Considering internal vulnerabilities and the attacker's knowledge to model the impact of cyber events as geometrical prisms

Gustavo Daniel Gonzalez Granadillo, Jose Rubio-Hernan, Joaquin Garcia-Alfaro, Hervé Debar

Considering internal vulnerabilities and the attacker's knowledge to model the impact of cyber events as geometrical prisms

Gustavo González-Granadillo, José Rubio-Hernán, Joaquin Garcia-Alfaro, Hervé Debar
Institut Mines-Telecom, Telecom Sudparis, SAMOVAR UMR 5157
9 rue Charles Fourier, 91011 EVRY, France
{name.last_name@telecom-sudparis.eu}

***Abstract*—We propose a model to represent graphically the information system and the impact of cyber events (e.g., attacks, countermeasures) as a prismatic instance of n-sides. The approach considers information about all entities composing an information system (e.g., users, IP addresses, communication protocols, physical and logical resources, etc.), as well as information about the attacker's knowledge, motivation and capabilities. The base of the prism is represented as an n-side polygon (e.g., triangle, square, pentagon, etc.) which depicts the internal information of the system, whereas the height of the prism is represented as a single axis which depicts the external information of the system. We propose geometrical operations to determine the impact of cyber security events (i.e., area, volume, event coverage, residual risk, and potential collateral damages). A case study is proposed at the end of the paper to show the applicability of the model in a scenario with multiple attacks.**

I. Introduction

Computing the economic impact of cyber security events is an open issue in the ICT domain. Specialized information security organizations e.g., Computer Emergency Response Team (CERT) [1], Ponemon Institute [2], Verizon [3], etc., perform annual reports on such estimations based on real-world experiences and in-depth interviews with thousands of security professionals around the world. The research is designated to help organizations make the most cost-effective decisions possible in minimizing the greatest risk to their organizations.

A range of difficult issues confront the assessment of the impact of cyber events. (i) Accuracy, the risk of potential threats cannot be accurately described unless their consequences are properly identified and quantified. (ii) Collateral damage, while impact models provide an assessment of the risk and estimation of the economic impact over the target system, most of them fail at considering propagation and side effects in their evaluations. (iii) contextual criteria, impact models generally evaluate the impact on assets, neglecting the analysis of impacts and resulting responses with respect to time, geographic space, and affected populations [4].

Previous researches propose simulation models [5], [6] and geometrical models [7], [8] to estimate and analyze the impact of cyber events. However, most of the proposed solutions are limited to three dimensions, making it difficult to provide a graphical representation of geometrical instances in four or more dimensions.

Furthermore, most of the solutions proposed to estimate the impact of cyber security events do not consider information from the attacker's side (e.g., knowledge, motivation, capabilities, etc.). A wide variety of adversary models are proposed in the literature [9]–[12]. The knowledge of such adversaries can be either prior to the attack (a priori) or after the attack is executed (a posteriori).

In this paper, we propose a geometrical model to calculate the impact of cyber events as n-sided prisms. The approach considers information about all entities composing an information system (e.g., users, IP addresses, communication protocols, physical and logical resources, etc.), as well as contextual information (e.g., temporal, spacial, historical conditions), and the attacker's information (e.g., knowledge, motivation, skills, etc.), to plot cyber attacks and countermeasures in a geometrical system. The ultimate goal of our model is to help organizations make the most cost-effective decisions in minimizing the risk of the studied cyber events.

In addition, we are able to perform geometrical operations (e.g., area, volume) over the prismatic instances, which allows us to compare the impact of multiple cyber events. Such comparison provides the means to compute the coverage of events with respect to the system, the residual risk, and potential collateral damage that may occur out of the implementation of the security countermeasures.

The contributions on this paper are summarized as follows:

- A qualitative and quantitative assessment of the impact of cyber events (e.g., attacks, countermeasures) based on the target's information and the attacker's knowledge.
- A model that projects the impact of security events in an n-sided geometrical system. The instances resulting from the model are regular or irregular prisms (e.g., triangular prisms, quadrilateral prisms, pentagonal prisms, etc).
- A process that performs geometrical operations to calculate the size of the prismatic instances (i.e., area, volume), which allows us to compare the impact of multiple cyber events.
- A process that computes the coverage of events (COV), the residual risk (RR), and potential collateral damage (PCD) that may occur out of the implementation of the security countermeasures.

- The deployment of our model in a case study with multiple security events over several dimensions.

The rest of the paper is structured as follows: Section II introduces the cyber event information required to build the instances and analyze their impact. Section III presents our proposed prismatic model and discusses about its construction. Section IV details the main prismatic instances that result from our model. Section V details the impact measurement of the different geometrical instances. Section VI presents a case study with multiple events (e.g., attacks and countermeasures) to illustrate the applicability of our approach. Related work are presented in Section VII. Finally, conclusions are presented in Section VIII.

II. Cyber Event Information

For the scope of this article, we consider sets of individual actions performed either by the attacker (e.g., malicious actions executed in order to exploit a system's vulnerability) or by the target system (benign actions executed as a response to an adversary) as a cyber security event.

