Taxonomy for Description of Cross-Domain Attacks on CPS

Mark Yampolskiy, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, Janos Sztipanovits
Vanderbilt University, Institute for Software Integrated Systems (ISIS)
myy@isis.vanderbilt.edu, phorvath@isis.vanderbilt.edu, Xenofon.Koutsoukos@Vanderbilt.Edu,
yuan.xue@Vanderbilt.Edu, janos.sztipanovits@vanderbilt.edu

ABSTRACT

The pervasiveness of Cyber-Physical Systems (CPS) in various aspects of the modern society grows rapidly and CPS become attractive targets for various kinds of attacks. We consider cyber-security as an integral part of CPS security. Additionally, the necessity exists to investigate the CPS-specific aspects which are out of scope of cyber-security. Most importantly, attacks capable to cross the cyber-physical domain boundary should be analyzed. The vulnerability of CPS to such cross-domain attacks has been practically proven by numerous examples, e.g., by the currently most famous Stuxnet attack.

In this paper, we propose a taxonomy for description of attacks on CPS. The proposed taxonomy is capable of representing both conventional cyber-attacks as well as cross-domain attacks. Furthermore, based on the proposed taxonomy, we define an attack categorization. Several possible application areas of the proposed taxonomy are extensively discussed. Among others, it can be used to establish a knowledge base about attacks on CPS that are known in the literature. Furthermore, the proposed description structure will foster the quantitative and qualitative analysis of these attacks, both of which are necessarily to improve CPS security.

Categories and Subject Descriptors

J.7 [**Computer in Other Systems**] Industrial control; Consumer products; Military; Real time; Process control

C.2.0 [**Computer-Communication Networks**] General – *Security and protection (e.g., firewalls).*

Keywords

Cyber-Physical Systems (CPS); CPS security; Cyber-Physical Attacks; cross-domain attacks; taxonomy.

1. INTRODUCTION

Currently, we are in the middle of an emergence of Cyber-Physical Systems (CPS) in almost all aspects of our life. Examples of CPS are manifold and include all kinds of unmanned or remote controlled vehicles, robotized manufacturing plants, critical infrastructure such as electrical power grid and nuclear power plants, smart homes, smart cities, and many more. Based on our experience with computer and network security, CPS will become targets of adversary attacks.

Attacks on CPS are neither science fiction nor the matter of the distant future. Multiple attacks on various CPS have been already performed. Currently, the most famous attack is Stuxnet. Stuxnet is considered to be the first professionally crafted attack against CPS. This attack has reportedly damaged over 1000 centrifuges at an Iranian uranium enrichment plant [1]. Multiple further examples of attacks on various CPS have been reported or shown in the research literature. These include attacks on modern car electronics [2], attacks on remotely controlled UAVs via GPS spoofing [3], or even attacks which use CPS as a carrier to infect the maintenance computer [4].

There is a broad consensus among researchers that adversary goals of attacks on CPS might differ from the goals of attacks on cyber systems. For instance, many attacks on CPS would try to compromise the system's safety or physical integrity instead of data privacy usually considered in cyber-security.

However, technical aspects have even more severe implications on the CPS security. Figure 1 depicts various attacks which can be performed at targets located at different system layers. It is clear that attacks will affect the attacked targets. Additionally, due to the high degree of the dependencies and interdependencies between CPS elements at different layers, secondary effects can occur at CPS elements which have not been directly attacked. These induced effects can occur at elements located in different layers or even belonging to different (cyber or physical) domains. Such cross-layer and cross-domain attacks on CPS are very intricate and barely understood so far. Below, we will use qualifier "cross-domain" as a synonym for both cross-domain and cross-layer.

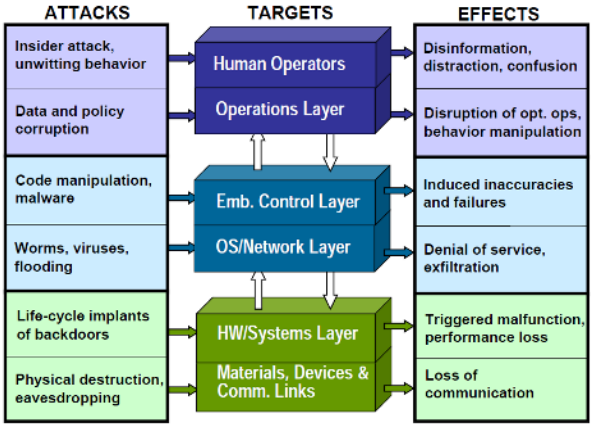

Figure 1. Layer Specific Attacks on CPS [12]

HiCoNS'13, April 9–11, Philadelphia, Pennsylvania, USA.

Surveying known attacks on CPS, one can notice that a significant portion exhibits cross-domain effects. This makes it extremely important to consider such attacks alongside with the conventional cyber-attacks. In order to do this, we first should be able to describe not only the single-domain but also cross-domain attacks.

