Characterizing Building Automation System Attacks and Attackers

Martino Tommasini, Martin Rosso, Emmanuele Zambon, Luca Allodi, Jerry den Hartog
Department of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, The Netherlands
m.tommasini@student.tue.nl, {m.j.rosso, e.zambon.n.mazzocato, l.allodi, j.d.hartog}@tue.nl

2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) | 978-1-6654-9560-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/EUROSPW55150.2022.00020

***Abstract*—A building automation system (BAS) is an instance of a cyber-physical-system (CPS) in control of building functionalities like lighting, ventilation, CCTVs, and access control. The amount of "smart" buildings has been growing over the years, introducing new technologies which are now being targeted by attackers. In this work, we present the first collection of publicly disclosed security incidents involving Building Automation Systems (BAS). We then provide a qualitative study of attackers targeting BAS and unveil their main characteristics and differences to traditional CPS attackers. We learn that, generally speaking, BAS attackers show a lower sophistication level and that most BAS attacks target the smart IoT components present in modern buildings. Further, access to the BAS is often not the attacker's final goal but "just" a mean to achieve their actual goal. Lastly, we do not observe any advanced, state-sponsored BAS attacks hinting that these play less of a role in BAS (compared to CPS).**

***Index Terms*—building automation system, BAS, industrial control system, ICS, CPS, attack model, cyber security**

1. Introduction

Over the recent years the topic of smart buildings and smart cities gained more and more traction, aiming to make buildings safer, more energy efficient, and more comfortable to use. Today, most, if not all, modern buildings come with a Building Automation System (BAS), [1] a Cyber-Physical System (CPS) [2] monitoring, managing, and automating central building services such as heating, ventilation, and air conditioning (HVAC), lighting, windows and window blinds, fire safety systems, elevator control, CCTV surveillance, or intelligent door locks and access control systems. For this purpose, modern buildings are equipped with a variety of sensors, actuators, and controllers that ensure the operation of the building according to operator-specified criteria.

Especially in the last two decades, many BAS devices became network-aware and IoT devices found their way into BAS networks, so that today a multitude of Internet-exposed BAS devices exist [2]. With this in mind, it is not surprising to see more of these systems to fall victim to cyber attacks. According to the Kasperky ICS CERT [3], in the first half of 2021 their anti-virus software identified and stopped attacks on roughly 40% of the BAS computers it was installed on. Similar figures have been reported for 2020 [4] and 2019 [5].

Given the pressure by attackers, proper protection of BASs is important and it requires to first understand who the attackers are, why they act, what motivates them and what they target. Traditionally, research on BAS security has focused on the manipulation or disruption of the building control system [6], essentially assuming that attackers targeting BASs would behave similarly to "typical" CPS attackers.

In this work, we show that the characterization of CPS attackers proposed in academic literature does not fully capture the attackers targeting BASs, in terms of their available knowledge, resources, and their aim(s). Our analysis shows that BASs are not "just another" Cyber-Physical control System and that there is a need for a dedicated BAS attacker model, since the lack of awareness of the different characteristics of BAS attackers may mislead the study of security measures for BASs. We highlight similarities and core differences between BAS and CPS attackers by instantiating a BAS attacker model based on reports of real-world BAS attacks, following the taxonomy and methodology presented by Rocchetto and Tippenhauer [1]. We then compare the BAS attacker model with the most comprehensive CPS attacker model to date. In particular, our two main contributions are:

First, we collect a database of 26 attacks involving building automation systems. While all the attacks are reported in publicly available resources, to the best of our knowledge this is the first public repository of incident reports for BAS. Most of the incidents in our repository are not listed in other repositories (i.e., IoT or CPS attack/incident libraries like RISI [7]). Our collection is freely available from our artifact repository [8] and can be used as starting point for further studies. [3] Generally speaking, BAS attackers show less sophistication than traditional CPS attackers. The main target are IoT devices, most likely because they pose the easiest target inside a BAS. The lack of observed advanced persistent threats (APT) and the prevalence of IoT botnet attacks are in line with this observation.

Secondly, we create and analyze the first attacker model for BAS based on empirical observations. We then

1. Sometimes called Building Management System (BMS) or similar.

2. For what falls under CPS, we follow the scope of Rocchetto and Tippenhauer [1], which is often also referred to as Industrial Control System (ICS). We will use the terms CPS and ICS interchangeably in this work.

3. Artifacts available online at https://gitlab.tue.nl/sec-lab/bas-security/basattacks/ or via DOI:10.4121/19617243.

DOI 10.1109/EuroSPW55150.2022.00020

analyze and highlight core differences and similarities between BAS and CPS attackers by comparing our BAS attacker model to the most comprehensive CPS attacker model available to date.

The remainder of this paper is organized as follows. In Section 2 we present the background on CPS attackers and attacker models, with particular focus to the publication by Rocchetto and Tippenhauer. The section ends with a gap analysis. In Section 3 we present our approach and how we used the work by Rocchetto and Tippenhauer to derive an attacker model for BAS. We present the results of our analysis in Section 4. Before we conclude in Section 7, we discuss our results in Section 5.

2. Background on CPS Attackers and Gap Analysis

2.1. CPS Attackers and Attacker Models

While there are no dedicated studies that focus on BAS attackers, different works heterogeneously capture the capabilities, available resources, and motivations of attackers targeting CPSs [9]–[13]. In these works, attackers with similar characteristics are often grouped in so-called *attacker profiles* to facilitate the analysis.

A *State APT* or *Nation-State* profile models a sophisticated and stealthy attacker who engages in targeted cyber-campaigns to exfiltrate trade secrets [11] or to disrupt the physical process (i.e., physical availability) controlled by the target CPS [9]. These state-sponsored attackers are associated with security incidents such as the attack on the Iranian uranium enrichment facility in Natanz (Stuxnet) and the attacks against the Ukrainian power grid between 2015 and 2016 (Black Energy and Industroyer/Crashoverride).

The *Insider* is a common threat actor, who is presented as a revenge-driven attacker with authorized access to the target system [9] or sitting in a privileged (physical) position in the target environment [10]. This attacker is also referred to as *Disgruntled Employee* [9], [12] or *Disgruntled system administrator* [12]. A famous CPS incident that is attributed to an insider is the Maroochy Water attack where an ex-contractor of the Australian Maroochy sewage treatment plant deliberately caused the malfunction of the wastewater system producing the copious release of untreated sewage into waterways and local parks [14].

The *Cybercriminal* profile models skilled attackers driven by economical profit [9]. Corman and Etue associates cybercriminals with organized crime [11]. Similar characteristics can be observed in the *Lone hacker* profile by LeMay et al. [12]. A recent CPS incident caused by cybercriminals is the cyber-attack that halted all operations of the Colonial gas and jet-fuel pipeline in May 2021. The hacker group (“DarkSide”), after exfiltrating some data, used ransomware to encrypt files on the computers used in the billing process. Colonial decided to halt all pipeline operations and eventually paid a ransom to resume operation [15].