Internal and external information are required to analyze the impact of a cyber security event. Internal information represents all physical and logical data from the local network or from the information system, such as assets, vulnerabilities, defense mechanisms, etc. External information is related to the attacker's knowledge, motivation, and capabilities to exploit a given vulnerability from the target system. This section details both the information from the target and the attacker's side.

A. Information from the target's side

For the scope of this article, we consider a set of elements with rules and data in common as an entity. An entity represents a group of people, objects, activities, or concepts that affects directly or indirectly the execution of a given cyber security event. Considering the characteristics of access control models [13], [14], we identified the following entities: $\langle Ua, Re, Ch\rangle$, where Ua is the *User Account* associated to a given status in the system (e.g., system administrator, standard user, guest, internal user, nobody); Re corresponds to the system's *Resources* e.g., physical components (host, server, printer) or logical components (files, records, database) of limited availability within a computer system; and Ch are the *Channels*, which represents all actions needed for a user to have access to a resource (e.g., protocols, IP addresses, port numbers).

In addition, we consider the notion of contexts proposed in the Organization based Access Control (OrBAC) model [15], [16], such as temporal conditions. (e.g., granted privileges only during working hours), spatial conditions (e.g., granted privileges when connected within the company premises), and historical conditions (e.g., granted privileges only if previous instances of the same equivalent events were already conducted). For instance, in order to access a web-server (resource) of a given organization, an external user (user account) connects remotely (spatial condition) to the system by providing his/her login and password (channel) at a given date (temporal condition).

Information security properties (e.g., confidentiality, integrity, availability) are also a key aspect in the analysis of a cyber security event. An event can be associated to a particular issue compromising the system's confidentiality (e.g., unauthorized access to sensitive information, disclosure resources, etc), integrity (e.g., unauthorized change of the data contents or properties, etc), or availability (e.g., unavailable resources, denial of service, etc). Every organization must define their own entities based on their historical data, expert knowledge and assessments they perform on their information systems.

B. Information from the attacker's side

According to Krautsevich et al. [17], adversaries can be either (i) omniscient, when they know all vulnerabilities and all possible patches of the system; (ii) deterministic, when they have a belief knowledge of the system and they choose the best possible action to break into the system; or (iii) adaptive, when they adapt the strategy to complete the attack, using updated knowledge about the system . We divide the information from the attacker's side into two main categories: a priori and a posteriori. The remaining of this section discusses both categories.

1) A priori knowledge: A set of information about the system, possessed by the attacker before exploiting a given vulnerability on the system. If the attacker has a priori knowledge about the operation of the entire system, he/she would be able to inflict a much severe attack.

We distinguish two types of a priori knowledge: the knowledge about the information system, and the knowledge about the attack. The former considers the understandings that the attacker has about the system, whereas the latter considers the skills and experience of the attacker in executing a given attack.

a) About the information system: In this category, we consider the known vulnerabilities of the information system that can be exploited by an attacker to access the system, and the impact in terms of confidentiality, integrity and availability. Following the common vulnerability system scoring method (CVSS) [18], we model the attacker's knowledge about the information system as a six-tuple: $\langle A_V, A_C, A_U, Conf, Int, Avail\rangle$, where A_V considers the required access vector used by the attacker to exploit a system's vulnerability (e.g., local access, adjacent network access, network access); A_C considers the complexity (e.g., high, medium, low) of the attack required to exploit the vulnerability; A_U considers the authentication the attacker requires before launching an attack (i.e., multiple, single, none); and $Conf, Int, Avail$ considers the impact in terms of confidentiality, integrity and availability of a successfully exploited vulnerability.

b) About the attack: In this category, we consider the information about the motivation of the attacker, the threat level, the minimum level of required resources to execute the attack, and the attacker's skills in executing the attack. The attacker's knowledge about the attack itself is modeled as $AK(A) = \langle M_O, T_H, R_E, S_K \rangle$, where M_O considers the different goals (motives) that can encourage an attacker to exploit a vulnerability on the system such as low (e.g., just for fun), medium (e.g., political motives), and high (e.g., for monetary profit; anger, revenge and other emotional drivers; sexual impulses; psychiatric illness) [19], [20]; T_H considers the impact level (e.g., low, medium, high) associated to the threat; R_E considers the minimum level of tangible resources and intangible resources (e.g., high, medium, low) required by the attacker to exploit a system's vulnerability; and S_K defines the level of skills and/or experience (e.g., high, medium, low) required by the attacker to execute a given attack.

2) A posteriori knowledge: A set of information gained by the attacker after a successful exploitation of a system's vulnerability [17]. The system can release information that improves the attacker's knowledge to exploit vulnerabilities or to overcome the security controls set by the system, however, the adversary knowledge is generally incomplete [11]. In this section we study the attacker's knowledge with respect to the system evolution (e.g., deployment of countermeasures).

a) About the countermeasures: From the adversary point of view, the ability to penetrate a system does not necessarily implies the ability to break into a system. Breaking a system means making the system to fail and keep on failing. It is more hostile, and more difficult than penetrating into the system, since it requires an understanding of what makes the system fail [12]. However, penetrating the system is the first step for an attacker to improve his/her knowledge about the system.

