Securing Networks of IoT Devices With Digital Twins and Automated Adversary Emulation

1st Ewout Willem van der Wal
CS Student
Twente University
Enschede, Netherlands
e.w.vanderwal@student.utwente.nl

2nd Mohammed El-Hajj
EEMCS (SCS)
Twente University
Enschede, Netherlands
m.elhajj@utwente.nl

***Abstract*—With the number of Internet-connected devices (things), expected to be almost 30 billion by 2030, the Internet of Things (IoT) technologies already became a part of everyday life, various areas like public health, smart cars, smart grids, smart cities, smart manufacturing and smart homes. On the other hand there is also the necessity of securing all these devices from possible cyber-attacks. In this paper, We investigate the current state of the art of IoT security and Digital Twins, digital representations of physical objects. We then use this knowledge to propose a novel methodology to use Cyber Digital Twins and Autonomous Adversary Emulation to improve the security of IoT devices. Consequently, we show that this methodology has the potential to improve the security of IoT applications. This work contributes a review of the state of the art in IoT security research and a novel method for improving IoT device security.**

***Index Terms*—IoT, Digital Twins, Security,Autonomous Adversary Emulation , DT.**

I. Introduction

Advancements in sensor, microprocessor, and battery technology in recent years has given rise to small, low-powered devices that can be used to collect information about the physical world [1], [2]. Due to their relatively low cost and small form factor, these sensing devices can be embedded into objects ranging from buildings, shipping containers, and infrastructure [3]. Connecting these devices together over wireless communication creates the Internet of Things (IoT), the term was initially coined by Kevin Ashton in 1999 when he proposed linked RFID enabled devices to the internet for Proctor and Gamble [4]. The technology has applications in many different fields, such as logistics tracking, environmental monitoring, theft prevention (a recent example being the Apple AirTag [5]), and patient monitoring in a medical context [6]. As an emerging technology, IoT has to deal with a number of growing pains [7], [8]. The management of the big data coming from the sensor equipment poses new networking and data science challenges, and optimizing software to work on low-power, battery restrained devices is being actively worked on with the benefit of Blockchain technologies [9]. Another problem that research has identified is the security of the IoT devices, as well as the security of the data moving between these devices. Due to the low-power nature of many IoT sensor nodes, traditional security techniques no longer work effectively [10], and issues such as communications happening without proper encryption or authentication are being documented in the existing literature. Another, quite insidious, issue is the large scale data collection that is enabled by these devices. Previous research has shown that an attacker may be able to infer private or sensitive information from seemingly innocuous sensor data [11].

The goal of this research is to improve the privacy and security of the data that is being collected and used in IoT applications. One area of research that shows promise in the field of IoT is Digital Twins (DTs), and we will be focusing our research on exploring what these are and how they can be utilised in improving the data security and privacy of IoT applications. The main contribution of this work is a proof of concept for a method to perform automated penetration testing on a Cyber Digital Twin of an IoT device. We show that it is possible to create automated attack patterns against weaknesses in the software configurations on the Cyber Digital Twin. We also present several directions for further research into using this method to improve automated security testing on IoT devices. The rest of this paper will be structured as follows. First, in section II we explore related work in the field of Security and the current usages of Digital Twins. In section III we detail the setup of our experiment to show how Digital Twins can be utilised to improve the security of IoT devices. Section IV goes into the results of our experimentation, and discussed the results achieved from the work done. Finally, section V concludes the research, and section and presents areas of interest for further research.

II. Related Work

In this section, we first reviewed the state of the art in Digital Twins applications, focusing on application in the context of IoT as well as Automated Adversary Emulation (AAE). Then, we combined these reviews to argue that the current issues in the state of the art motivate the creation of a framework to apply AAE to networks of IoT devices.

978-1-6654-9198-3/22/$31.00

A. Digital Twins

When used properly, DTs and cyber twins, which concentrate on cyber security issues, offer tremendous opportunity to enhance the cyber security of vital services or infrastructures. There are a wide range of meanings due to the dynamic nature of DT technology. A digitally determined model that uniquely represents a physical instance, process, system, or similar abstraction is known as a "DT," in broad terms [12]. The Digital Twin was first introduced by Michael Grieves in a 2003 presentation on Product Life-cycle Management (PLM), where Grieves was working with John Vickers of NASA [13]. Following that, in the PLM courses, this conceptual model served as a "Mirrored Spaces Model" by Grieves [14]. Grieves in [13] also defined the architecture to be used while dealing with digital twins. This architecture consisted of 3 main components: The physical component, the virtual one and the the connection to establish a communication channel between the physical and virtual components. The whole process is illustrated in Figure 1.