Our contribution in this paper is as follows. We propose a taxonomy for description of attacks on CPS. The proposed taxonomy is capable of representing both conventional cyber-attacks as well as cross-domain attacks on CPS. Furthermore, based on the proposed taxonomy we define an attack categorization. Numerous examples illustrate the application of the proposed taxonomy for the attack description. Moreover, we provide an extensive discussion of possible taxonomy application areas. During this discussion we explain how the proposed taxonomy can be used for attack documentation, vulnerability assessment, and description of attack propagation.

The reminder of this paper is structured as follows. After discussing the state of the art regarding CPS security and cyber-security taxonomies in Section 2, we propose a novel taxonomy for description of attacks on CPS in Section 3. We discuss the taxonomy application areas in Section 4. We conclude this paper with the outline of our future plans and a short review in Sections 5 and 6 respectively.

2. RELATED WORK

We consider both known attacks on CPS and taxonomies elaborated in the cyber-security for classification and description of attacks on computer systems and networks.

2.1 Known Attacks on CPS

Compared to the vast amount of attacks on computer systems and networks we have faced in the last decades, the amount of attack on CPS is quite limited. Nevertheless, a fair amount of attacks on different kinds of CPS is known, including attacks on critical or industrial infrastructure, transportation systems, and remote controlled unmanned vehicles.

2.1.1 Critical or industrial infrastructure

Currently, the most famous attack on CPS is the Stuxnet [1], [5]. Stuxnet is considered to be the first professionally crafted attack on an industrial infrastructure. It contains very sophisticated techniques to infect targeted systems, to spread infection, and to evade its detection. However, from the cross-domain attack point of view, probably the most notable aspect of Stuxnet is the fact that it inflicts physical damage to the industrial infrastructure via manipulations in cyber-space.

However, it is wrong to assume that the Stuxnet was the only or even the first attack on CPS. According to [6], attacks on various industrial or critical infrastructures can be traced back as far as 1995. In [6], based on the analysis of 41 known security incidents in industrial control systems, authors present the attack trends. Whereas before 2001 most of the attacks were internal, i.e., carried out by company members, after 2001 the vast majority of the attacks are of external nature.

According to [7], the reasons for the growing vulnerability of CPS to various kinds of external cyber-attacks can be attributed to two main factors: urge to interconnect all devices and the usage of off the shelf solutions such as operating systems and network protocols.

A very good overview of various cyber-attacks on critical infrastructure can be found in [13]. From the cross-domain perspective, an attack on Maroochy Water Services on Queensland's Sunshine Coast in Australia is especially relevant for our discussion. In March 2000, a cyber-attack caused severe disruptions of this plant, including disruption of proper pump operation, suppression of alarms, and even releasing of untreated sewage into local waterways [14].

Additionally to the description real of security incidents, it became very common to discuss the implications of potentially possible attacks on critical infrastructure, such as electrical power grid, or national gas distribution system. Especially notable is the existence of various interdependences between various critical infrastructures. In [11], following four classes of interdependencies between critical infrastructures have been identified: physical, cyber, geographical, and logical. Because of these interdependencies, effects of an attack can propagate through different domains and inflict secondary damage to further infrastructure.

2.1.2 Transportation systems

Modern transportation systems, such as cars or airplanes, can be seen as CPS because they embody numerous embedded systems controlling various physical components. Among others, these systems are responsible for auto piloting, controlling of fuel injection and ABS, releasing airbags, etc. The controlling part of these functionalities is realized via millions of lines of code executed on tenths to hundreds internetworked Electronic Control Units (ECUs) [15]. Furthermore, the communication between ECUs is increasingly realized via wireless communication. The vulnerabilities of both running software and network communication to various attacks have had been extensively studies in cyber-security. Additionally, ECUs can be compromised by hardware Trojans. The detection of such Trojans is a very hard problem [21]. Regardless of how a control over a part of a CPS has been gained, it opens possibilities for numerous follow-up attacks.

There are numerous research papers describing experimental attacks on modern vehicles. For instance, in [2], the authors present a sequence of cyber-attacks executed on modern car's electronics. They experimentally show how attacks on ECUs can be prepared and performed, enabling execution of various cross-domain attacks endangering the safety of the car occupants. For instance, they have shown that it is possible to disable breaks, kill car engine during driving at a high speed, permanently lock the doors, manipulate speed indication, etc.

2.1.3 Remote controlled unmanned vehicles

Due to their proliferation, unmanned vehicles increasingly move into the focus of security concerns. In the recent years there were numerous reports that even military Unmanned Aerial Vehicles (UAVs) can become victims of cyber-attacks. From the cyber-security perspective, the example reported in [8] shows that a virus can spread even in a highly controlled environments, such as a military air base. In this example, the infection has been spread between vehicles through removable drives used for mission data updates. As it has been shown in [2], the infection of CPS can be used to perform cross-domain attacks and thus producing devastating consequences in physical domain.