The *Terrosist* profile is often depicted with limited skills and a lack of stealthiness [12]. Some authors instead emphasise on the terrorist’s strong interest in harming the availability of physical processes [9].

2.2. CPS Attacker Model by Rocchetto and Tippenhauer

All the aforementioned works highlight different academical insights and perspectives on CPS attackers. These heterogeneous perspectives have been summarized and reviewed by Rocchetto and Tippenhauer [1]. In their work from 2016, Rocchetto and Tippenhauer analyze the main literature on attacker models and threat characterization for CPS, including all the aforementioned publications, and propose a comprehensive model based on consensus in academic literature. This makes their work the most comprehensive characterization of attackers targeting CPSs to date. The authors also verify that the attacker model they propose is a correct generalization of the CPS attacker models found in the literature. Even though the study was published in 2016, we are not aware of more recent papers which try to characterize generic CPS attackers.

The unified CPS attacker model proposed by Rocchetto and Tippenhauer consists of six attacker profiles, namely *Basic User*, *Cybercriminal*, *Hacktivist*, *Insider*, *Nation-State*, and *Terrorist*. Each profile is described by a (hierarchy of) 29 dimensions (see the X_{CPS} entries in Table 5 for the attacker model and Figure 3 for the hierarchy, in the Appendix). Rocchetto and Tippenhauer group dimensions into (a) the knowledge and experience of the attacker, (b) the available resources, and (c) the attacker psychology, which includes the behavior and the aims. In particular, aims are distinguished between *physical*, i.e., involving the physical process controlled by the CPS and *virtual*, i.e., involving logical properties of CPS devices.

The attacker model shows the strong interest of *Insider*, *Terrorist*, and *Nation-State*-sponsored CPS attackers to either impair the functionality of the control system (e.g., to manipulate what is done or can be done in the physical world) or to steal data from process control devices (e.g., process knowledge, industrial secrets, . . .). The strong interest is captured by the dimensions describing an aim towards *physical confidentiality*, *physical integrity*, or *physical availability*. The model also shows *Hacktivist*s’ and *Cybercriminal*s’ interest in targeting CPS devices to either exfiltrate data (captured by the dimension describing an aim towards *virtual confidentiality*), or to impair their availability (captured by the dimension describing an aim towards *virtual availability*).

Instead, the dimension describing an aim towards *virtual integrity*, suggests that tampering the logical properties of CPS devices without an effect on the physical world is not an objective of the CPS attacker. In fact, we are not aware of an attack targeting ICS where the attacker tampered a device controlling the physical world when the goal was not connected to the physical world (e.g., only to gain a foothold on the IT network of the target). If we look at BAS, however, we see cases where the attacker tampered a BAS device controlling the physical world without a physical aim. For instance, in an attack against a North American Casino in 2017 [16], cybercriminals manipulated an Internet-reachable smart fish tank used to automate fish feeding and control water quality. The attackers used the compromised fish tank as stepping stone to access the Casino IT network, where they compromised

a database containing data of high-roller customers, managing to exfiltrate 10 Gigabytes of user data.

2.3. Gap between CPS and BAS Attackers

The Casino-Fish-tank-Attack highlights differences in aim and modus operandi between CPS and BAS attackers that an attacker characterization focused on CPS cannot capture in their entirety, even though BASs are an incarnation of a CPS. In this case, the cybercriminals did not aim at compromising *virtual confidentiality* or *virtual availability* of BAS devices, as suggested by the CPS attacker model. Instead, the attackers compromised the *virtual integrity* of the fish tank just as stepping stone to access the more valuable database of high-roller customers. We believe this is not an isolated case and that it may be caused by general differences between typical CPS and typical BAS setups.

From a technological perspective, BASs are much more "open" and interconnected than other CPSs. Gateways allow to interface legacy and/or proprietary devices through standards like e.g., BACnet. These allow the inter-operation of BAS devices from multiple vendors in the same building. Secondly, in BASs, old operational technology (OT, e.g., to control ventilation) is integrated with a variety of IoT devices that are not so common in traditional CPS (e.g., smart sensors, or CCTV cameras). From an environmental perspective, BASs are present in almost every organization, but in the majority of the cases they are substantially less mission critical for an organization compared to other CPS, including e.g., CPS in critical infrastructure or industrial settings. Outages in building automation systems do not necessarily render a building (or part of it) unusable, because many functionalities can either be controlled manually or do not provide strictly required functionalities to keep the building operational (e.g., energy saving).

Considering the different nature of CPS and BAS, and supported by the clear mismatch highlighted by the Casino-Fish-tank-Attack, we believe an attacker model specific to BAS can unveil unique characteristics, that are not currently captured by CPS attacker models.

3. Methodology

To create an attacker model for BAS we adapt the methodology presented by Rocchetto and Tippenhauer [1]. Instead of summarizing the attacker characteristics from the literature, we use empirical observations from real-world BAS security incidents. In this way, the resulting attacker model captures the actual attackers targeting BAS and it is not restricted by the lack of literature on BAS attacker models.

Our approach is illustrated in Figure 1 and consists of four sequential phases.

1) In the *attack collection* phase we methodically collect the largest number of security incidents involving BAS. This collection represents the first public repository of BAS security incidents.
2) In the *attack characterization* phase, we systematically dissect the BAS security incidents collected in the previous phase and we extract the characteristics of attackers targeting BAS.

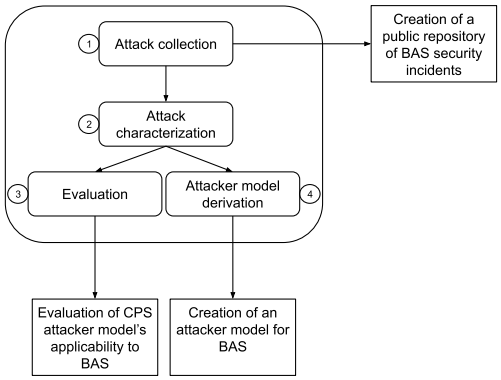

Figure 1. Methodology diagram. The central rounded square summarizes the steps of our methodology; the outer squares represent the output of the steps.

3) In the *evaluation* phase we assess how well the attacker model for CPS describes the characteristics of the attackers causing the collected security incidents. With this assessment we confirm our initial intuition that the existing CPS attacker model does not fully describe BAS attackers.
4) Finally, in the *attacker model derivation* phase we derive the BAS attacker model by processing the attacker characteristics resulting from phase two.