In the current state of the art, the only consensus is that a

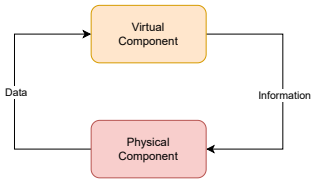

Fig. 1. The Twinning between Physical and Virtual components

Digital Twin is a virtual representation of a physical object. Authors in [15] shown that over half of the reviewed literature also consider a bi-directional connection and the ability to perform simulations on the digital representation integral parts of the definition of Digital Twins. Being able to persist across multiple phases in the physical object's life cycle is explicitly mentioned in about one third of the reviewed literature. [15].

Digital Twins have a wide range of industrial, smart city, and built environment applications. One area of research is the development of Digital Twins for agriculture, enabling farmers to monitor their livestock or crops in real time, model nitrogen levels in the soil, and enable logistic partners to keep track of products in the cold chain [16], [17]. We see that effective modeling and management techniques are required in practice, for example in the management of the nitrogen crisis in the Netherlands. The Government of the Netherlands is setting aside millions of Euros to make farmers drastically more sustainable in their nitrogen output [18], and agricultural Digital Twin technology could become instrumental in this change.

Another application of Digital Twins is in the architecture, engineering and construction (AEC) industry, where digital models of a building may serve to improve the understanding of the state of the building across its lifecycle [19] as well as improve the design and construction process of future buildings by using digital models to assess the impact of design decisions on the construction process and surrounding environment [20]. An example of this impact is the renovation of King's Cross station in the UK. Kaewunruen and Xu investigate the use of Digital Twins in improving the efficiency of information sharing and impact modeling of the renovation [21]. Their study shows that while there are limitations to the technology that will need to be investigated further, the use of Digital Twins in construction shows promise.

We also see the emergence of frameworks that enable faster, modular programming of Digital Twins using low powered IoT devices [22]. Picone et al. present a library that provides built-in MQTT and CoAP engines that programmers of IoT devices can use to transmit data from an IoT enabled device to a central server without having to worry about the underlying transmission protocol. This library can speed up the development of IoT services by abstracting away and standardizing the code for transmitting data.

However, linking the physical and digital realms comes with completely new security issues that are currently not yet solved [19], [23], [24]. The low powered nature of IoT devices means that existing security measures are considered infeasible for use on these devices, often because of the processing power required to implement these security measures. For example, the security measures in MQTT, a widespread transmission protocol for IoT devices, are actively being investigated, with the originally proposed TLS solution being deemed too costly to use [25].

This is where another aspect of Digital Twins comes into play. Not only are Digital Twins useful in monitoring and controlling physical objects, they can also be used to model systems of IoT enabled devices themselves without having to deploy any physical devices. This modeling capability can be used to test updates or changes to the system in a controlled environment [23].

Table I gives an overview of the works discussed in the context of Smart Cities. We see that even in recent papers there is no clear definition of what a Digital Twin is exactly. We do see that most papers share the idea that a Digital Twin is a connection between a physical object and its digital counterpart. Digital Twins have a variety of use-cases in the Agriculture and Construction sectors, and we see work on standardising both the security and programming aspects of Digital Twins. The authors of the taxonomy papers also still identify barriers for Digital Twins that require more research in the future, making Digital Twins an interesting topic of research.

B. Automated Adversary Emulation

Another trending body of research is Automated Adversary Emulation (AAE), a practice where penetration tests on networks are automated in order to reduce cost, improve problem detection, and provide repeatable security testing [26]. The