It has been experimentally shown that a UAV can be hijacked by spoofing a GPS signal [3]. According to [13], such attacks can be

classified as attack on the estimation algorithms. In the physical domain, such location estimation errors can lead to collisions, which, in turn, can cause physical damage of UAV and/or object it collides with.

Even though focusing on SCADA networks, the authors in [16] make very important observation that real-time operating systems (RTOS) "may be more susceptible to DoS attacks because even minor disruptions in device operation can lead to a significant loss of system availability in a real-time application." Applied to unmanned or remote controlled CPS, such susceptibility can also lead to consequences in the physical domain, e.g., because collision could not be avoided.

In [4], we have analyzed which attacks can be performed on a remotely controlled UAV via cyber means only. We have identified numerous effect propagation chains breaking out from the cyber into physical domain. It is remarkable that about a third of all identified attacks have shown domain crossing property. During the analysis, we have faced the problem that it was not possible to describe those cross-domain attacks with the means available in cyber-security. This experience has motivated our present work.

2.2 Attack Taxonomies in Cyber-Security

In network and computer security, taxonomies have been successfully used for single category classification, multi-dimensional characterization, attack description, and even for identification of new possible attacks. Several criteria for taxonomy have been elaborated, such as unambiguity, or mutually exclusiveness. However, as pointed out in [17], not all taxonomies should fulfill every listed criterion. For instance, not all taxonomies strive to be mutually exclusive.

2.2.1 Single category classification

There is a number of very good classification taxonomies proposed for various kinds of cyber-attacks. We have analyzed these taxonomies because most (if not all) attacks on computer systems and networks can be applied to CPS as well.

Classification taxonomies tend to focus on a particular aspect of cyber-security. For instance, in [18] the author focuses on the information security in wireless communication. The following attack classification groups are given: traffic analysis, active eavesdropping, unauthorized access, man-in-the-middle, session hijacking, and replay attacks.

Most of classification taxonomies we have analyzed do not take into account anything but cyber domain properties. However, there are also several classification taxonomies that consider physical domain properties. For instance, in [9] the authors present a taxonomy of attacks on embedded systems in Venn diagram form. This taxonomy distinguishes between the pure cyber-domain "logical" and cross-domain "physical and side channel" attacks. Even though the considered goals of such attacks are always within the cyber domain, techniques like power or electromagnetic analysis incorporate measurements in the physical domain.

2.2.2 Multi-dimensional characterization

Categorization of an attack in a single category is not always possible or reasonable. In some cases it is reasonable to characterize an attack based on a combination of multiple properties. Several taxonomies pursue this approach, organizing these properties as top-level tree elements. The elements in sub-trees are used to classify the attack within every dimension (similar to the single category classification described above).

The taxonomy for the characterization of computer worms proposed in [10] consists of the following dimensions: target discovery, distribution mechanism, activation, payload, and motivation. This taxonomy consists of two levels. For instance, for the distribution mechanism it lists following classification options: self-carried, second channel, and embedded.

The taxonomy presented in [19] is designated to characterize hardware Trojans. The top-level categories are physical characteristics, activation characteristics, and action characteristics. The overall tree has a slightly more complex structure as the sub-trees are of different depth. However, from our perspective, most interesting is the fact that the tree elements can characterize both cyber and physical properties.

Another example of taxonomy covering both cyber and physical aspects is presented in [11]. The authors focus on interactions and interdependencies between different critical infrastructures. The proposed taxonomy consists of six dimensions: Environment, Coupling and Response Behavior, Type of Failure, Infrastructure Characteristics, State of Operation, and Type of Interdependencies. Authors identify four types of interdependencies between critical infrastructures: Physical, Cyber, Logical, and Geographical.

2.2.3 Multi-dimensional description

Finally, there are taxonomies used for the description of attacks. Similar to the multi-dimensional characterization, they usually specify attack properties which have to be described. However, in contrast to the above outlined taxonomies, no fixed list of possible values is specified for these dimensions. Such taxonomies are required in bodies like CERT to describe newly discovered attacks, because often the categories within dimensions have to be extended.

A good example of such taxonomy is given in [17]. The authors discuss the characteristics of cyber-attacks and conclude that a tree-like taxonomy does not suit well to describe them. Instead they propose to describe attacks based on four dimensions: attack vector (i.e., method by which an attack reaches the target), attack target, exploited vulnerability, and additional payload or effect beyond the attack themselves. Although the authors propose several multi-level extensible categorizations within these dimensions, these are supposed to be extendible on demand.

3. TAXONOMY

Summarizing the related work presented in Section 2, there are several known attacks on CPS. However, their description mostly focuses on cyber means used to perform these attacks and tend to overlook the attack's cross-domain aspects. This provides us some knowledge but not really deep insights into cross-domain attacks. However, elaboration of a single category classification or multi-dimensional categorization taxonomy requires both broad amount of data about and deep insights into properties of attacks. As we currently have neither of them, a solution is to develop taxonomy for description of attacks on CPS.