3.1. Attack Collection

The aim of the attack collection phase is to collect relevant security incidents involving building automation, to enable the characterization of attackers. To achieve this, we search the Internet to identify publicly available resources reporting security incidents affecting BASs.

The collection consists of three repeated sessions. We start searching for generic keywords and at each iteration we refine the search keywords using terms we derived from the previous iteration. By iteratively searching terms at different abstraction levels we are able to broaden the scope of relevant resources identified. An iteration stops when we do not learn any new search term and we find no new security incident for 3 hours.

In the **first iteration** we search the Internet for articles and reports containing terms which directly point to attacks against BASs. This search is a combination of words which suggest an attack (e.g. *hack*,*attack*, *incident*) with terms that refer to BAS (e.g. *building*, *BAS*, *Building Automation*, *smart building*). In the **second iteration** the generic BAS descriptions are replaced by expressions that identify a subsystem of the BAS, such as *surveillance*, *HVAC*, *access control*, *heating*. In the **third iteration** the BAS subsystems are replaced by specific BAS device types, such as *door controller*, *HVAC controller*, *security camera*, *elevator*.

To include only relevant security incidents, we follow the following three rules.

1) We are only interested in attacks which involve at least one cyber-component. For instance, security incidents such as [17], are considered out of

scope as they entail no elements characterizing a cyber attack. [4]

2) We are only interested in real attacks, as we aim to derive an attacker model which reflects the actual threat landscape against BASs. Consequently, exercises of penetration testing, security demonstrations or security researches are excluded.
3) Attacks which involve BAS as an externality are included, as they concern Building Automation, although indirectly, and might be useful for future studies (e.g., to investigate the unintentional repercussions that IT attacks can cause to BASs).

3.2. Attack Characterization

The aim of the attack characterization phase is to systematically dissect the security incidents to extract the dimensions characterizing the attackers. This process follows the approach adopted by Rocchetto and Tippenhauer [1] to dissect the attackers into a comprehensive set of dimensions (see dimensions in Figure 3), which is suitable for every CPS, including BAS.

The security incidents analyzed in this phase need to satisfy additional requirements, namely:

1) The security incident provides a sufficient level of detail. The level of information is considered insufficient if no information on the attacker can be derived.
2) The involvement of BAS in the attack **is not** an externality (externalities were considered during the attack collection phase), i.e., the attack on BAS was not an accidental consequence of an attack in another domain. In this way, we model attackers that intentionally target BAS, directly or indirectly.

The thresholds used to map attacker traits to the numeric values defined by Rocchetto and Tippenhauer (i.e., 1, 2, 3) are described in Table 1. While the grey cells indicate labels which are originally defined by Rocchetto and Tippenhauer, the white cells contain labels we refined, as the preexisting labels given by Rocchetto and Tippenhauer were too vague and left large space to subjective interpretation. In general, we precisely describe how each dimension value should be assigned, thus providing more objectivity and, consequently, reproducibility of the mapping process. These less ambiguous thresholds are only a refinement of the original labels and thus maintain the original meaning of the dimension. The detailed explanations can be found in the artifact repository [8]. To converge on the conclusive definition of the labels, multiple rounds of attack characterization are done on a sub-sample of attacks, the agreement ratio (i.e., joint agreement between individual raters) is computed, and conflict resolution is performed after each iteration. In line with other approaches to evaluate consistency of response items, we set the lower bound acceptable agreement score to 70% [18].

Note that we assign a value to a dimension only based on factual data and on observations which are derivable from the attack mechanics, avoiding speculations on attack and attacker behaviours. When information is insufficient to objectively assign a value to a dimension we use the null value, depicted as $\emptyset$. Similarly, if an attacker did not show traits related to a particular dimension, e.g., because the attack did not require it, then the value for such dimension is also null. Attacks are attributed to the creator of the attack. In cases of botnets, the creator of the botnet is the analyzed attacker, and not the botnet user. Only the parts of the attack relevant to BAS are considered. For instance, if a BAS device is compromised and then used as a stepping stone to attack another system, only the part of the attack relevant to BAS is considered.

Finally, based on the information found in the incident reports we attribute each attack to one of the attacker profiles identified by Rocchetto and Tippenhauer: *Basic User*, *Insider*, *Hacktivist*, *Terrorist*, *Cybercriminal*, and *Nation State-Sponsored*.

3.3. Evaluation

To assess to what extent the CPS attacker model describes BAS attackers, we follow the approach of Rocchetto and Tippenhauer and compute the *profile distance metric* [5] between the dimension vector characterized for each attack and the vectors of the six CPS attacker profiles they described. For a given attack, the *predicted* attacker profile is the profile with the smallest distance, while the *expected* attacker profile is the attacker profile tag we assigned in the attack characterization phase. A prediction is considered correct, if the predicted and the expected attacker profiles coincide. A high rate of correct predictions would suggest that the CPS attacker model can model BAS attackers reasonably well, while a high number of incorrect predictions would suggest that the CPS attacker model cannot completely capture the BAS attackers. The results of this phase are presented in Section 4.3.

3.4. Attacker Model Derivation

The aim of this phase is to derive an attacker model which describes the characteristics of attackers targeting BAS. The approach leverages the real-world attack data resulting from the attack collection phase (see Section 3.1, [8]) in order to draw a BAS-specific attacker model which captures the actual threat landscape against Building Automation.

As a result of the attack characterization phase described in Section 3.2, each attack in our BAS database is attributed to an attacker profile, and has a set of instantiated dimension values assigned to it. As we are interested in understanding which are the most common characteristics of each type of attacker against BAS, we group the security incidents by attacker profile and use the rounded average to the nearest integer as grouping function for the more specific non-null sub-dimensions. The parent dimensions are then reconstructed according to the work of Rocchetto and Tippenhauer [1], using an averaging function. The function is only applied to sub-dimensions (i.e., not to automatically computed aggregation-dimensions) in order

4. A man manually pulled the fire alarm in a stadium and fled afterwards.

5. Euclidean distance on a n-dimensional space between two attacker profiles, where n is the number of non-null dimensions.

TABLE 1. MAPPING DIMENSION-VALUE FOR ATTACK CHARACTERIZATIONS

Cells with a grey background are directly taken from Rocchetto and Tippenhauer. Values with white background represent our refined definitions as these values were not clearly specified by Rocchetto and Tippenhauer. For Honesty, Rocchetto and Tippenhauer only defined two values.