TABLE I
AN OVERVIEW OF THE RELATED WORK IN THE DIGITAL TWIN FIELD

Reference	Year	Paper Focus	Findings
[15]	2021	Taxonomy	The state of the art in the field of Digital Twins lacks consensus on the definition of a Digital Twin. The authors perform a meta-review of the state of the art to attempt to extract a definition.
[16]	2021	Agriculture	Digital Twins are not yet established in agriculture, and could see use in various applications. An implementation road-map is proposed.
[17]	2021	Agriculture	Digital Twins in combination with AI have the capacity to enable new information and recommendation systems for farmers looking to optimise their livestock management. This information could enable farmers to make more effective choices.
[19]	2021	Security	Building Information Modeling enables a Digital Twin of a building during its entire life-cycle, but current security methods are not capable of keeping this data safe. The authors proposed a rework of the existing Building Information Modeling standards that incorporate security practices into the standard.
[20]	2021	Taxonomy	A review of the state of the art that explores the origins Digital Twins and proposes a definition. The authors also identify key features of a Digital Twin, and highlight some case studies into applications of Digital Twins. They also consider the challenges for wider adoption of Digital Twins.
[21]	2018	Construction	A case study where an analysis of King's Cross station using Building Information Modeling enables construction participants to make more sustainable building choices.
[22]	2021	Software	A standardised, general purpose software library for rapid Digital Twin programming is proposed.
[23]	2021	Taxonomy	A review of the security implications of Digital Twins. The authors showed that Digital Twins have many security risks, but could also be used to improve the security of a system.
[24]	2020	Taxonomy	A review of the enablers and challenges facing Digital Twin technologies. The authors look specifically at the process industry.

MITRE research group, the creators of the MITRE ATT&CK framework [27], have created an Open Source tool to perform AAE known as CALDERA [28]. This tool allows security researchers, red teams, and blue teams to develop penetration testing operations that can be run autonomously against a target system or network.

An important part of the AAE domain is the ability to chain multiple individual abilities from different compromise stages together into one operation. This allows for automated lateral movement and privilege escalation in a network where command & control has been achieved. By emulating a certain attacker, previous work has shown that the security of systems is improved beyond what traditional threat detection is able to achieve [29], [30].

Previous work has shown that it is possible for AAE to be used in both the pre-compromise and post-compromise domain, making it possible to do comprehensive security testing of a computer system or network of systems [31].

So far, Automated Adversary Emulation has been used on traditional computer networks. We opt to employ a cross-domain approach by applying the knowledge existing in the AAE domain to the field of IoT. In the rest of this document we describe a proof of concept for combining Digital Twins of IoT devices with AAE to show the feasibility of automated security testing for IoT networks. This would allow IoT developers to define automatic, repeatable, and low barrier of entry security testing on an IoT device or network of IoT devices without needing access to the physical devices. This can improve the security and stability of IoT networks.

III. METHODS

In this section we detail our methodology for setting up a Digital Twin of an IoT device as well as how we use the AAE tool MITRE CALDERA and the *precomp* plugin to create a repeatable, autonomous attack on this Digital Twin. We start by listing the materials, then explain the setup of the Cyber Digital Twin, and finally show how we set up the AAE software to automatically attempt to perform a cyber attack on this Cyber Digital Twin.

A. Materials

The materials used in this research are mostly software packages. We focus on using Free and Open Source Software (FOSS) applications whenever possible. The choice to use primarily FOSS applications creates a low barrier of entry to replicate the steps detailed in the rest of the methodology. All of the tools in this research are contained in one network of Virtual Machines (VMs) running in Oracle VirtualBox [32].

For the Cyber Digital Twin we used the newest version of the operating system *Raspberry Pi Desktop*, at the time of writing the version released on January 11th 2021. This VM is given 4 logical CPUs and 4GB of memory.

Our choice of Automated Adversary Emulation tool is MITRE CALDERA [26], [28], version 4.0.0-alpha. CALDERA is installed on a VM running Ubuntu version 20.04 with 4 logical CPUs and 4GB of memory. The tool was built and run from source using a Docker Compose file, and has the *sandcat*, *stockpile*, and *precomp* [31] packages installed.

The VMs are hosted on a desktop computer with Windows 10, a Ryzen 5 2600 (6C/12T @3.4GHz), and 16GB of memory.

B. Software Configuration

To perform the experimentation we create a virtual environment that houses the Cyber Digital Twin as well as the AAE tool we will use to attack it. Figure 2 is an overview of the different software components, their configurations, and the most important interactions between them. The rest of this section will go into more detail for each of these components.

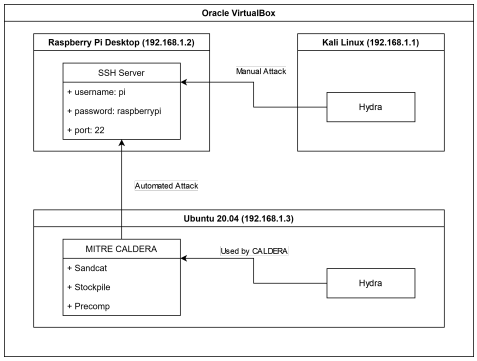

Fig. 2. Scheme

As explained above, we use the Oracle Virtual-box software to run the Virtual Machines for the experiment. There are several reasons for using Virtual-Box. First, it is Open Source software maintained by a large organisation which means it is available for everyone to use, and will likely be supported and updated for quite some time into the future. Also, Virtual-Box supports taking snapshots of the state of a virtual machine, and even exporting and importing virtual machines between computers. This means that sharing Virtual Machine(VM) configurations and quickly rolling back to a Pre-defined state are possible with this software.