In this section, we first propose a six-dimensional taxonomy for description of attacks on CPS. For every taxonomy dimension we describe its semantics. Based on the domain affiliation of two of these dimensions, we then introduce a categorization for various attacks on CPS.

3.1 Taxonomy Dimensions

In cyber-security, it is common to consider that an attack (action) on a target element (subject) causes effects on this element (state change). As this view considers only a single subject, which can belong either to cyber or to physical domain, no cross-domain attacks can be described.

In our proposal, we keep *Targets*, *Elements*, and *Attacks* as a top-level abstraction for three groups of taxonomy dimensions (see Figure 2). However, we propose an important redefinition of their semantics. An attack still can be viewed as an action, but we distinguish between *Attack Means* and *Preconditions* for these means to be successful. The Targets group contains both element(s) immediately influenced by an attack (subject) as well as the immediate influence (state change). We use the Effects group to describe effects induced by changes described in the group Targets. Similar to the Targets group, the Effects group contains *Victim Element* (subject) and *Impact on Victim* (state change) dimensions. Please note that this induction of Effects is caused by the high degree of dependencies and interdependencies between CPS components. In this paper, we focus on the description of the cause-effect relationships.

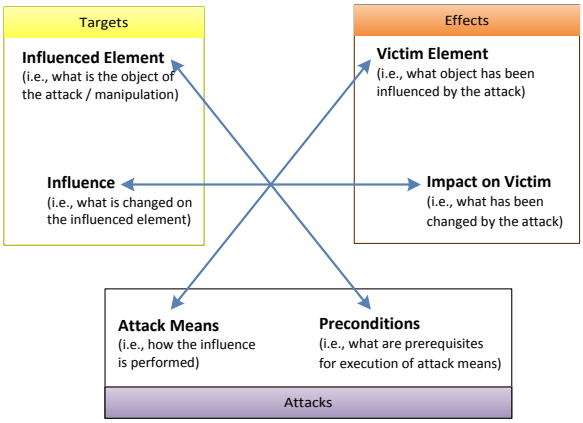

Figure 2. Taxonomy of Cyber-Physical Attacks

More formally, the semantics of every taxonomy dimension is defined as follows:

- **Influenced Element** describes the object that is manipulated by an attack. This element can reside in cyber or physical domain. It can be either an integral part of CPS or be part of cyber or physical environment CPS is interacting with.

- **Influence** describes the manipulation on the Influenced Element. In the case of an active attack on an element in the cyber domain, it can be the change of the element's state. If the influenced element belongs to the physical domain, influence describes the change of its physical property, e.g., temperature, or Signal to Noise Ratio (SNR). In the case of a passive attack, it can describe the fact of having knowledge about the element's state. Note that this dimension does not describe the means of the manipulation, but only the manipulation by itself. In other words, we distinguish between "what is done" (influence) and "how it is done" (means).

- **Victim Element** can be seen as a counterpart of the Influenced Element dimension. It can but should not necessarily be the same element. These elements can but should not necessarily belong to the same (cyber or physical) domain. Finally, these elements can but should not necessarily be at the same system layer or level of abstraction. The distinction between influenced and victim element is as follows: whereas the influenced element is directly manipulated by an attack, the victim element becomes manipulated via interactions existing in CPS.

- **Impact on Victim** is the counterpart of the Influence dimension. It describes the impact on the Victim Element. In the case of an active attack, it can be a change of the element's state or its physical property. In the case of a passive attack, it can describe the change of the knowledge about Victim Element. Please note that, in general, even a single Influence on a single Influenced Element can cause one or more Impact(s) on one or more Victim Element(s).

- **Attack Means** defines how the manipulation on the Influenced Element has been performed. Note that, in general, various means might exist to achieve the same influence on the same element.

- **Preconditions** dimension defines conditions under which Attack Means will lead to the consequences described in Effects dimensional group. Note that for the accomplishment of a particular Attack Means the fulfillment of several preconditions might be required. Therefore, this can take a form of a logical expression over state of one or more elements, existing vulnerabilities, and adversary knowledge.

We would like to illustrate the semantics of the proposed taxonomy dimensions describing the core of Stuxnet – a cross-domain attack, which is designated to inflict physical damage to centrifuges. However, the immediate effect of this attack is that the attacked centrifuge rotated with the speed exceeding its designated operational range (see Table 1). Note that this particular attack generates multiple impacts on the victim element.

