farooqui *et al*., discuss the effectiveness of TrueTime, which is used for simulating controller task network transmissions and continuous plant dynamics [8]. To evaluate their testbed, two varied DoS attack scenarios are conducted. The first is an attack on the PID Controllers, the second involves the generation of false control signals for a specific actuator node. Whilst, the research is noteworthy, in that TrueTime can be used to model network data to a detailed level. This means that a close evaluation of the effects of 2 different DoS attacks can be understood when affecting the normal system behaviour. There is, however, no comparison with a physical application presented. Meaning that, the mental model of the researchers is being evaluated.

PentesterLab, is an online tool for educating users on exploiting SQL injections in a PHP-based website [9]. The idea is to educate how the technique can be used for gaining access to administration pages. Unlike the above simulation approaches, PentesterLabs, has a focus on education and teaching about the techniques used to implement an attack. Whilst beneficial for an attack, there is a limited realism as the application is set to a predefined attack scenario.

Other projects do recognise the need to integrate physical components into testbed developments. For example, Van Leeuwen *et al*., propose a methodology, which is a hybrid testbed combining real and simulated components [10]. The idea, much like the research presented in this paper, is to develop a testbed, which is transportable and functions on a single unified-platform. The main challenge faced by the hybrid approach, as detailed, is that the simulated components must be able to cope with the real-time functionality of the physical components. To compensate for this, estimation algorithms are implemented in order to support the real-time functionality of the simulation.

This type of approach is referred to as cyber-physical, where an amalgamation of both simulation tools and physical components are merged to develop a testbed. One of the more advanced cyber-physical-based testbeds is detailed by Siaterlis *et al*., who present an emulation-capable testbed construction termed EPIC [11]. The testbed is able to recreate the cyber-part of interconnected critical infrastructures and makes use of multiple software simulators to represent physical components. The testbed demonstrates effective results under cyber-security experimentation. However, the technical construction of the testbed means that it would not be an ideal tool for pedagogical use and the replicability would be unfeasible.

Physical testbed constructions are common place, but often are bespoke and expensive to recreate. Heracleous *et al*., for example, detail the design and construction of a critical infrastructure testbed, which is able to emulate the operation and faults commonly found in a water supply system, such as leaks or pump and value faults [12]. Specifically, the testbed emulates a small-scale version of a city water supply system. The system, makes use of tanks, pipes, pumps and valves to process the water. A SCADA system is in place to act as the control system software. However, whilst the testbed is an effective achievement, the large-scale implementation of the device, with for example 15000 m3 tanks in place, means that replicability costs would be high and not accessible to the average researcher. The nature of the testbed also means that it is confined to one critical infrastructure type and is not adaptable to additional critical infrastructure varieties or indeed capable of experiments on networked critical infrastructures.

C. Discussion

To summarise, by using simulation-based techniques, a hands-on learning experience is missed. This can be an integral experience for understanding effective cyber-security practices and techniques. It also means that the development of new and innovative cyber defence systems are tested against mental models as opposed to a real-world scenario. In addition, the background research presented above, has also led us to believe, that while effective physical testbeds are in existence, there is limited access and replicability for researchers and students. As such, we consider also the following main challenges related to cyber-security education.

- Traditional school education is limited, even security certifications are seldom hands-on. While applicable for managerial roles, this is not sufficient for technical personnel;
- Traditional virtual machine-based labs focus upon single high-value targets. This does not resemble the IoT with its multitude of connected devices. Some labs, e.g., Offensive Security Certified Professional (OSCP), do offer advanced functions in this pivotal area, but they mostly focusing upon segregated networks;
- Traditional protection techniques are not 100% fitting for IoT. Hardware architectures sometimes lack basic hardware requirements for security techniques, e.g., IoT CPUs often lack a Memory Management Unit (MMU) and thus cannot perform memory protection. Power usage is more important than security;
- Typical web-application centric testbeds do focus on web-application technologies. Within IoT and ICS there is a development back to insecure technologies like telnet, etc.;
- IoT and ICS have the same update problem as mobile devices. For example, the process for automatically installing updates. These update procedures can be attacked by offensive actors.