According to [17], an attacker observes a system and can influence its behavior by making actions at a given moment. The system responds to an action probabilistically. Attackers do not make decisions about actions blindly. Instead, they take into account past, current, and possible future states of the system, as well as possible rewards that are connected with the actions. The goal of the attacker is to maximize the expected total reward according to a sole criterion.

We define the attacker's a posteriori knowledge based on the actions the defender performs to protect the system against a given attack (e.g., implementing security countermeasures). Following the formalism proposed in [17], we model the attacker's a posteriori knowledge as a set $A_K(C) = \langle S_T, P_A, P_R, R_W, D_E \rangle$, where S_T corresponds to the system state, P_A considers the probability that the attacker executes an action in the state S_{Ti}, P_R corresponds to the probability that the system transits from state S_{Ti} to S_{Ti+1} in response to attacker's actions, R_W considers a set of rewards functions dependent on the state and the actions, and D_E corresponds to a set of decisions available to the attacker.

III. Proposed Model Description and Construction

Our geometrical model is proposed to represent cyber security events (e.g., attacks, countermeasures) as prismatic instances of n-sides. The base of the prism integrates the information from the target's side (internal entities), whereas the height of the prism integrates the information from the attacker's side (external entities). Our proposed geometrical model has the following characteristics:

- There are at least two internal entities and one external entity represented in the geometrical instance;
- The base of the geometrical instance is an n-sided polygon;
- Each axis of the prism's base represents an internal entity affected by the security event. Such affectation is measure by the contribution of the axis;
- All external entities are merged to compute a global contribution. Such value represents the height of the prism;
- The end point of each axis is connected to form a polygon;
- The contribution of each axis must be greater than zero and no more than one hundred percent;
- Polygons can be regular, irregular, and/or convex;
- Concave polygons are excluded from our model since it is not possible to plot instances in which one or more interior angles are greater than 180 degrees;
- Polygons are closed with no holes inside;
- Polygons are not self-intersecting;
- The prism results out of the projection of the polygon base and height;

The remaining of this section details the contribution calculation of the internal and external dimensions of our prismatic model.

A. Internal Axes

As previously stated, each axis composing the base of the prism represents an entity. Each entity contributes differently in the event impact calculation. Following the CARVER methodology [21], [22], which considers six criteria (i.e., criticality, accessibility, recuperability, vulnerability, effect, recognizability), we assign numerical values on a scale of 1 to 10 to each type of element within the entity. As a result, we obtain a weighting factor (WF) that is associated to each type of element. Examples of the practical implementation of this methodology in real case scenarios can be seen in [7], [8].

The contribution Co of each internal entity T_i in the execution of an event E is a value than ranges from zero (when there is no element of the axis affected to a given event), to one (when all elements of the axis are affected to a given event). The contribution of an entity T_i is calculated as stated in Definition 1.

Definition 1 (Internal Axes Contribution): Let $X = x_1, x_2, ..., x_i$ be a finite set of size i, namely Total_E, and composed by

the total number of elements integrating the internal entity T_i; and let Y = y_1, y_2,..., y_j be a finite set of size j, namely Affected_E, and composed by the affected elements of the entity T. Knowing that the set Y is a subset of X, thus $Y \subseteq X$, then, the contribution Co of the entity T in the execution of event E is computed using Equation 1.

$$Co(T_i, E) = \frac{\sum_{j=1}^{n} Y_j \times WF(Y_j) \ \ \forall j \in Y}{\sum_{i=1}^{n} X_i \times WF(X_i) \ \ \forall i \in X} \quad (1)$$

In order to apply Equation 1 in a practical case, let us consider the entities defined in the previous section. The contribution for the user account, for instance, can be evaluated as the number of users affected by a given attack over the total number of active users from the system. Similarly, the contribution of the confidentiality can be evaluated as the number of alerts indicating a confidentiality issue over the total number of alerts in a given period of time. For spacial contexts, we can evaluate the number of incidents occurring in a given location over the total number of reported incidents within a period of time.

B. External Axis

Contrary to the information about the target, that is modeled as an n-sided polygon (which can be mono-axial, bi-axial or multi-axial), the information about the attacker is modeled as a single entity (i.e., mono-axial), which represents the height of the prismatic instance.

The contribution Co of the external entity T_e in the execution of an event E is a value than ranges from zero to one. Such contribution represents the level of information possessed by the attacker regarding the system, the exploited attack, and/or the countermeasures implemented by the system. The greater the attacker knowledge, the greater the impact, and therefore, the larger the prism's height. The a priori and a posteriori contribution $Co(T_e)$ is calculated as stated in Definitions 2 and 3.