Dimension	Low (1)	Medium (2)	High (3)
Physical	General user without offensive expertise	Aware of offensive techniques but no experience	Advanced offensive experience
Network	General user without offensive expertise	Aware of offensive techniques but no experience	Advanced offensive experience
Software	General user without offensive expertise	Aware of offensive techniques but no experience	Advanced offensive experience
Source code	Black Box	Grey Box	White Box
Protocols	Black Box	Grey Box	White Box
Credentials	User	Supervisor	Admin
Distance	Far	Near	Physical Access
Manpower	Individual	Small group	Structured team or large group
Effort	Willingness to overcome a single obstacle	Willingness to overcome multiple obstacles	Unstoppable
Tools	Publicly available tools and easy to use	Tools with non-trivial customization	Advanced custom tools
Financial support	Personal finances	Collective fund	Sponsored fund (almost unlimited)
Honesty	Benign	Malicious	———
Periodicity	Once	Anytime	Continuous
Camouflage	Visible	Stealthy	Invisible
Strategy	Random	Brute-force	Structured
Determination	First attempt	Several attempt	Untiring
Confidentiality	No confidentiality aim	Secondary confidentiality aim	Primary confidentiality aim
Integrity	No integrity aim	Secondary integrity aim	Primary integrity aim
Availability	No availability aim	Secondary availability aim	Primary availability aim

to keep the approximation error to a minimum. Moreover, we only apply the average on non-null entries so they do not influence the outcome. We adopt the rounded average function as grouping function as it captures the average capabilities of the attacker. A graphical representation of this process is depicted in Figure 2.

The result of this operation are six attacker profiles characterized by a set of dimensions which together represent the attacker model for BAS. The results of this phase are presented and discussed in Section 4.4.

4. Results

4.1. Attack Collection

Adopting the approach defined in Section 3.1, we managed to collect 26 security incidents from publicly

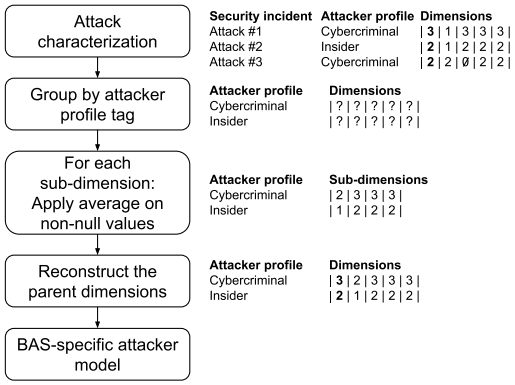

Figure 2. Attacker model derivation diagram. The example consists of a dataset of three attacks, characterized by one parent dimension (in bold) and four sub-dimensions.

available articles reporting cyber security incidents. The collection can be found in the artifact repository [8]. To the best of our knowledge, this repository is the first public database collecting security incidents involving BAS.

The time of occurrence of the security incidents ranges from 2009 to 2021 with an isolated security incident in 1995, when a student illegally accessed a rudimentary heating controller in the heating room of his school. However, around 70% of the attacks are recorded between 2016 and 2021 when the BAS industry also experienced a significant growth.

Large portion of the collected attacks (11/26) consists of botnet threats, often involving IoT devices. Although Bashlite- or Mirai-like botnets against IP cameras are the most frequent, botnets which pursue an ethical purpose, despite controversial means, are also present. Examples of such cases are BrickerBot and Silex which infect machines by exploiting default credentials in common software and aim at bricking the devices to prevent them from being infected by Mirai. Other collected security incidents involve supply-chain attacks between HVAC vendor and contractors, so as revenge-driven attacks carried out by disgruntled employees against building automation devices they previously worked with.

4.2. Attack Characterization

Only 22 out of the 26 security incidents found in the attack collection phase satisfy the additional requirements for the attack characterization phase (see Section 3.2). Two of the security incidents are excluded as the BAS involvement is an externality and another two attacks are ruled out as they provide an insufficient level of detail. The process of label refinement has been repeated three times following Section 3.2; three rounds of three attacks were compared before the authors reached an agreement ratio of 74% (i.e. 50%, 68%, 74%). With the refined definitions, all 22 valid security incidents are characterized and a final agreement ratio of 79.5% is computed on the attacks that were excluded from the training rounds. We describe the attack characterization process for two attacks in detail.

Mirai Botnet. Mirai is an IoT botnet which exploits default credentials in open Telnet ports of Internet-facing devices. Given the poor security of surveillance cameras,

TABLE 2. CHARACTERIZATION OF THREE CASE STUDY ATTACKS.

	Attacker profile	Knowledge	Offensive	Physical	Network	Software	System	Source code	Protocols	Credentials	Resources	Distance	Manpower	Effort	Tools	Financial support	Psychology	Honesty	Periodicity	Camouflage	Strategy	Determination	Aim-physical	Integrity-Physical	Confidentiality-Physical	Availability-Physical	Aim-virtual	Integrity-Virtual	Confidentiality-Virtual	Availability-Virtual
Mirai IoT botnet	Cybercriminal	2	2	∅	2	2	1	1	1	1	2	1	2	2	2	1	2	2	3	2	3	2	1	1	1	1	2	3	1	1
Boston Hospital HVAC-vendor attack	Cybercriminal	2	2	∅	2	∅	1	1	1	1	1	1	∅	∅	∅	∅	2	2	1	∅	3	∅	2	1	3	1	1	1	1	1
Casino-Fish-tank-Attack	Cybercriminal	2	3	∅	3	2	1	1	1	1	2	1	∅	2	2	∅	2	2	2	2	3	2	1	1	1	1	2	3	1	1

a large portion of these devices was compromised, recruited into the botnet and used to perform DDoS attacks. To characterize the attack as described in Section 3.2, the (original Mirai botnet) attack is evaluated according to the dimensions, starting from the more specific sub-dimensions, and the appropriate attacker profile tag is added to classify the attacker (i.e., Cybercriminal). While no information can be derived on the physical offensive knowledge of the attackers (Physical ∅), the attackers show offensive experience in the network and software field, as they are aware of bruteforcing techniques, C&C patterns and implementations. However, no advanced offensive knowledge is shown, and for this reason values are set to 2. Attackers do not have preexisting knowledge of source code, protocols and credentials of the target systems (Source code 1, Protocols 1, Credentials 1). The creators of the botnet are a small group of three students (Manpower 2) and the attack is carried out remotely (Distance 1). The effort to perform the attack is minimum, as only credential bruteforcing on the Telnet service is performed. However additional commitment is necessary in the preparation phase to write, test and debug the malware (Effort 2). Although the botnet tool created is indeed non-trivial, the tool does not offer advanced functionalities (Tools 2). No finances are needed to perform the attack (Financial support 1). Attackers are motivated by a malicious aim (Honesty 2) and the botnet is continuously scanning the Internet to infect new devices (Periodicity 3). Although the attacker's desire to remain undetected, the botnet can easily be spotted in the device (Camouflage 2). The attack follows a structured strategy (Strategy 3). In fact, it first scans the Internet for devices exposing open Telnet ports, then performs a dictionary attack to guess the correct credentials. Once a device is infected, it connects to the C&C and waits for commands from the attackers. Although the attacker proved determination in the large scale attack, by writing the malware and sustaining the attack over time, the attack is automated and has not significantly evolved over time (Determination 2). Finally, the attackers' only aim is to infect devices to install malware that can enable their enrollment as bots in DDoS attacks. Therefore, Virtual integrity is set to maximum (Integrity-Virtual 3) and all the other aims are set to the minimum value. Once the aforementioned sub-dimensions are set, the parent dimensions are recursively reconstructed, yielding the complete characterization of the Mirai attack as shown in Table 2.