For the Cyber Digital Twin we opt to use Raspberry Pi Desktop, a version of the Raspberry Pi operating system that can run on a desktop computer [33]. This is the machine that we will be attacking automatically. Therefore, we need a security vulnerability to be present on the machine that we can exploit. We achieve this vulnerability by giving the user *pi* an insecure password *raspberrypi*. The user *pi* is the root user, and the password is not the default password. This emulates a scenario where the Raspberry Pi was set up to be used remotely, but the setup was done improperly, and is a security risk.[1] One area where we might expect to see such a machine is in a development machine that was entered into production without proper security configuration.

For the first part of our testing, we attempt to attack the insecure SSH server on the Raspberry Pi manually to show that the attack is viable. To do this, we run a Virtual Machine with Kali Linux installed. This operating system is shipped with the Metasploit framework, part of which is a password spraying command line tool called *Hydra* [34].

The second part of testing consists of automating the Hydra attack on the Raspberry Pi Cyber Digital Twin. To do this we run an Ubuntu 20.04 Virtual Machine with the MITRe CALDERA tool and the plugins *sandcat*, *stockpile*, and *precomp*. We also had the Hydra tool installed on this VM. This is required for CALDERA to be able to perform the attack successfully.

One important aspect of the system is the contained nature of the network of Virtual Machines. Any of the attacks are done inside of a network that we control. This means that there is no chance of attacking a network or machine that we do not control, which could lead to damages or legal trouble.

C. Attacking the Cyber Digital Twin

The attack that we are performing is a password spraying attack targeting the SSH server on the Cyber Digital Twin. A successful user authentication on an SSH connection happens as in Figure 3 [35]. After the initial encryption handshake (not shown in the sequence diagram) the SSH client sends a message containing the username and password by which they want to log in on the remote machine. When this authentication succeeds the SSH server responds positively and a session is initiated. The client may then send commands to the server and receive the output of those commands from the server.

A password spraying attack uses a list of potentially viable passwords, which could be obtained from a leaked password database, to attempt to obtain an SSH session on the target machine. Figure 4 shows the sequence diagram for the attack

[1]We specifically chose to use a different password than the default password to imitate a scenario where a seemingly secure configuration fails due to a misconfiguration. This mimics a potential real-world scenario where a password was used in multiple places and was part of a database leak outside of the control of the owner of the Raspberry Pi.

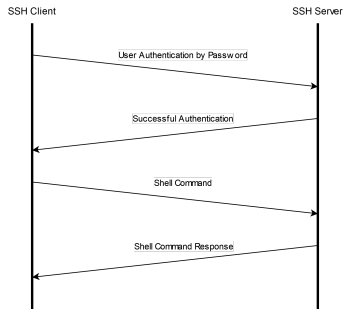

Fig. 3. An SSH session with password authentication, where the username and password are correct

on the SSH server. The attacking tool makes many SSH requests with a different password each time until a username and password combination results in an SSH session.

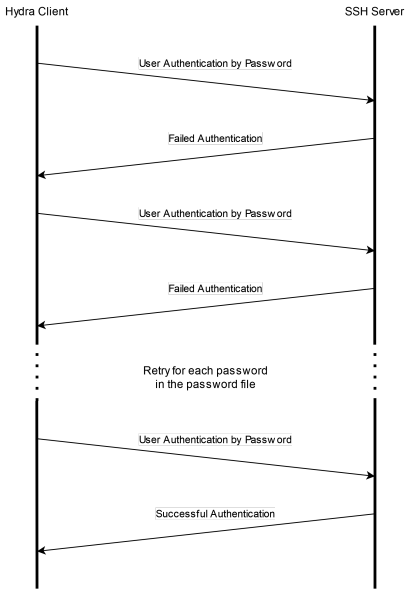

Fig. 4. An SSH session being attacked, we use Hydra to perform a password spraying attack

IV. Results

In this section we outline the results of the methodology described in section III. In this research, we collected the results in two steps. First, we perform the attack on the Cyber Digital Twin manually to show that the attack itself is viable, and produces the expected result. In this step we also show that the password file that is given to Hydra must contain the right password for the attack to succeed. Then, we show that CALDERA can use the *precomp* plugin to run the same attack autonomously against the intended target. Finally, we discuss the results, as well as the limitations of the work and recommendations for future research done based on this result.