Definition 2 (A Priori Contribution):
Let Exp be the level of exploitability of a given vulnerability in terms of access vector (A_V), access complexity (A_C) and authentication (A_U); let Imp be the impact level in terms of confidentiality ($Conf$), integrity (Int), and availability ($Avail$); and let Mot and Res be the attacker's motivation and resources respectively. The a priori contribution Co^a of the external entity T_e in the execution of an event E is computed using Equation 2.

$$Co^a(T_e, E) = \frac{1}{2}Exp + \frac{1}{4}Imp + \frac{1}{4}Goal + \frac{1}{4}Res \quad (2)$$

Where
$Exp = A_V \times A_C \times A_U$
$Imp = 1 - [(1 - Conf) \times (1 - Int) \times (1 - Avail)]$
$Res = R_S$
$Goal = S_K \times T_H \times M_O$

From the previous equation, the more remote an attacker is from the host, the greater the A_V score; the higher the complexity to access the system, the lower the A_C score; the higher the number of required authentication methods, the lower the A_U score, and the higher the level of impact in terms of confidentiality, integrity and availability, the greater the $Conf$, Int, and $Avail$ scores. In addition, the higher the level of resources and skills required by the attacker to exploit a system's vulnerability, the lower the R_S and S_K scores. The higher the threat level and motivation, the higher the T_H and M_O scores.

The height h of the prismatic instance I a priori is therefore equivalent to value of the external axis contribution a priori e.g., $h(I^a) = Co(T_e, E)$. Table I depicts the possible values of the parameters composing Equation 2.

TABLE I
QUANTITATIVE VALUES OF PARAMETERS A PRIORI

Parameter	Level	Value	Level	Value	Level	Value
A_V	Local	0.395	Adjacent Network	0.646	Network	1.0
A_C	High	0.3	Medium	0.61	Low	0.71
A_U	Multiple	0.395	Single	0.646	None	1.0
$Conf, Int, Avail$	None	0.0	Partial	0.275	Complete	0.660
R_S	High	0.34	Medium	0.67	Low	1.0
S_K	High	0.34	Medium	0.67	Low	1.0
T_H	Low	0.34	Medium	0.67	High	1.0
M_O	Low	0.34	Medium	0.67	High	1.0

Note that levels and values refer to the corresponding qualitative and quantitative assessments of each parameter. Our approach considers the scores proposed in the CVSS v2.0 for the exploitability and Impact parameters. For the rest of values, we consider three levels (e.g., low, medium, high) in which the lowest score is 1/3, the medium score is 2/3 and the highest score is 3/3.

In case the prismatic instance is the information system, we take a pessimistic approach, where the values of each parameters composing Equation 2 corresponds to the worst case scenario that could occur in the system. Otherwise, if the prismatic instance is an attack, we consider a more specific approach, where the parameter values correspond to those associated to the exploited vulnerability.

Definition 3 (A Posteriori Contribution): Let S_T be the system state, P_A the actions available for the attacker, P_R the probability that the system transits from one state to another in response to attacker's actions, R_W be the reward function, and D_E a set of decisions taken by the attacker, then, the a posteriori contribution Co^b of the external entity T_e in the execution of an event E is computed using Equation 3.

$$Co^b(T_e, E) = \frac{1}{2}\left[S_T + \frac{(P_A \times P_R) + (R_W \times D_E)}{2}\right] \quad (3)$$

From the previous equation, the higher the a priori knowledge about the system, the greater the S_T score; the higher

the number of possible actions for the attacker to exploit a vulnerability, the greater the P_A score; the higher the probability that the system will react against the attacker's actions, the lower the P_R score, the higher the level of reward that the attacker can obtain, the greater the R_W score, and the higher the number of decisions available to the attacker, the greater the D_E score.

The height h of the prismatic instance I (a posteriori) is therefore equivalent to the value of the external axis a posteriori contribution e.g., $h(I^b) = Co(T_e, E)$. Note that the impact of the attacker's a posteriori knowledge about the countermeasure ($Co^b(T_e, C)$) should be lesser or equal to the more pessimistic impact of the attacker's a priori knowledge about the system ($Co^a(T_e, S)$), therefore, the product of $P_A \times P_R$ and $R_W \times D_E$ should be lesser or equal to the S_T value. Table II depicts the possible values of the parameters composing Equation 3.

TABLE II
QUANTITATIVE VALUES OF PARAMETERS A POSTERIORI

Parameter	Level	Value	Level	Value	Level	Value
S_T	Low	0.34	Medium	0.67	High	1.0
P_A	Low	0.34	Medium	0.67	High	1.0
P_R	High	0.34	Medium	0.67	Low	1.0
R_W	None	0.0	Partial	0.5	Total	1.0
D_E	None	0.0	Single	0.5	Multiple	1.0

IV. EXAMPLE OF INSTANCES

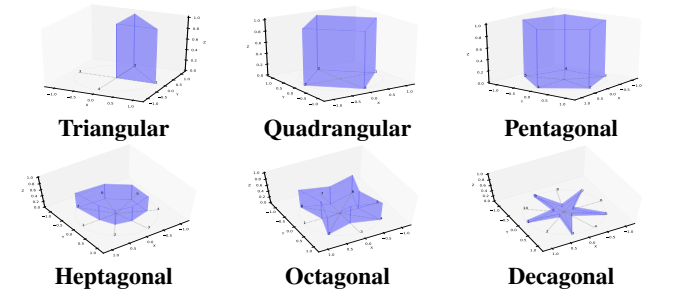
A variety of geometrical instances (e.g., regular and irregular prisms) results from the analysis of the internal and external information related to a given cyber security event. The remaining of this section details the different prismatic instances.