Table 1. Cross-domain attack in Stuxnet

Influenced Element: ▪ Centrifuge motor rotation controlling process	**Victim Element:** ▪ Centrifuge
Influence: ▪ Frequent changes of designated rotation speed between values below and above operational range	**Impact on Victim:** ▪ Rotation with speed outside of the specified boundaries ▪ Frequent changes of rotation speed ▪ Excessive vibrations
Attack Means: ▪ Send commands from the infected Programmable Logic Controller (PLC) to the centrifuge motor controller with the modifications of the designated rotation speed	
Preconditions: ▪ PLC infected by Stuxnet	

3.2 Attack Categorization

The most significant feature of the proposed taxonomy is the clear distinction between Influenced Element and Victim Element. As both these dimensions are independent from each other, elements of these dimensions can belong to cyber or physical domain regardless of the domain affiliation of each other. Therefore, the description of cross-domain attacks becomes possible.

Furthermore, based on the domain of these elements, we can define following four attack categories: Cyber-to-Cyber (C2C), Cyber-to-Physical (C2P), Physical-to-Physical (P2P), and Physical-to-Cyber (P2C). These derivatives (see Figure 3) can be used to characterize attacks.

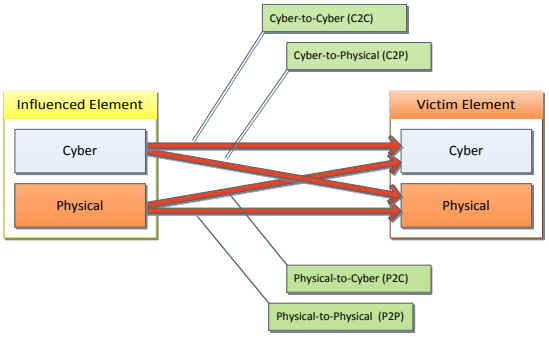

Figure 3. Characterization of attacks on CPS

In the Stuxnet's cross-domain attack presented in Table 1, the Influenced Element belongs to the cyber domain and the Victim Element belongs to the physical domain. Therefore, this attack can be characterized as a C2P attack. Currently, this category of attacks is the least understood one.

Table 2. Buffer overflow attack

Influenced Element: ▪ Running process	**Victim Element:** ▪ The same process
Influence: ▪ Corruption of stack	**Impact on Victim:** ▪ Process ether crashes or executes injected malicious code (depends on injected payload)
Attack Means: ▪ Buffer overflow attack: send to the process more data than it expects under normal conditions	
Preconditions: ▪ Unguarded buffer boundary ▪ No W-xor-X Memory Protection[1]	

Cyber security focuses on C2C attacks, i.e., attacks with both Influenced and Victim Elements residing in cyber domain. Examples of such attacks are manifold and include buffer overflow, Denial of Service (DoS), man in the middle, and many other attacks. The C2C attacks have been intensively investigated for many years; they are comparatively well understood. In cyber-security, multiple methods have been elaborated for C2C attack prevention, detection, and mitigation. The description of the buffer overflow attack is presented in Table 2. Depending on the abstraction level of description, Influenced Element can be ether a running process or its stack. The Victim Element of this attack is the running process. As both elements belong to cyber domain, this attack can be categorized as C2C.

We have defined P2P attack as an attack with both Influenced and Victim Elements located in the physical domain. Despite the name similarity with the cyber security, physical security does not considers P2P attacks. Instead, it focuses on restricting physical access by unauthorized personnel to the equipment. Nevertheless, P2P attacks still can be seen as a well understood area, e.g., in material science which covers the wear of physical component under influence factors like speed, temperature, or vibration.

P2P attacks can either be executed by Attack Means manipulating Influenced Element, or as a consequence of Impact caused by some other attack. For instance, the immediate impacts of the Stuxnet's C2P attack described in Table 1 are excessive vibrations and rotation with speeds exceeding the normal operational range. These, in turn, can lead to accelerated wear (and thus to the reduction of life time) of centrifuge components and even to its irreparable physical damage (see Table 3). Please note that not all effects on the Victim Element of the original C2P attack cause effect propagation. Further, describing the effect propagation we don't have to specify Attack Means. However, it should not always be the case for Preconditions, as they can specify constraints under which the effect propagation is possible.

Table 3. P2P Effect Propagation

Influenced Element: ▪ Centrifuge	**Victim Element:** ▪ Centrifuge
Influence: ▪ Rotation with speed outside out of the specified boundaries ▪ Excessive vibrations	**Impact on Victim:** ▪ Reduced life time ▪ Physical damage
Attack Means: ▪ N/A	
Preconditions: ▪ N/A	

The security perspective of P2C effect propagation has been studied within the embedded system security. In this context, so called side-channel attacks use physical domain information in order to compromise the privacy of cyber domain. Applied to CPS, this principle can be used, e.g., for analysis of the used communication protocol. In Table 4 an attack is described which correlates the eavesdropped communication between a Remote Control (R/C) and the controlled UAV with the physical reaction of the UAV. This example presents a passive attack. Therefore, Influence describes the knowledge about Influenced Elements.