As such, in the following section, our approach is put forward for the development of a hackable and replicable testbed for cyber-security training and education.

III. APPROACH

The testbed will be developed based on the Semantic sensor networks (SSN) [17], which was proposed by the W3C semantic sensor network incubator group (SSN-XG) [18], to describe and discover IoT devices and their data.

A. Previous Implementation

In our past work, we presented the design of a rudimentary water distribution plant testbed [13]. As illustrated in Figure 1, there are two reservoir tanks, which are fed by two pumps moving water from external sources. The remote terminal unit is used to monitor the outgoing flow rate and water level, to dynamically adjust the pump speed ensuring adequate replenishment of the reservoir tanks. However, vulnerabilities exist in the system, meaning that it is possible for an external source to cut off the water supply or flood the reservoir tanks.

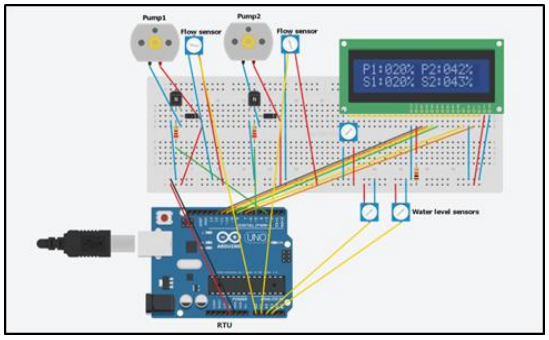

Figure 1. Physical wiring schematics

This can be achieved by switching off or speeding up either of the pumps used to control the water flow. The practical implementation of the testbed includes the following physical components: an Arduino Uno Rev. 3 as the RTU, two 12v peristaltic pumps as the water pumps, two liquid flow meters, two water level sensors, two amplification transistors, diodes, resistors and an LCD. In the schematics shown in Figure 1, potentiometer symbols have been used in place of sensors; this is due to the limited symbols available in the blueprint software. As the maximum output of the Arduino is only 5v, transistors amplify this to the 12v required by the pumps. Lastly, the diodes are used to ensure the current can only travel in one direction, thus preventing damage to the Arduino.

The hardware specification used is modest, meaning there is scope for future expansion; yet is sufficient in size to produce realistic infrastructure behaviour datasets for research purposes. The construction is displayed in Figure 2. For the purpose of this experiment, the Arduino board remains connected to a PC via a USB cable (although this could be replaced with a network connection for similar experiments). The system is also inactive. Through this USB connection, a serial connection is established to supply a real-time data feed, which is recorded and preserved by the PC (as illustrated in Figure 2).

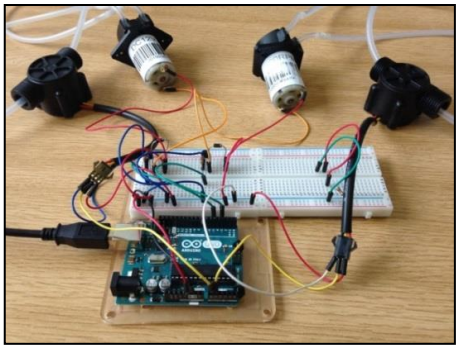

Figure 2. Testbed Construction

The metrics collected in this instance include: Water level sensor1/2 readings, Flow meter1/2 readings and Pump1/2 speeds. These readings are taken from each sensor every 0.25 seconds (4Hz) and written to the serial data stream.

B. Implementation

The above testbed can be used for simple data collection, which in turn can be used to understand simple cyber-attack behaviours, such as Distributed Denial of Service (DDoS) attacks [14]. However, to advance this, the testbed must be open to penetration testing experimentation and further realistic attack scenario creation. To achieve this, we incorporated an Internet of Things approach. Specifically, the testbed was made Internet-ready with the integration of a webpage which allows for the control of the individual device components. The framework layout is presented in Figure 3.