A. Triangular Prisms (Two or Three Axis)

Plotting the contribution of two internal entities (e.g., user account, resource) results into a right triangle polygon (i.e., right isosceles, right scalene). The contribution of the external axis (attacker's information) allows to project the polygon in a three-dimensional space, which results into a right triangular prism. Let us consider, for instance, an event E_1 that compromises 25% of users $Co(T_1)$ = 0.25, and 25% of resources $Co(T_2)$ = 0.25, with 100% of the attacker's knowledge of the information system. The graphical representation of the impact contribution of event E_1 over the user and resource entities is depicted in Table III as a Triangular Prism. We obtain the base of the prismatic instance by connecting the end point of each internal axis (user, resource). The prism's height is represented by the contribution of the external axis.

Plotting the contribution of three internal entities (e.g., user, resource, time), results into a non right triangle polygon (e.g., equilateral, scalene, isosceles). In this category, we find obtuse triangles (instances with one angle greater than 90 degrees, and/or acute triangles (instances with all their angles less than 90 degrees). The contribution of the external axis (attacker's information) allows to project the polygon in a three-dimensional space, which results into a non-right triangular prism.

TABLE III
N-PRISMATIC REPRESENTATIONS



B. Quadrangular Prisms (Four Axes)

Plotting the contribution of four internal entities (e.g., user, resource, channel, time), results into a quadrilateral polygon (e.g., square, rhomboid, kite, etc.). We exclude rectangles, since it is not possible to represent instances that have both: two equal alternate sides and right angles. In addition, we discard rhombus from our graphical representation, since it is not possible to represent instances that have both: equal lengths and non-right angles.

The contribution of the external axis (attacker's knowledge) allows to project the polygon in a 3D space, resulting in a quadrangular prism (e.g., parallelepiped, cube). We exclude rectangular parallelepipeds and cuboids, since it is not possible to obtain a rectangular base. In addition, we discard rhombohedrons[1] since we can only plot the height of the instance as a right straight line. However, it is possible to obtain square cuboids[2] from our model.

Let us consider, for instance, an event E_1 that compromises 50% of the system's users, physical resources, logical resources, and channels with 100% of the attacker's knowledge. The graphical representation of the impact contribution of event E_1 is depicted in Table III as a Quadrangular Prism (in this case, a Square Cuboid).

C. N-Polygonal Prisms (N Axes)

Plotting the contribution of five or more internal entities (e.g., user, physical resource, logical resource, channel, time, location, etc.), results into an n-sided polygon (e.g., pentagon, hexagon, heptagon, etc.). Polygons can be regular or irregular. The contribution of the external axis (attacker's knowledge) allows to project the polygon in a 3D space, resulting in an n-prism (e.g., pentagonal prism, hexagonal prism, heptagonal prism, etc.), as depicted in Table III. For instance, let us

[1] a special case of a cube with rhombi faces
[2] a special case of a cuboid in which at least two faces are squares

consider an event E_1 that compromises 100% of the even axes and 10% of the odd axes from a 10-sided polygon (i.e., decagon). The contribution of the attacker's knowledge is 10%, resulting in a decagonal prism (with a star shape), as shown in Table III.

D. Exclusions

It is not possible to obtain prismatic instances with information of only one type of entity. In case of retrieving information of one internal axis (information about the target) and no information from the attacker's side, we will obtain straight lines as the resulting impact of the security event. In case of retrieving information of one internal and one external axis, their projection will result into a surface (i.e., square, rectangle). We exclude such cases from our analysis, since we require information of at least two internal axes, and the information of the attacker's knowledge, in order to build the resulting prisms.

Considering the characteristics of our geometrical model, we constraint our model to right prisms (n-sided prisms whose bases and joining faces are perpendicular to each other). The resulting instance must have identical bases joined together by flat faces and identical cross section along its length. The bases of the prism are polygons and the side faces must necessarily be parallelograms. Based on this, we exclude from our research the following geometrical instances:

- Oblique prisms, since their bases and joining faces are not perpendicular;
- Twisted prisms and antiprisms, since their bases are twisted relative to each other, making the side faces be triangles instead of parallelograms;
- Platonic solids, i.e., tetrahedron, octahedron, dodecahedron, and Icosahedron, except from the cube, the other platonic solids are excluding from our research, since their side faces are not parallelograms;
- Circular solids (e.g., cylinder, cones and spheres), since they have curved surfaces, not flat faces;
- Pyramids, since they have triangular sides instead of parallelograms. In addition, the base of the pyramid is not projected to the top, instead, they connect the polygonal base to a single point, called the apex;
- Rectangular-based solids (e.g., rectangular parallelepipeds), since it is not possible to plot instances with two equal alternate sides and right angles;
- Prisms whose bases are self intersecting polygons, concave polygons, or open geometrical figures with holes inside.