Concluding, with the exception of C2P all other categories of attacks have been more or less intensively studied. Unfortunately, all these categories have been studied independently of each other within different disciplines. However, in CPS we face the potential presence of all four attack categories. With the examples we have illustrated how the proposed taxonomy can be used to describe all four categories of attacks on CPS, i.e., C2C, C2P, P2P, and P2C.

[1] This protection mechanism is not effective against the Return Oriented Programming (ROP).

Table 4. Protocol Analysis

Influenced Element: ▪ R/C to UAV Communication ▪ UAV Reaction	**Victim Element:** ▪ Communication protocol
Influence: ▪ Knowledge: R/C ⇔ UAV communication ▪ Knowledge: UAV movement [changes]	**Impact on Victim:** ▪ Inform. Disclosure: Command Meaning
Attack Means: ▪ Correlation of eavesdropped communication and UAV's physical reactions	
Preconditions: ▪ Statistically unique correlation possible	

4. APPLICATION AREAS

We see several application areas of the proposed taxonomy. In this section, we will outline three application areas which we consider as the most important: structured representation of attacks described in the literature, CPS vulnerability analysis, and representation of attack propagation.

4.1 Attack Documentation and Analysis

The most intuitive application of the proposed taxonomy is the structured representation of attacks on CPS described in the literature. Currently, without such structure, the comparison between attacks described in various case studies is very complicated and time consuming. Among others, it is very difficult to verify whether the described attack is a principally new one or just an already known attack applied to another CPS. Furthermore, for new attacks it is also important to understand what exactly is new. For instance, whether it is a new Attack Means which can be used to produce already known Influence on some Influenced Element, or whether it is a new to date not documented relationship between some Influence on an Influenced Element and the Impact on the Victim Element. For instance, in [2] and in [4] protocol analysis attacks are described (see also Table 4 and the corresponding description). These attacks differ solely in Influenced Elements, information about which is correlated.

Description of attacks from different case studies according to the same structure has several further advantages. This will enable the development of a catalogue listing known attacks on CPS in a similar structured manner. We consider such catalogue as a necessary prerequisite for further advances in the understanding of attacks on CPS. Most importantly, it will enable qualitative and quantitative analysis of known attacks.

Based on the qualitative analysis, it should be possible to identify elements in every dimension. Furthermore, we expect that the knowledge about and the analysis of these elements will enable construction of tree-like singe category classification taxonomies of elements belonging to particular dimensions. We expect that taxonomies elaborated in cyber-security can be integrated as parts of these "taxonomies within dimensions." This process can potentially transform our current proposal to multi-dimensional characterization taxonomy. Such knowledge is extremely important for the CPS vulnerability assessment, as it will provide the basis for the analysis whether CPS is susceptible to particular kind of manipulation or not.

The qualitative analysis is helpful to identify which elements within different dimensions are more common in different attacks. Such information is extremely important for assigning probabilities for different manipulations to occur. Such probabilities can be used, e.g., to compute comparable security grades of different CPS designs and/or configurations.

4.2 CPS Vulnerability Analysis

The common way to improve the system's security is to perform its vulnerability assessment and to make a cost-effective decision regarding which elements should be improved. The proposed taxonomy provides a good basis for both these tasks.

The taxonomy dimensions Influenced Element, Attack Means, and Preconditions are well known in cyber-security. For instance, it is common to analyze whether the network components or computers (i.e., Influenced Elements) are configured in the way (i.e., Preconditions) that it makes them susceptible to different attacks (i.e., Attack Means). This approach is also applicable to CPS. Especially in conjunction with the knowledge base containing information about possible attacks, the vulnerability assessment of a CPS model can become automated. Similar vulnerability assessment procedures for computer networks have been proposed in the literature, e.g., in [20].

Additionally, through distinction between dimensions within Targets and Effects groups, we foster the analysis of dependencies and interdependencies between Influenced Element and Victim Element(s) within a particular CPS. Please note that these dependencies can vary to a high extent between different CPS. Nevertheless, there are numerous modeling tools capable to compute with high accuracy which Effects can be caused, e.g., by increasing temperature or rotation speed of a particular Influenced Element of a CPS. The combination of the common cyber-security approach for the vulnerability assessment with the understanding of the cause-effect relationships existing in a CPS can result in an approach for the CPS vulnerability assessment.

Finally, it is common to weight the costs of measures for the security improvement against the costs which can be inflicted by an attack if these measures are not installed. Victim Element and Impact on Victim dimensions provide the basis for the analysis of costs of a successful attack. For instance, comparing two attacks described in [2], the attack capable of "killing" the engine can be seen as more severe (and more costly) than the one which permanently locks doors. Of course, these costs should be considered in conjunction with the probability of such Impact on the Victim Element to occur. The later can be computed based on the probabilities of all attacks leading to these Effects. As we have mentioned in the previous subsection, such probabilities can be derived based on the quantitative analysis of attacks described in the literature.