A. Manual testing

The first order of business is manually testing the attack on the Cyber Digital Twin with Hydra. The goal of the manual test is to show that the Hydra tool is able to perform an attack against the intended target inside the network of Virtual Machines. We choose to do two manual tests. The first is a test with the correct password in the password file given to Hydra, the second does not have the password in the file that is given to Hydra.

We start by performing the attack where the correct password is in the list of possible passwords that we give Hydra. As previously explained, in this case we expect Hydra to be able to find a username and password combination that will provide access to the Cyber Digital Twin. Indeed, when Hydra is executed the output file shows that one username and password combination was found that would give access to the Raspberry Pi over SSH. We confirm that this is the user *pi* with the password *raspberrypi*, as we expect.

Next, we run the same attack where the list of possible passwords does not contain the correct password. In this case, we expect Hydra will not be able to find a valid combination of username and password to access the Raspberry Pi VM over SSH. The most important reason to perform this negative testing is to show that the method will fail under the right circumstances. Once we switch to automated testing, we will know that Hydra works as expected. With the password not in the list of passwords, Hydra finds no suitable combination of username and password that will allow us to SSH into the Cyber Digital Twin.

B. Autonomous testing

Now that we have shown that using Hydra to obtain the SSH credentials for the machine is possible manually, we move on to using CALDERA to perform the same attack autonomously. We perform each of the steps outlined in the method in section III.

Creating the adversary is a straightforward process, and is done in the web interface as described in the method. Once the operation finishes, we are able to access the output of the password spraying ability to verify it has succeeded. The output of the ability shows the same username and password combination as the output of the manual step, meaning we have successfully autonomously attacked the insecure SSH configuration on the Cyber Digital Twin.

We have shown it is possible to use CALDERA to autonomously attack a Cyber Digital Twin of an IoT device in order to test the security of the software and configuration of the IoT device.

V. Conclusion

To conclude, in this work we have identified a need for security in the field of IoT, shown that the current state of the art is still actively being worked on, and proposed a methodology for automated security testing of IoT devices

using Autonomous Adversary Emulation and Cyber Digital Twins. In the section I, we defined a main goal for this work. To achieve this goal, we have set up an experiment to show that the proven method of Autonomous Adversary Emulation could also be used in combination with Cyber Digital Twins to improve the security of IoT devices. From the methodology and results (sections III and IV) it follows that it is possible to combine these techniques to improve the security of an IoT device. As Smart Cities will be using more IoT devices to collect data about the city, this knowledge could improve the security of these networks of devices, and in turn the privacy of in different IoT applications.

In short, the contribution of this work was the development of a novel method for combining Autonomous Adversary Emulation and Cyber Digital Twins to improve IoT device security.

REFERENCES

[1] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in internet of things (iot)," in *Cyber Security in Networking Conference (CSNet), 2017 1st*. IEEE, 2017, pp. 1–3.

[2] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, 2019.

[3] M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of cryptographic algorithms on iot hardware platforms," in *2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, 2018, pp. 1–5.

[4] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[5] Apple, "Apple AirTag," https://www.apple.com/airtag/.

[6] P. Datta and B. Sharma, "A survey on iot architectures, protocols, security and smart city based applications," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2017, pp. 1–5.

[7] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "Ethereum for secure authentication of iot using pre-shared keys (psks)," in *2019 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Oct 2019, pp. 1–7.

[8] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A taxonomy of puf schemes with a novel arbiter-based puf resisting machine learning attacks," *Computer Networks*, vol. 194, p. 108133, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621002036

[9] ——, "Ethereum for secure authentication of iot using pre-shared keys (psks)," in *2019 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2019, pp. 1–7.

[10] M. Elhajj, H. Jradi, M. Chamoun, and A. Fadlallah, "Lasii: Lightweight authentication scheme using iota in iot platforms," in *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*. IEEE, 2022, pp. 74–83.

[11] J. Kröger, "Unexpected inferences from sensor data: A hidden privacy threat in the internet of things," in *Internet of Things. Information Processing in an Increasingly Connected World*, L. Strous and V. G. Cerf, Eds. Cham: Springer International Publishing, 2019, pp. 147–159.