Boston Hospital HVAC-vendor attack. The second security incident we characterize in Table 2 is the Boston Hospital HVAC-vendor attack. Here, the attackers compromised EME Systems, a large HVAC Controls contractor which manages the building automation and security for the clients. With this access, the attackers were able to access the HVAC interfaces of the customers, one of which is the Boston Children's Hospital (BCH). The attackers then took screenshots of diagrams and floor layout of the hospital and demanded the HVAC vendor to pay a ransom fee. Using the same approach demonstrated for the *Mirai Botnet*, the attack is characterized and presented in Table 2. The quality and quantity of reported information is not sufficient to map all the dimensions, thus resulting in few null values.

TABLE 3. ATTACKER PROFILES DISTRIBUTION

Attacker profile	nr	%
Cybercriminal	11	50
Basic user	6	27
Insider	3	14
Hacktivist	2	9
Nation-state	0	0
Terrorist	0	0

The same process applies to the remaining 20 valid security incidents. The complete list of characterized attacks can be found in the artifact repository [8]. A concise summary of the attacker profiles distribution can be found in Figure 3. The Figure illustrates the number of attacks and relative percentage of each attacker profile.

4.3. Evaluation

Here we report the results of the evaluation phase (Section 3.3). We use the two case studies of Section 4.2 as examples. We compute the *profile distance metric* to identify the attacker profile predicted by the CPS attacker model and then compare it to the expected one. According to the *profile distance metric*, the attacker profile that most accurately describes the Mirai attack is the *Cybercriminal* (with a distance of 3.87). In this case, the predicted value and the expected profile match (i.e., both *Cybercriminal*). Instead, for the *Boston Hospital HVAC-vendor attack*, the *profile distance metric* between the attack and the six attacker profiles predicts *Basic user* (with Euclidean distance 3.60) and only scores the expected attacker profile (i.e., *Cybercriminal*) as fifth, thus hinting that the characteristic of the typical CPS-*Cybercriminal* are very different to the traits showed by this BAS-*Cybercriminal*.

TABLE 4. PROFILE DISTANCE METRIC BETWEEN SECURITY INCIDENTS AND THE SIX CPS ATTACKER PROFILES

Security incident	#1	#2	#3	#4	#5	#6
Mirai IoT botnet	**C** (3.87)	**H** (4.58)	**B** (4.89)	**T** (5.19)	**N** (6.0)	**I** (6.08)
Boston Hospital HVAC-vendor attack	**B** (3.60)	**N** (3.60)	**H** (4.12)	**T** (4.35)	**C** (4.58)	**I** (5.38)
Casino-Fish-tank-Attack	**C** (3.46)	**H** (4.24)	**B** (5.09)	**N** (5.09)	**T** (5.38)	**I** (6.24)
Target Data Beach	**H** (2.64)	**C** (3.31)	**N** (4.35)	**T** (5.09)	**B** (5.91)	**I** (6.16)
Ghost exodus HVAC hack	**I** (4.58)	**B** (5.0)	**H** (6.16)	**C** (6.24)	**T** (6.32)	**N** (8.06)
Hack on security cameras	**B** (2.44)	**T** (4.79)	**H** (6.08)	**I** (6.24)	**C** (6.40)	**N** (7.34)
Stadium SEA Games camera hack	**I** (4.12)	**B** (5.29)	**C** (5.91)	**T** (6.40)	**H** (6.55)	**N** (8.94)
Industrial heating system hack / niagara	**B** (3.16)	**H** (3.16)	**C** (3.60)	**T** (3.87)	**N** (5.29)	**I** (5.47)
Hack on heating system in supermarket	**I** (3.87)	**B** (4.79)	**T** (6.0)	**C** (6.78)	**H** (6.92)	**N** (7.93)
BrickerBot IoT botnet	**C** (3.31)	**H** (3.74)	**B** (4.69)	**T** (4.69)	**I** (5.74)	**N** (6.16)
Silex IoT botnet	**C** (3.46)	**H** (4.0)	**B** (4.58)	**T** (4.89)	**I** (5.83)	**N** (6.70)
Bashlite IoT botnet	**C** (3.87)	**H** (4.58)	**B** (4.89)	**T** (5.19)	**N** (6.0)	**I** (6.08)
Persirai IoT botnet	**C** (3.74)	**H** (4.58)	**B** (4.79)	**T** (5.19)	**N** (5.91)	**I** (6.0)
Aidra IoT botnet	**C** (4.0)	**B** (4.58)	**H** (4.89)	**T** (5.29)	**I** (6.16)	**N** (6.70)
Linux/IRCTelnet IoT botnet	**C** (3.74)	**H** (4.58)	**B** (4.79)	**T** (5.19)	**N** (5.91)	**I** (6.0)
Hajime IoT botnet	**C** (3.74)	**H** (4.58)	**B** (4.79)	**T** (5.19)	**N** (5.91)	**I** (6.0)
OMG IoT botnet	**C** (3.74)	**H** (4.58)	**B** (4.79)	**T** (5.19)	**N** (5.91)	**I** (6.0)
Hide 'n' Seek (HNS) IoT botnet	**C** (3.16)	**H** (4.12)	**B** (4.69)	**T** (5.0)	**N** (5.74)	**I** (5.91)
Dark Nexus botnet	**C** (3.87)	**H** (4.58)	**B** (4.89)	**T** (5.19)	**N** (6.0)	**I** (6.08)
Hack on Dallas emergency alarm system	**B** (3.0)	**T** (3.0)	**I** (3.74)	**H** (4.35)	**C** (5.29)	**N** (5.38)
Student access heating system in school	**B** (2.44)	**T** (4.79)	**H** (5.91)	**I** (5.91)	**C** (6.24)	**N** (8.12)
KNX-based smart building hacked	**B** (3.87)	**T** (4.0)	**H** (4.47)	**C** (4.69)	**I** (5.47)	**N** (5.56)
# Total	13	3	4	1	1	0

B=BasicUser, C=Cybercriminal, H=Hacktivist, I=Insider, N=NationState, T=Terrorist, (Float)=Euclidean distance, X(x.x)=Expected mapping
Profiles are ordered by distance. The profile with the smallest distance (i.e., left-most) is the prediction, the underlined profile is the actual/expected profile.