4.3 Attack Propagation and Encapsulation

As mentioned before, every CPS is a very complex heterogeneous system with multiple dependencies and interdependencies between its components. Therefore, an attack can take different paths how it influences the system, including cross-domain and cross-layer attacks. This makes the relationship between different sequences of attack steps and/or effect propagation stages much more complex and diverse than it is the case in the cyber systems. The proposed taxonomy is sufficient to capture various kinds of attack propagation and thus provides the basis for their analysis.

On the example of the Stuxnet attack we have already presented how the stages of the effect propagation can be described (see Table 1 and Table 3). It shows that elements of Victim Element and Impact on Victim can be "reused" as elements of Influenced Element and Influence in the induced attack. Please note that such cause-effect propagation chains are possible in all categories of attacks, and not only in P2P attacks.

Another kind of attack propagation is distinctive to complex attacks executed as a sequence of multiple stages. In the car case study [2], an infected Electronic Control Unit (ECU) spreads infection in two stages. In the first stage, it sends to a target ECU a request to enter the reprogramming mode. As no protection mechanisms is implemented, such as Authentication and Authorization (AA) of the command's issuer, the target ECU enters this mode (see Table 5).

Table 5. Entering Reprogramming Mode

Influenced Element: ▪ Attacked ECU	**Victim Element:** ▪ Attacked ECU
Influence: ▪ Receive request to enter reprogramming mode	**Impact on Victim:** ▪ Stops code execution ▪ Enters new state: reprogramming mode
Attack Means: ▪ Send command to the attacked ECU via CAN bus	
Preconditions: ▪ Target ECU is reprogrammable ▪ No physical access needed to enter this mode ▪ No AA protection for command verification	

From the attack propagation perspective, the first stage enables certain preconditions required for the second stage of this attack. In the particular case, the goal of the second stage is to reprogram the target ECU with a malicious code (see Table 6).

Table 6. Reprogramming ECU with a Malicious Code

Influenced Element: ▪ Attacked ECU	**Victim Element:** ▪ Attacked ECU
Influence: ▪ Receive new code to update ECU	**Impact on Victim:** ▪ Malicious code burned in ECU flash memory ▪ After burning and reboot, malicious code is running
Attack Means: ▪ Send new program code to the attacked ECU via CAN bus	
Preconditions: ▪ ECU current state: reprogramming mode ▪ No code verification mechanisms are implemented	

Additionally, we would like to discuss the reusability of the attack description. This is especially important because basic attacks can be used in numerous more complex attacks. The proposed taxonomy is capable to cope with the attack encapsulation too. Let us assume that the attack described in Table 5 has the unique ID `#koscher10-enter-reprogram-mode`. In this case one or more effects of this attack can be used to describe influenced element and influence of the more complex attack, the unique attack ID can be used as attack means causing these influences (see Table 7).

As shown in [2], this attack is even possible during car is driving at high speed. It is self-evident that if this attack is executed on a highway, it can cause a severe car accident. From the attack description perspective, we use this to show that this is possible to "fold" the exact effect propagation sequence in the attack description. Instead of description of the detailed effect propagation stages (i.e., if motor ECU enters reprogrammable state motors stops rotating, therefore car stops, therefore collisions become possible) it is possible to describe only relevant effects of the original attack.

Table 7. Reusability of attack

Influenced Element: ▪ Motor ECU	**Victim Element:** ▪ Motor ▪ Car ▪ Environment
Influence: ▪ Enter reprogramming mode	**Impact on Victim:** ▪ Motor: Stops rotating ▪ Car: stops ▪ Car & Environment: collisions, injuries
Attack Means: ▪ #koscher10-enter-reprogram-mode	
Preconditions: ▪ No command prevention during driving at high speed	

5. FUTURE WORK

We have analyzed the applicability and the limitations of the proposed taxonomy by describing attacks from three different case studies, the Stuxnet attack on industrial infrastructure [5], attacks on modern car [2], and attacks we have identified during the vulnerability assessment of a quad-rotor UAV [4].

In all these case studies, we have been able to represent both conventional cyber as well as CPS specific cross-domain attacks. Moreover, it was also possible to describe attacks which change the abstraction layer, e.g., between CPS element and the whole CPS. It is further possible to describe interactions with and impact on objects of CPS environment.

However, we have also faced several limitations of the proposed taxonomy. Most noticeable, although the proposed structure is suitable to capture all relevant information we could think of, the meta-information such as relationships between elements of different dimensions cannot be expressed intuitively. For example, in many cases an attack will generate multiple impacts on one or more influenced elements[2]. Furthermore, the cardinality relationship between different dimensions can vary to high extent between different attacks. Therefore, we are currently working on definition of *Cyber-Physical Attack Description Language* (CP-ADL). This is the natural extension of the proposed taxonomy. CP-ADL should be able to reflect meta-information such as relationship between dimensional elements. Additionally, this language should be useful for the storage of attack descriptions as

[2] We have presented one such example in Table 7. Another example with similar issues is jamming, which is nothing else but Influence on communication medium property (in physical domain) which leads to multiple Impacts at all network layers (in cyber domain). Even though the description of multiple pairs of Victim Element and Impact on Victim is possible, correlation between these elements described in a table form is not easy.

well as for the export of such information to other tools, e.g., for the automatic vulnerability assessment.