It is important to note, that although very similar, circular prisms and cylinders are not the same. Technically a cylinder has curved sides, whereas a circular prism has parallelogram sides. However, geometrically, prisms with very large number of sides of regular polygonal bases, are similar to cylinders since the side faces tend to have the parallelograms of negligible width. In our model, prisms with a huge number of lateral sides are considered as polygonal prisms, and cylinders are excluded from our research since their base is circular and not polygonal.

V. Geometrical Operations

This section details the measurements of the different geometrical figures described in the previous section. Such measurement allows the mathematical computation of the impact of multiple events in the system.

A. Area (A)

The area (A) of a given event measures the amount of space inside the boundary of a flat (2-dimensional) object such as a triangle or square. We calculate the surface area of the base of a prism using Definition 4.

Definition 4 (Area (A)): Let b be the base of a prism. The area A of b is computed as the sum of the contribution value of entity T_i times the contribution value of entity T_{i+1} divided by two. Results are expressed in $units^2$, using the following equation:

$$A(b) = \frac{\sum_{i=1}^{n} Co(T_i) \times Co(T_{i+1})}{2} \tag{4}$$

For the previous Equation, note that in the last term (i.e., $Co(T_n)$), the expression must wrap back to the first term (i.e., $Co(T_1)$). This method works correctly for triangles, regular and irregular polygons, as well as convex and concave polygons, but it will produce wrong answers for self-intersecting polygons, where one side crosses over another. However, such cases are excluded from our research.

Let us take an example of an attack A_1 that affects 60% of resources (T_1), 60% of channels (T_2), 80% of users (T_3) and requires 40% of recovery time (T_4). Attack A_1 will have an area equal to $A(Quadrilateral)$ = $[(60 \times 60) + (60 \times 80) + (80 \times 40) + (40 \times 60)]/2$ = 700 $units^2$

B. Volume (V)

The volume (V) of a prism (P) measures the three-dimensional space enclosed by the boundary of a prismatic instance (e.g., triangular prism, pentagonal prism, octagonal prims, etc.). We calculate the volume of a prism using Definition 5.

Definition 5 (Volume (V)): Let P be a prism with base b and height h. The volume V of P equals the surface area of the base times the height of the prism. Results are expressed in $units^3$, using the following equation:

$$V(P) = A(b) \times h \tag{5}$$

C. Coverage of Events

The coverage (COV) of events is a value that ranges between zero and one, and represents the portion of an event E_x that is affected or controlled by an event E_y. We calculate the coverage of events using Definition 6.

Definition 6 (Coverage (COV)): Let M be the measurement of an event (e.g., area, volume), and let E_1 and E_2 be two distinct events. The coverage (COV) of event E_1 respect to event E_2 is computed as the ratio between the impact measurement of E_2 overlapping with the impact measurement of E_1 over the impact measurement of E_2. Results are expressed in $\%$, using the following equation:

$$COV(E_1/E_2) = \frac{M(E_1 \cap E_2)}{M(E_2)} \times 100 \quad (6)$$

D. Residual Risk

The Residual Risk (RR) of an event E_x is a value that ranges between zero and one, and represents the portion of the event E_x that is left untreated by any control. We calculate the residual risk of events using Definition 7.

Definition 7 (Residual Risk (RR)): Let E_1 be a security incident, and E_2 its corresponding security control. The Residual Risk (RR) of event (E_1) after the implementation of event E_2 is computed as the difference between the maximal risk level (i.e., 100%) and the coverage of event (E_2) respect to event (E_1). Results are expressed in $\%$, using the following equation:

$$RR(E_1/E_2) = 100\% - COV(E_1/E_2) \quad (7)$$

E. Potential Collateral Damage

The Potential Collateral Damage (PCD) of an event E_x is a value that ranges between zero and one, and represents the portion of the event E_x that affects elements in the system that are not compromised by the detected security incident. We calculate the PCD of events using Definition 8.

Definition 8 (Potential Collateral Damage (PCD)): Let event E_1 be a security incident, and event E_2 be its corresponding security control. The potential collateral damage (PCD) of event E_2 is computed as the ratio between the portion of event E_2 that is not intersecting with event E_1 and the total impact measurement of E_2. Results are expressed in $\%$, using the following equation:

$$PCD(E_1/E_2) = \frac{M(E_2) - M(E1 \cap E_2)}{M(E_2)} \times 100 \quad (8)$$

VI. Use Case

A telecommunication company has detected a great number of alerts related to confidentiality and availability issues that affect most of its users and resources. Two main security incidents have been identified: A_1 (CVE-2016-0800), a cross-protocol attack that could lead to decryption of TLS sessions by using a server supporting SSLv2 and export cipher suites as a Bleichenbacher RSA padding oracle; and A_2 (CVE 2015-1787), a Denial of Service attack on applications compiled with OpenSSL library.