The same process is repeated over the remaining 20 incidents; the results are shown in Table 4. The table shows, that only 60% (13 out of 22) attackers were correctly matched to the appropriate attacker profile. The most frequently misclassified attacker profiles are *Basic User*, *Cybercriminal* and *Hacktivist*. This low rate of correct predictions confirms our initial intuition that the CPS attacker model cannot fully capture the attackers targeting BAS.

4.4. BAS Attacker Model

Supported by the results obtained in Section 4.3, which highlight the need of an attacker model specific to BAS, we present the results of the attacker model derivation phase (see Section 3.4). The resulting attacker model consists of six attacker profiles with clear and formal characteristics which can be observed in Table 5. The profiles for *Terrorist* ($\mathbf{T}_{BAS}$) and *Nation-State* ($\mathbf{N}_{CPS}$) remain undefined as there are no respective BAS security incidents in our database. The distribution of attacks by attacker profile is shown in Table 3.

5. Discussion

5.1. Discussion of Results

Low Attacker Sophistication and Basic User. Table 5 shows that BAS attackers seem to have similar but often lower sophistication than the respective CPS attackers. We interpret this as an indicator that BAS attacks are generally easier to carry out. This implies that more sophisticated attackers do not have to show their full repertoire, while at the same time less sophisticated attackers can successfully carry out attacks against BASs.

The only exception is the *Basic User* profile ($\mathbf{B}_{BAS}$) where the BAS attacker shows to posses more *Offensive-Knowledge* and a slightly stronger interest on *Virtual-Aims*. This is the result of multiple IoT botnets involving smart building devices such as CCTV cameras, as 4 out of 6 *Basic User* attackers are botnet creators. This share of the botnet incidents is attributed to *Basic users* as the attackers behind the botnets are not motivated by commercial interests (and thus not fall into the *Cybercriminal* profile), or moved by a political motivation (and thus not fulfill the requirements Rocchetto and Tippenhauer pose on an *Hacktivist*). Indeed, the sophistication of a botnet author is higher than the typical "Script Kiddie", and this reflects in higher scores for *Basic User*.

BAS as Mean and not Final Target. Many of the BAS attacker profiles show attackers aiming to compromise *Virtual-Integrity*. This is particularly evident in the *Cybercriminal* profile which does not show any other aim, differently from CPS. The minimum scores for availability and confidentiality, together with the interest at aiming the *Virtual-Integrity* is a clear confirmation of a trend that is particularly evident in the dataset. Namely, BAS is often not the final target of the attack, but only a mean to achieve other goals (in other domains). Particularly, we observed three ways an attacker (usually a *Cybercriminal*) leverages BAS to target other systems. First, the attacker can compromise a BAS device to use it as a stepping stone to an IT network, as in the Casino-Fish-tank-Attack. Second, the attacker can target an HVAC service provider (i.e., integrator and maintenance contractor) and, because of that, gain access to internal computer networks of their

TABLE 5. BAS VS CPS ATTACKER MODEL

	Knowledge	Offensive	Physical	Network	Software	System	Source code	Protocols	Credentials	Resources	Distance	Manpower	Effort	Tools	Financial support	Psychology	Honesty	Periodicity	Camouflage	Strategy	Determination	Aim-physical	Integrity-Physical	Confidentiality-Physical	Availability-Physical	Aim-virtual	Integrity-Virtual	Confidentiality-Virtual	Availability-Virtual
$\mathbf{B}_{BAS}$	◐	◐	○	◐	◐	○	○	○	○	○	○	○	◐	◐	○	◐	●	◐	○	●	◐	○	○	○	○	◐	◐	○	◐
$\mathbf{B}_{CPS}$	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
$\mathbf{C}_{BAS}$	◐	◐		◐	◐	○	○	○	○	◐	○	◐	◐	◐	○	◐	●	◐	◐	●	◐	○	○	○	○	○	◐	○	○
$\mathbf{C}_{CPS}$	◐	◐	○	●	◐	○	○	○	○	◐	○	○	◐	●	◐	◐	●	◐	◐	●	◐	○	○	○	○	●	◐	●	●
$\mathbf{H}_{BAS}$	◐	◐	○	◐	◐	○	○	○	○	○	○	◐	○	○	○	○	●	○	○	○	○	○	○	◐	○	○	○	◐	○
$\mathbf{H}_{CPS}$	◐	◐	○	●	●	○	○	○	○	◐	○	◐	●	◐	○	◐	●	○	◐	◐	●	○	○	○	○	◐	○	●	●
$\mathbf{I}_{BAS}$	◐	○	○	○	○	●		●	●	○	◐	○	○	○	○	○	●	○	○	◐	○	○	◐	○	○	◐	◐	○	◐
$\mathbf{I}_{CPS}$	◐	○	○	○	◐	●	●	●	●	◐	●	○	◐	◐	○	◐	●	○	◐	●	◐	◐	◐	◐	◐	◐	○	◐	◐
$\mathbf{N}_{BAS}$																													
$\mathbf{N}_{CPS}$	◐	●	●	●	●	○	○	○	○	●	○	●	●	●	●	◐	●	○	●	●	●	●	◐	●	●	○	○	◐	○
$\mathbf{T}_{BAS}$																													
$\mathbf{T}_{CPS}$	○	○	○	○	○	○	○	○	○	◐	○	◐	●	◐	◐	◐	●	○	○	○	●	◐	○	○	●	◐	○	◐	◐

Each row resembles an attacker profile for either BAS or CPS. The symbols ○, ◐, ● represent values 1, 2, 3; a blank space represents the null value (∅). The abbreviations **B**, **C**, **H**, **I**, **N**, **T** refer to the attacker profiles *Basic User*, *Cybercriminal*, *Hacktivist*, *Insider*, *Nation State*, and *Terrorist* respectively.

customers, as in the Boston Hospital HVAC-vendor attack and the Target Data Breach [19]. Third, the attacker can compromise easily accessible IoT devices such as CCTV cameras to recruit them in a botnet, which can serve other purposes (e.g. use computational power of the device for DDoS or mining, sell access to device).

These behaviors, most of the times exhibited by *Cybercriminals*, clearly show that BAS is often not the final target of the attack but a mean to reach another goal. This consequently suggests that *Cybercriminals* have not yet found a profitable business model targeting BAS, but leverage BAS to increase their chances to find profit in other domains.

Botnets and IoT as the Weakest Link. Another contributor to the *Virtual-Integrity* is the prevalence of botnets (11 out of 22 attacks in our database are botnets). These botnets do not especially target building automation devices but any IoT device accessible from the Internet. In the last two decades previously isolated building automation devices and subsystems became network-aware and smart replacing old operational technology (OT). Especially modern CCTV cameras and the smart fish tank (from Casino-Fish-tank-Attack [16]) are an example of such smart IoT-like devices in a building automation setup. We believe smart devices make easier targets than classic OT systems as they come with more common software and protocol stacks. As a direct result we observe more attacks against CCTV cameras (in total 13/22 attacks involving CCTV cameras, of which 11 are botnets).