Another direction we consider for our future work is the automation of CPS vulnerability assessment. In [4] we have presented a systematic approach for the manual vulnerability assessment. As it has been successfully shown, e.g., in [20] for computer networks, an automatic vulnerability assessment is possible if the system model and the database of known attacks are available. However, we see the automatic vulnerability assessment rather as a plan for the distant future because first we have to understand which properties have to be reflected in the CPS model as well as to develop and to populate the knowledge base of known attacks on CPS.

6. CONCLUSION

Cyber-Physical Systems become increasingly embedded in our life. As we have seen through several examples, CPS are exposed to various kinds of attacks. Most noticeable, as CPS consist of highly interdependent components in both cyber and physical domains, attacks crossing this domain boundary become possible.

In this paper, we have proposed taxonomy for the structured description of cross-domain attacks on CPS. This taxonomy consists of six semantically clear distinct dimensions. We have illustrated the application of this taxonomy on numerous examples. We see our proposal as a first step on the way to the better understanding of cross-domain attacks and thus to the improvement of the CPS security. In this context, we have provided an extensive discussion of possible taxonomy application areas.

ACKNOWLEDGEMENT

This work is supported in part by the National Science Foundation (CNS-1035655), U.S. Army Research Office (AROW911NF-10-1-0005) and Lockheed Martin. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

REFERENCES

[1] Albright, D., Brannan, P., Walrond, C. 2010. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? In *Institute for Science and International Security* (ISIS) *report*.

[2] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., Savage, S. 2010. Experimental security analysis of a modern automobile. In *Proceedings of Symposium on Security and Privacy* (SP), 447-462.

[3] Shepard, D. P., Bhatti, J. A., Humphreys, T. E., & Fansler, A. A. 2012. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks.

[4] Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. 2012. Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In *Proceedings of the 5th International Symposium on Resilient Control Systems* (Salt Lake City, Utah, August 14-16m 2012), 55-62.

[5] Falliere, N., Murchu, L. O., & Chien, E. 2011. W32. stuxnet dossier. *White paper*, Symantec Corp., Security Response.

[6] Byres, E., & Lowe, J. 2004. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116).

[7] Levy, E. 2003. Crossover: online pests plaguing the off line world. In *Security & Privacy*, 1(6), 71-73.

[8] Shachtman, N. 2011. Computer Virus Hits US Drone Fleet. In CNN.com.

[9] Ravi, S., Raghunathan, A., Kocher, P., & Hattangady, S. 2004. Security in embedded systems: Design challenges. In *ACM Transactions on Embedded Computing Systems*, 3(3), 461-491.

[10] Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. 2003. A taxonomy of computer worms. In *Proceedings of the 2003 ACM workshop on Rapid malcode*, 11-18.

[11] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. In *Control Systems*, 21(6), 11-25.

[12] Sztipanovits, J. 2012. Towards Science of System Integration for CPS. Keynotes at *The 1st ACM International Conference on High Confidence Networked Systems* (HiCoNS)

[13] Cárdenas, A. A., Amin, S., & Sastry, S. 2008. Research challenges for the security of control systems. In *Proceedings of the 3rd conference on Hot topics in security*, 1-6.

[14] Slay, J., & Miller, M. 2007. Lessons learned from the maroochy water breach. In *Critical Infrastructure Protection*, 73-82.

[15] Charette, R. N. 2009. This car runs on code. In *IEEE Spectrum*, 46(3), 3.

[16] Wang, J., & Yu, X. 2007. Security strategies for SCADA systems. In *Recent advances in security technology*, 378.

[17] Hansman, S., & Hunt, R. 2005. A taxonomy of network and computer attacks. In *Computers & Security*, 24(1), 31-43.

[18] Welch, D., & Lathrop, S. 2003. Wireless security threat taxonomy. In *Information Assurance Workshop*, 76-83.

[19] Rad, R. M., Wang, X., Tehranipoor, M., & Plusquellic, J. 2008. Power supply signal calibration techniques for improving detection resolution to hardware Trojans. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, 632-639.

[20] Lippmann, R. P., Ingols, K. W., Scott, C., Piwowarski, K., Kratkiewicz, K. J., Artz, M., & Cunningham, R. K. 2005. *Evaluating and strengthening enterprise network security using attack graphs*. Project report.

[21] Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P., & Sunar, B. 2007. Trojan detection using IC fingerprinting. In *Proceedings of Symposium on Security and Privacy*, 296-310.