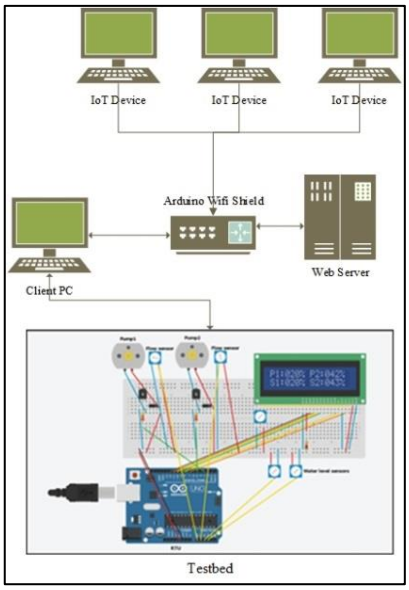

Figure 3. IoT Framework

To begin with, a webpage, which can be used to control a light on the Arduino board and a basic HTML page with buttons to turn it on an off was set up. This enables the possibility to add pumps/flow controls/etc. and control them

through the web page. Other IoT devices can connect to the webserver through the Arduino Ethernet shield, which is where security and penetration testing can take place. The Arduino Ethernet shield provides access to the web server and the testbed. The Client PC displays the control screen for the testbed. Figure 4 displays the IoT setup, where the phone in the middle (which can also be replaced with a raspberry pi instead) represents the web server (1) and it is accessed through the Arduino's wifi shield (2). The laptop and second phone (3) represent other IoT devices which can connect to the webserver, if given the correct IP address. At this stage it becomes possible to integrate security, firewall and intrusion detection systems to identify unauthorised access of the web page.

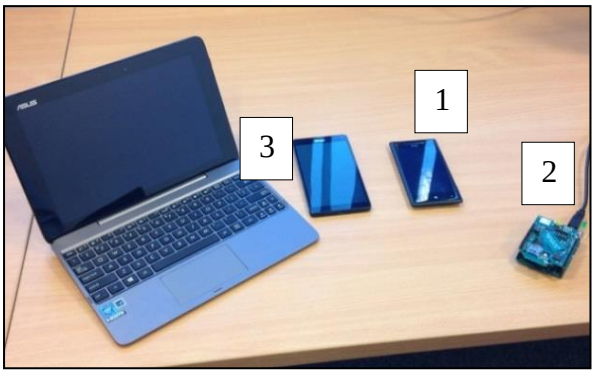

Figure 4. Testbed Extension

Specifically, the proposed system focuses on a water distribution plant; however, the design is extendable and testbeds can be extended to incorporate other infrastructure types, such as an ecologically-aware power plant.

IV. EVALUATION

This testbed is evaluated through the demonstration of a Distributed Denial of Service attack.

A. Test Case Scenario

The metrics collected in this instance include: Water level sensor1/2 readings, Flow meter1/2 readings and Pump1/2 speeds. These readings are taken from each sensor every 0.25 seconds (4Hz) and written to the serial data stream.

To examine the quality of the data produced by the Micro-CI implementation, a dataset was recorded over the period of 1 hour. During this time, the testbed was operating under normal parameters (i.e. no cyber-attacks were present). Essentially, this means that the pump speeds are configured to slowly continue filling the tanks at a controlled speed until full (even if no water is being used) and to cover the current rate of water consumption (if possible). The outflow (water being consumed) is a randomly applied value within a specific range (to make usage patterns more realistic). In this instance, the water source pipe is 60% smaller than the outflow pipe, which allows for a more accurate representation of overflow.

The initial configuration of the testbed was as follows: Tank1 is 65% full, Tank2 is 69.9% full, Outflow1 is functioning at 20 + (1-35)% of capacity and Outflow 2 is operating at 30 + (1-35)% of capacity. A small sample of the data obtained at 00:10.5 of run time is shown in Table 1. From this dataset, we can see that there is no significant variation present in the data. We can also see that all the metrics maintain consistent trends in operation.