Lack of Nation-State and Terrorist Profiles. The profiles for *Terrorist* ($\mathbf{T}_{BAS}$) and *Nation-State* ($\mathbf{N}_{BAS}$) remain undefined because we were unable to identify any BAS attack motivated by terrorism or performed by a Nation-State actor. We link the absence of such attackers to the less critical role played by the BAS in the achievement of the company's mission and, consequently, the limited impact an attack against most building automation system can have.

Since Stuxnet, the general public observed a multitude of state-sponsored attacks against CPS (e.g., the Black Energy and Industroyer/Crashoverride malware responsible for power outages in Ukraine 2015 and 2016). These high-end attacks are also usually well described in public reports, either because of the attack sophistication level, or because of the impact they have. The fact that we were unable to observe any such attack on BAS strongly hints that there are no advanced persistent threats (APT) in this domain.

(Recent) Attacks against Physical Availability. Even though none of the BAS attacker profiles shows particular interest in targeting *Physical Availability* so far, the recently reported KNXlock attack [20] shows a different picture. Using an Internet-facing IP-to-KNX gateway that was most likely forgotten by the integrator, the attackers could connect to the message bus of a KNX-based Building Automation solution from remote. For all KNX devices connected to the message bus, the attackers purged the configuration files and set a device password (the BCU

key) that cannot or can only be reset by the device vendor. The password prevents the building integrator from simply re-deploying a previously backed-up configuration onto the devices, making this one of the few examples of attacks aimed to compromise *Physical-Availability*, and the only one targeting the *Availability* of the BAS itself.

This attack does not require advanced resources or knowledge. [6] Because of the low resource requirements, we find it reasonable to expect we will witness more attacks like this in the mid-term future, most likely from economically motivated attackers (i.e., *Cybercriminals* demanding a ransom).

5.2. Limitations

Our attacker model derives from the analysis of publicly disclosed articles reporting security incidents involving BAS. The quantity and quality of articles available online is a natural limitation of our approach. However, we expect the number of (publicly available) security incidents to grow over time and thus allow to better model attackers in the future. Additionally, our approach can only describe attackers based on the capabilities shown during the attack. The actual capabilities of the attackers may be higher as any given attacker might have shown only a subset of their capabilities (i.e., that necessary to successfully execute the attack). Naturally, the capabilities shown by attackers might evolve over time, as attackers need to respond to improved defensive security measures that could be deployed in the future.

6. Related Work

6.1. Attack Databases

While there are a few prominent databases of CPS security incidents, there is no such collection dedicated to BAS attacks. In particular, only very few BAS attacks appear in dedicated CPS attack collections.

The Repository of Industrial Security Incidents (RISI) [7] is an online database collecting security incidents involving ICSs. The database is now no longer updated (last update was in January 2015), thus not capturing the current attacker trends.

The Operation Technology Cyber Attack Database (OTCAD) [21] consists of 133 (and growing) publicly known cyber attacks, mapped to the MITRE ATT&CK for ICS matrix. The database has been published in 2021 and collects CPS incidents extracted from VERIS, RISI, and five research papers. There is only a minimal overlap between OTCAD and our database (i.e., at the time of writing we are only aware of one attack present in both databases).

The VERIS Community Database (VCDB) [22] is a community driven database of ICS security incidents. The database aims to capture all publicly disclosed security incidents and counts more than 8000 individual security incidents. Only 3 attacks are shared between the VCDB and our collection.

6. knowledge of the public IP address of the IP-to-KNX gateway and a copy of the KNX "ETS" engineering tool software are sufficient.

6.2. Attacker Modelling

The scientific literature presents different studies on an attacker model for IT and CPS. However, to the best of our knowledge, no studies on an attacker model are specifically tailored to BAS. In this section, we concisely review the main literature related to attacker modelling.

Alan Magar [23] presents a study on the state of the art of cyber-threat modelling up to 2016. The author collects and presents methodologies covering threat characterization and threat modelling. Although many different papers are reviewed and contextualised in this work, none of them describes a methodology which is suitable to analyze the characteristics of BAS attackers. In fact, either the approaches do not aim to create an attacker model, or they require data which is rarely available in the BAS context.

Doynikova et al. [24] propose a general approach to derive an attacker model from raw data (e.g. network traffic, event logs). Particular focus is given to the prediction of attacker behaviours. The authors also review various techniques which aim at classifying the attackers. Such analyzed approaches include techniques based on attack graph analysis, hidden Markov model, fuzzy inference, statistics and neural networks. The proposed methodology relies on the accessibility of raw data, which is usually unavailable for BAS.

Watters et al. [25] present a modelling approach to find patterns in data based on the analysis of dependent and independent variables. The authors apply the model to analyze the impact of socio-economic variables to the level of card skimming. We believe the methodology might be applied to build an attacker model from real-world attacks, by selecting a relevant set of dependent and independent variables, which best describe the attack's and attacker's characteristics to study. Although the methodology is flexible, it would require the availability of large quantities of publically available data, which is missing in BAS.

Mayer et al. [26] present an abstract model of a building automation system and develop attack trees which model few pathways an attacker might take in a cyber attack against BAS. Although the attack trees model threats against BAS, they do not provide a model of the attacker.

Ahmadian et al. [27] propose a taxonomic framework aimed at analyzing and dissecting ICS attacks. The authors combine the main characteristic of the known taxonomies and define new attributes to classify ICS security incidents. The authors also analyzed 248 ICS security incidents using their framework and extracted the main attacks' and attackers' patterns. However, the authors do not provide the collection of analyzed ICS attacks. Moreover, although the framework offers a formal taxonomy to dissect security incidents, the solution is tailored to ICS and defines few attributes which are not meaningful to BAS. Therefore, the framework could only be applied partially to the BAS context.

7. Conclusions and Future Work

After creating a knowledge base of BAS security incidents of 26 attacks involving Building Automation Systems from public sources, we showed that the most comprehensive CPS attacker model to date is unable to

fully capture BAS attackers. We created a BAS attacker model from the collected attacks and highlight similarities and differences between BAS and CPS attackers.

In general, BAS attackers show less sophistication, potentially because BAS devices make easier targets than CPS devices. We did not observe any APT, instead half of the attacks are botnets targeting generic IoT devices, including IoT in BAS settings. This shows that, at least at present time, IoT devices are an easier target than other CPS devices found in a building automation system (e.g., controllers, sensors and actuators). Finally, we observed attackers targeting BAS device vendors and integrators to then leverage their privileged access to customer software and hardware. Defensive measures to improve BAS security should be focused accordingly.