Both attacks affect services that rely on SSL/TLS protocols. Attack A_1 allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data, whereas attack A_2 allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.

The following security controls are proposed to mitigate both attacks:

C1 Install patched version of OpenSSL;
C2 Disable the SSLv2 protocol in all the SSL/TLS servers;
C3 Reconfigure web servers, SMTP servers, IMAP and POP servers, and any other software that supports SSL/TLS to avoid the use of weak cipher suites.

Table IV shows the affected entities and categories for the system S, attacks A_1, and A_2, as well as countermeasures C_1, C_2, and C_3. Each entity has at least one category with a given number of elements. Each category has an associated weighting factor (WF), which indicates its priority on the system. The higher the WF, the higher the priority of the entity's category. The rest of the table's columns show the number of elements from the system S that are affected by attacks A_1, A_2, and countermeasures C_1, C_2, and C_3.

TABLE IV
System Information (internal axes)

Entity	*Category*	S	WF	A_1	A_2	C_1	C_2	C_3
User	administrator	2	5	2	2	2	2	2
	regular user	63	2	33	25	63	0	0
Channels	IP address	65	3	2	12	0	0	12
Resources	workstation	57	2	17	28	57	0	22
	server	7	5	7	7	7	7	7
	database	2	4	2	2	2	2	2
Location	inside	26	2	3	3	0	0	26
	outside	94	4	35	48	35	48	75
Security	Confidentiality	48	4	38	0	48	0	24
property	Availability	72	5	0	51	0	72	31

Table V shows the information about the attacker's a priori and a posteriori knowledge about system S, attacks A_1, and A_2, and countermeasures C_1, C_2, and C_3. Note that the values of parameters for attacks A_1, and A_2 are obtained from the National Vulnerability Database[3]. The values for the system S are obtained by taking a pessimistic approach (the worst case scenario); and the values of parameters for the countermeasures C_1, C_2, and C_3 are first assessed qualitatively and then transformed into their corresponding quantitative values.

A. Impact Calculation

1. Internal Axes Size: We compute the size of each axis composing the system S, using information from Table IV, as follows:

- Ua = $(2 \times 5) + (63 \times 2)$ = 136 $units$
- Ch = 65×3 = 195 $units$
- Re = $(57 \times 2) + (2 \times 4) + (7 \times 5)$ = 157 $units$

[3]https://nvd.nist.gov/

TABLE V
ATTACKER'S KNOWLEDGE (EXTERNAL AXIS)

A Priori Knowledge										
Instance	A_V	A_C	A_U	$Conf$	Int	$Avail$	R_E	S_K	T_H	M_O
S	1.0	0.71	0.704	0.66	0.66	0.275	1.0	1.0	1.0	1.0
A_1	1.0	0.61	0.704	0.275	0.0	0.0	0.675	0.67	0.67	1.0
A_2	1.0	0.30	0.704	0.0	0.0	0.275	0.34	0.34	1.0	1.0
$A_1 \cup A_2$	1.0	0.61	0.704	0.275	0.0	0.275	0.675	0.67	1.0	1.0

A Posteriori Knowledge					
Instance	S_T	P_C	P_R	R_W	D_E
C_1	0.67	0.34	0.34	0.50	0.50
C_2	0.34	0.67	0.34	0.00	0.00
C_3	0.34	0.34	0.67	0.50	1.00
$C_1 \cup C_2$	0.67	0.67	0.34	0.50	0.50
$C_1 \cup C_3$	0.67	0.34	0.67	0.50	1.00
$C_2 \cup C_3$	0.34	0.67	0.67	0.50	1.00
$C_1 \cup C_2 \cup C_3$	0.67	0.67	0.67	0.50	1.00

- Lo = $(26 \times 2) + (94 \times 4)$ = 428 $units$
- Sp = $(48 \times 4) + (72 \times 5)$ = 552 $units$

2. Internal Axes Contribution: We calculate the contribution of each axis on the execution of the events (i.e., A_1, A_2, C_1, C_2, and C_3) with respect to the system value, using Definition 1. For instance, Countermeasure C_1 affects the following axis:

- Ua = $(2 \times 5) + (63 \times 2)$ = 136 $units \rightarrow 100.00\%$
- Ch = 0×3 = 0 $units \rightarrow 0.00\%$
- Re = $(57 \times 2) + (2 \times 4) + (7 \times 5)$ = 157 $units \rightarrow 100.00\%$
- Lo = $(0 \times 2) + (35 \times 4)$ = 140 $units \rightarrow 32.71\%$
- Sp = $(48 \times 4) + (0 \times 5)$ = 192 $units \rightarrow 44.86\%$

3. External Axis Contribution: We calculate the contribution of the attacker's knowledge (a priori and a posteriori) using Definitions 2 and 3. For instance, for system S, the most pessimistic a priori contribution is calculated as follows:
$h(S)$ = $\frac{1}{2}(0.49984)$ + $\frac{1}{4}(0.91619)$ + $\frac{1}{4}(1.0)$ + $\frac{1}{4}(1.0)$ = 97.90%