TABLE 1 – PHYSICAL TESTBED DATA SAMPLE (%)

Sample (*t*)	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**
00:10.5	65.0	69.9	47.3	55.4	81.9	85.1
00:10.7	65.0	69.9	39.4	48.5	74.1	78.8
00:11.0	65.0	69.9	39.4	53.4	74.1	83.1
00:11.2	65.0	69.9	33.6	50.5	69.0	81.1
00:11.5	65.0	69.9	41.4	39.7	76.0	70.2

Components:

- P1 - Water Level 1 - this depicts the water level in tank one.
- P2 - Water Level 2 - this depicts the water level in tank two.
- P3 - Water Flow 1 - this refers to the flow rate through pipe one.
- P4 - Water Flow 2 - this refers to the flow rate through pipe two.
- P5 - Pump Speed 1 - this is the operating speed of pump one which controls the flow of water from tank one.
- P6 - Pump Speed 2 - this is the operating speed of pump two which controls the flow of water from tank two.

For this case study, data for the water distribution plant is recorded whilst operating under normal conditions. This allows for the building of a behavioural norm profile for the system, in order to identify anomalies. Within the testbed, during the DDoS attack, only intermittent readings from the sensors are received, forcing it to make drastic (and therefore uncharacteristic) changes to the pump speeds, rather than gradual as when operating as normal. In this cyber-attack dataset, a DDoS attack is launched against the RTU's communications channel, so it is only able to get sensor readings intermittently. Whilst no new values are readily available, the RTU will continue to maintain the previous pump speed.

In Figure 5, the components are displayed along the x-axis, with labels 1 to 6. The y-axis displays the operating capacity of the component. The exact behaviour induced by this experiment was relatively unknown. The results obtained showed that one tank kept filling whilst the other maintained the same level. As such, Figure 5 displays box plots of the distribution values for the testbed data for normal behaviour.

Figure 6 displays the alteration in data when in a cyber-attack scenario. The change in behaviour, as a result of the attack, can be seen in the average value changes in the datasets, as previously for the simulation dataset. Particularly a change in the output for P5 is visually apparent.

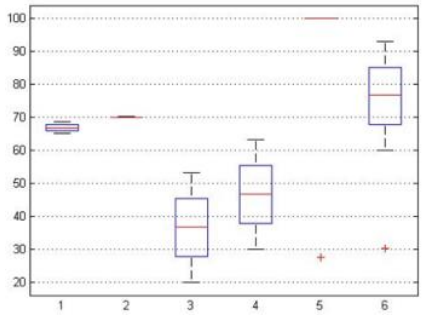

Figure 5. Distribution values for Testbed Normal Data Plot

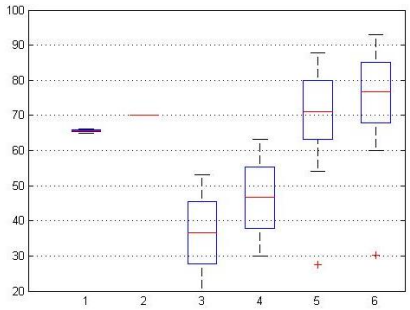

Figure 6. Distribution values for Cyber-Attack Data Plot

The data constructed during normal operation and under cyber-attack is used to assess the potential of the data to be used for cyber-security training and research. The data is evaluated using data classification techniques to identify the nature and timing of the conducted cyber-attacks.

V. CONCLUSION AND FUTURE WORK

One of the most effective aspects of the Micro-CI testbed, as demonstrated in this paper, is its expandability. This means the scale of the testbed can be expanded to incorporate additional components and sensors. One of the aims of this project is to devise a testbed, which is suitable for cyber-security training and research. It is our belief that the use of real-life data is more suitable for cyber-security research, than that of simulation only. However, as with all solutions, there are some drawbacks to our approach. The first is that the use of low cost hardware reduces the level of accuracy that can be achieved. For example, the Arduino Uno uses an ATMega microcontroller, which is only capable of recording 4-byte precision in double values. This can present problems if precision is a crucial part of the research being undertaken. This can be mitigated by purchasing more expensive hardware. Another limitation is that in comparison to simulation software, the practical approach may require a greater level of improvement to students' skillsets (which is not a detrimental attribute), and a longer initial construction time, to accomplish a working implementation.