Additional data regarding BAS security incidents is necessary to improve the quality of our attacker model and to clarify observed trends. For this reason, access to (high-quality) undisclosed BAS security incidents can significantly improve the quality of the model, however gaining access to this type of data is unlikely as most parties are not willing to share such sensitive information.

Acknowledgments

This research was funded in whole, or in part, by the Dutch Research Council (NWO), project DEPICT (grant no. 628.001.032) and the ITEA3 program by Rijksdienst voor Ondernemend Nederland, project DEFRAUDIfy (grant no. ITEA191010). For the purpose of open access, a CC BY public copyright license is applied to any Author Accepted Manuscript version arising from this submission. As part of the open-report model followed by the Workshop on Attackers & CyberCrime Operations (WACCO), all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO/tree/main/WACCO-2022.

References

[1] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *Computer Security – ESORICS 2016*, ser. Lecture Notes in Computer Science, vol. 9879. Springer, 2016, pp. 427–449.

[2] O. Gasser, Q. Scheitle, C. Denis, N. Schricker, and G. Carle, "Security implications of publicly reachable building automation systems," in *2017 IEEE Security and Privacy Workshops (SPW)*, 2017.

[3] "Threat landscape for industrial automation systems. Statistics for H1 2021." [Online]. Available: https://ics-cert.kaspersky.com/reports/2021/09/09/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2021/

[4] "Threat landscape for smart buildings. H1 2020 in brief." [Online]. Available: https://www.kaspersky.com/about/press-releases/2020_share-of-attacks-against-the-building-automation-and-oil-gas-industries-grow-in-the-first-half-of-2020

[5] "Threat landscape for smart buildings. H1 2019 in brief." [Online]. Available: https://ics-cert.kaspersky.com/publications/reports/2019/09/19/threat-landscape-for-smart-buildings-h1-2019-in-brief/

[6] W. Granzer, F. Praus, and W. Kastner, "Security in building automation systems," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3622–3630, 2010.

[7] RISI database. [Online]. Available: https://www.risidata.com/

[8] M. Tommasini, "BAS attack database and attacker characterization," dataset. [Online]. Available: https://gitlab.tue.nl/sec-lab/bas-security/basattacks

[9] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Workshop on Future Directions in Cyber-physical Systems Security*. DHS, 07 2009. [Online]. Available: http://chess.eecs.berkeley.edu/pubs/601.html

[10] D. Urbina, J. Giraldo, N. O. Tippenhauer, and A. Cardenas, "Attacking fieldbus communications in ICS: Applications to the SWaT testbed," in *Singapore Cyber-Security Conference (SG-CRC) 2016*, 2016.

[11] J. Corman and D. Etue, "Adversary ROI: Evaluating Security from the Threat Actor's Perspective," 2012, rSA Conference Europe.

[12] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)," in *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, 09 2011.

[13] R. Heckman, "Attacker classification to aid targeting critical systems for threat modelling and security review," ROCKYH, Tech. Rep., 2005.

[14] Maroochy shire sewage spill. [Online]. Available: https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill

[15] Colonial hackers stole data thursday ahead of shutdown. [Online]. Available: https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

[16] "Fish tank Casino hack." [Online]. Available: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/

[17] "Gillette Stadium fire-alarm." [Online]. Available: https://www.sbnation.com/2017/1/22/14350196/

[18] M. Tavakol and R. Dennick, "Making sense of cronbach's alpha," *Int J Med Educ*, vol. 2, pp. 53–55, 2011.

[19] "Target Data Breach." [Online]. Available: https://coverlink.com/cyber-liability-insurance/target-data-breach/

[20] K. J. Higgins. Lights out: Cyberattacks shut down building automation systems. [Online]. Available: https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems

[21] OTCAD: Operational Technology Cyber Attack Database. [Online]. Available: https://github.com/SecuraBV/OTCAD

[22] VERIS Community Database. [Online]. Available: https://github.com/vz-risk/VCDB

[23] A. Magar, "State-of-the-Art in Cyber Threat Models and Methodologies," Department of National Defence of Canada, Tech. Rep., 2016. [Online]. Available: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803699_A1b.pdf

[24] E. Doynikova, E. Novikova, and I. Kotenko, "Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects," *Information*, vol. 11, p. 168, 3 2020.

[25] P. A. Watters, S. McCombie, R. Layton, and J. Pieprzyk, "Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP)," *Journal of Money Laundering Control*, vol. 15, pp. 430–441, 10 2012.

[26] D. Meyer, J. Haase, M. Eckert, and B. Klauer, "A threat-model for building and home automation," in *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, 07 2016.

[27] M. M. Ahmadian, M. Shajari, and M. A. Shafiee, "Industrial control system security taxonomic framework with application to a comprehensive incidents survey," *International Journal of Critical Infrastructure Protection*, 06 2020.

Appendix

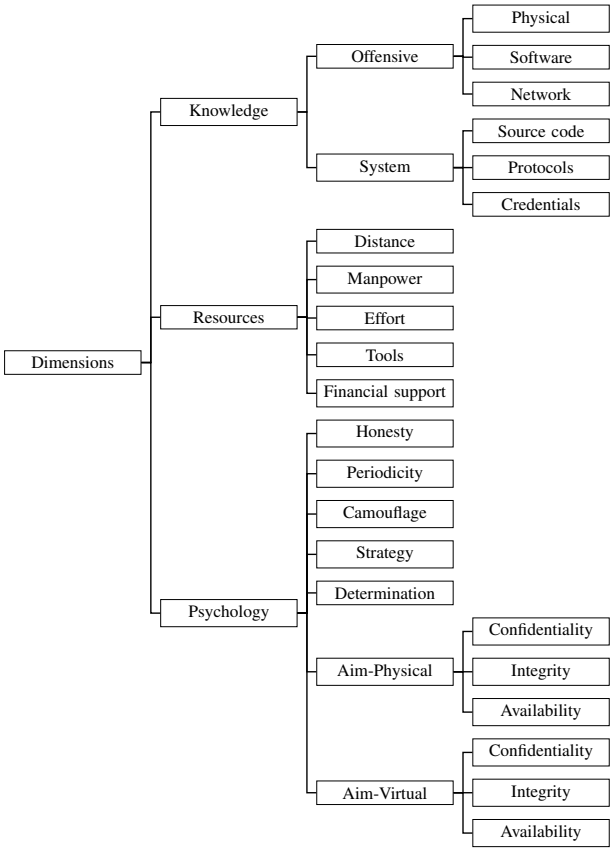

Figure 3. Dimensions hierarchy as defined by Rocchetto and Tippenhauer [1]