[12] R. Vrabič, J. A. Erkoyuncu, P. Butala, and R. Roy, "Digital twins: Understanding the added value of integrated models for through-life engineering services," *Procedia Manufacturing*, vol. 16, pp. 139–146, 2018, proceedings of the 7th International Conference on Through-life Engineering Services. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2351978918312897

[13] M. Grieves, "Digital twin: manufacturing excellence through virtual factory replication," *White paper*, vol. 1, no. 2014, pp. 1–7, 2014.

[14] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in *Transdisciplinary perspectives on complex systems*. Springer, 2017, pp. 85–113.

[15] K. J. Kuehner, R. Scheer, and S. Strassburger, "Digital twin: Finding common ground – a meta-review," *Procedia CIRP*, vol. 104, pp. 1227–1232, 2021, 54th CIRP CMS 2021 - Towards Digitalized Manufacturing 4.0. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212827121011045

[16] C. Pylianidis, S. Osinga, and I. N. Athanasiadis, "Introducing digital twins to agriculture," *Computers and Electronics in Agriculture*, vol. 184, p. 105942, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0168169920331471

[17] S. Neethirajan and B. Kemp, "Digital twins in livestock farming," *Animals*, vol. 11, no. 4, 2021. [Online]. Available: https://www.mdpi.com/2076-2615/11/4/1008

[18] Government of the Netherlands, "New steps to tackle nitrogen pollution offer prospects for farmers," https://www.government.nl/latest/news/2020/02/07/new-steps-to-tackle-nitrogen-pollution-offer-prospects-for-farmers.

[19] K. Alshammari, T. Beach, and Y. Rezgui, "Cybersecurity for digital twins in the built environment: current research and future directions," *Journal of Information Technology in Construction*, vol. 26, pp. 159–173, 2021.

[20] R. Al-Sehrawy and B. Kumar, "Digital twins in architecture, engineering, construction and operations. a brief review and analysis," in *Proceedings of the 18th International Conference on Computing in Civil and Building Engineering*, E. Toledo Santos and S. Scheer, Eds. Cham: Springer International Publishing, 2021, pp. 924–939.

[21] S. Kaewunruen and N. Xu, "Digital twin for sustainability evaluation of railway station buildings," *Frontiers in Built Environment*, vol. 4, 2018. [Online]. Available: https://www.frontiersin.org/article/10.3389/fbuil.2018.00077

[22] M. Picone, M. Mamei, and F. Zambonelli, "WLDT: A general purpose library to build iot digital twins," *SoftwareX*, vol. 13, p. 100661, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352711021000066

[23] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal, and H. Janicke, "Digital twins and cyber security – solution or challenge?" in *2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, 2021, pp. 1–8.

[24] M. Perno, L. Hvam, and A. Haug, "Enablers and barriers to the implementation of digital twins in the process industry: A systematic literature review," in *2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2020, pp. 959–964.

[25] S. Shin, K. Kobara, C.-C. Chuang, and W. Huang, "A security framework for mqtt," in *2016 IEEE Conference on Communications and Network Security (CNS)*, 2016, pp. 432–436.

[26] D. Miller, R. Alford, A. Applebaum, H. Foster, C. Little, and B. Strom, "Automated adversary emulation: A case for planning and acting with unknowns," MITRE CORP MCLEAN VA MCLEAN, Tech. Rep., 2018.

[27] MITRE, "MITRE ATT&CK Framework," https://attack.mitre.org/.

[28] ——, "MITRE CALDERA," https://github.com/mitre/caldera.

[29] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam, "Offensive security: Towards proactive threat hunting via adversary emulation," *IEEE Access*, vol. 9, pp. 126 023–126 033, 2021.

[30] A. C. Franco da Silva, S. Wagner, E. Lazebnik, and E. Traitel, "Using a cyber digital twin for continuous automotive security requirements verification," *IEEE Software*, pp. 0–0, 2022.

[31] D.R. Bakker, "Autonomous emulation of adversary procedures in the (pre-)compromise domain," https://essay.utwente.nl/90473/, April 2022.

[32] Oracle, "VirtualBox Virtual Machine Manager," https://www.virtualbox.org/.

[33] Raspberry Pi Foundation, "Raspberry Pi Desktop," https://www.raspberrypi.com/software/raspberry-pi-desktop/.

[34] Heuse, Marc, "HYDRA," https://github.com/vanhauser-thc/thc-hydra.

[35] C. M. Lonvick and T. Ylonen, "The Secure Shell (SSH) Authentication Protocol," https://www.rfc-editor.org/info/rfc4252, jan 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4252