REFERENCES

[1] S. Badri., P. Fergus., and W. Hurst., Critical infrastructure automated immuno-response system (CIAIRS), In Proceedings of the IEEE International Conference on Control, Decision and Information Technologies, 2016

[2] A. Ashok., P. Wang., M. Brown., and M. Govindarasu., Experimental evaluation of cyber-attacks on Automatic Generation Control using a CPS Security Testbed, In Proceedings of the IEEE Society General Meeting on Power & Energy, 2015

[3] Boston University Libraries, Research Data Management, What is 'Research Data'?, reference, available at [http://www.bu.edu/datamanagement/background/whatisdata/], access 08/12/2016

[4] G. Bernieri., F. Del Moro., L. Faramondi., and F. Pascucci., A testbed for integrated fault diagnosis and cyber security investigation, In Proceedings of the IEEE International Conference on Control, Decision and Information Technologies, 2016

[5] P. Singh., S. Garg., V. Kumar., and Z. Saquib, A testbed for SCADA cyber security and intrusion detection, In Proceedings of the IEEE Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, 2015

[6] B. Somekh., C. Lewin., D. Saxon., D. Woodrow., et al., Evaluation of the DfES ICT Test Bed Project, The Qualitative Report, Coventry: Becta, 2007

[7] A. Almalawi., Z. Tari., I. Khalil., and A., Fahad, SCADAVT-A framework for SCADA security testbed based on virtualization technology, In Proceedings of th 38th IEEE Conference on Local Computer Networks, 2013

[8] A. A Farooqui., S. S. Haider Zaidi., A. Y Memon., and S. Qazi., Cyber Security Backdrop: A SCADA testbed, In Proceedings of the IEEE Computing, Communications and IT Applications Conference, 2014

[9] PentesterLab, available at [https://pentesterlab.com/] accessed 08/12/2016.

[10] B. Van Leeuwen., V. Urias., J. Eldridge., C. Villamarin., and R. Olsberg, In Proceedings of the IEEE International Carnahan Conference on Security Technology, 2010

[11] C. Siaterlis., B. Genge., and M. Hohenadel., EPIC: A Testbed for Scientifically Rigorous Cyber-Physical Security Experimentation., IEEE Transactions of Emergining Topics in Computing, 2014

[12] C. Heracleous., E. E. Miciolino., R. Setola., F. Pascucci., D. G. Eliades., G. Ellinas., C. G. Panayiotou., and M. M. Polycarpou., Critical Infrastructure Online Fault Detection: Application in Water Supply Systems, In Proceedings of the Springer Journal on Critical Information Infrastructures Security, vol 8985, pp 94-106

[13] W. Hurst., N. Shone., Q. Shi., and B. Bazli., Micro-CI: A Critical Systems Testbed for Cyber- Security Research, In Proceedings of The Eighth International Conference on Emerging Networks and Systems Intelligence, At Venice, Italy, Volume: Special Session on Big Data Analytics in Critical Systems (BDA-CS), 2016

[14] K. Alieyan., M. M. Kadhum., M. Anbar., and S. Ul Rehman., et al., An overview of DDoS attacks based on DNS, In Proceedings of the IEEE International Conference on Information and Communication Technology Convergence, 2016.

[15] Bill Miller and Dale Rowe. A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual conference on Research in information technology (RIIT '12). ACM, New York, NY, USA, 51-56, 2012.

[16] Marjan Kuchaki Rafsanjani and Neda Kazeminejad. Distributed denial of service attacks and detection mechanisms. J. Comp. Methods in Sci. and Eng. 14, 6, 329-345, 2014.

[17] Compton M et al., The SSN ontology of the W3C semantic sensor network incubator group, Web semantics: science, services and agents on the World Wide Web, vol 17. Elsevier, London, 2012

[18] Semantic Sensor Network Incubator Group. https://www.w3.org/2005/Incubator/ssn/. Retrieved Dec 2016