4. Impact Calculation: We calculate the geometrical operations of attack A_1, A_2, and countermeasures C_1, C_2, and C_3, using Definitions 4 and 5. For Countermeasure C_1, for instance, we compute the area and volume as follows:
A(C_1) = $4,612.19$ $units^2$
V(C_1) = $4,612.19$ $units^2 \times$ 42.64 $units$ = $196,663.92$ $units^3$

5. Coverage Calculation:

We calculate the coverage of attacks A_1 and A_2 with respect to system S, and the coverage of countermeasures C_1, C_2, and C_3 with respect to the combined attack $A_T = A_1 \cup A_2$, using Definition 6. In addition, the residual risk (RR) is computed using Definition 7, and the potential collateral damage (PCD) is calculated using Definition 8. For instance, the coverage of countermeasure C_1 with respect to the combined attack $A_T = A_1 \cup A_2$ is computed as follows:

A($C_1 \cap A_T$)= 2,604.45 $units^2$
V($C_1 \cap A_T$)= 2,604.45 $units^2 \times$ 42.64 $units$ = 111,053.82 $units^3$
COV (C_1/A_T) = $\frac{111,053.82 \times 100}{374,202.28}$ = 29.68%
RR(C_1/A_T) = 100 - 29.68 = 70.32%
PCD(C_1/A_T) = $\frac{(196,663.92 - 111,053.82) \times 100}{196,663.92}$ = 43.53%

Table VI summarizes the impact values of all events. Attacks A_1 and A_2 are compared against both, the system S and all countermeasures (C_1, C_2, and C_3). The union of both attack $A_T = A_1 \cup A_2$ affects 15.32% of the total system area. Applying countermeasures individually will reduce part of the attack impact. However, if multiple countermeasures are implemented, the risk is expected to be reduced substantially.

TABLE VI
EVENT IMPACT EVALUATION

Event	**A** ($units^2$)	**h** ($units$)	**V** ($units^3$)	**COV** (%)	**RR** (%)	**PCD** (%)
S	25,000.00	97.90	2,447,418.75	-	-	-
A_1	2,595.97	56.44	146,528.08	5.99	-	-
A_2	5,140.25	34.44	177,004.55	7.23	-	-
$A_1 \cup A_2$	5,599.32	66.96	374,909.89	15.32	-	-
C_1	4,612.19	42.64	196,663.92	29.68	70.32	43.53
C_2	2,810.19	22.70	63,777.17	10.83	89.17	36.47
C_3	5,485.26	35.20	193,053.89	32.29	67.71	37.41
$C_1 \cup C_2$	8,335.23	45.45	378,794.34	53.62	46.38	47.03
$C_1 \cup C_3$	11,302.11	51.70	584,262.61	76.69	23.31	50.88
$C_2 \cup C_3$	6,626.15	40.72	269,833.29	37.64	62.36	47.81
$C_1 \cup C_2 \cup C_3$	13,622.73	57.22	779,526.57	85.62	14.38	58.90

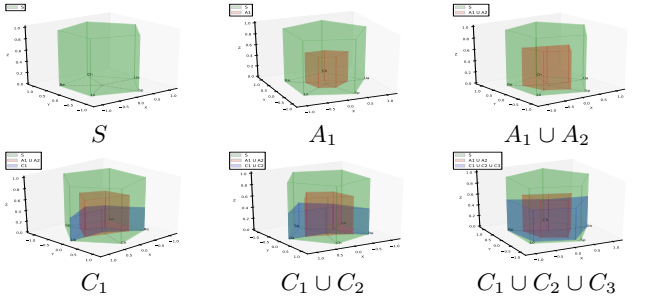
B. Graphical Representation

Table VII shows the graphical representation of the system S (in green), attacks A_1 and A_2 (in red), and countermeasures C_1, C_2, and C_3 (in blue). System S is represented as a regular pentagonal prism, whereas attacks and countermeasures are represented as irregular pentagonal prisms. The graphical representation of the combined attacks $A_1 \cup A_2$ shows a higher impact over the system S than their individual representations. Similarly, the graphical representation of the countermeasures shows that their combined implementation has a higher impact over the system, which generally results into a lower residual risk level and a higher potential collateral damage. Countermeasures are plotted along with the system S and the combined attack $A_1 \cup A_2$ to show their level of coverage.

While computing the impact of events, we must consider the fact that events can be joint or disjoint. If comparing two or more security incidents, the bigger the measurement, the higher the impact on the system. It is important, however, to compare the impact of events using the same unit scale (e.g., $units^2$, $units^3$), and to avoid mixing them up.

If comparing two or more security controls, the bigger the measurement of the events, the higher the protection of the system's elements. However, this does not imply that such an event protects effectively the system from the detected

TABLE VII
PRISMATIC REPRESENTATIONS



incident. For this, it is necessary to compute the coverage of events. This latter indicates the portion of the incident that is mitigated by a given control. The coverage of events is generally used to compare the impact of incidents over the system, and/or to compare the impact of security controls over the incidents.

If the impact measurement of a given control (e.g., $M(E_1)$) is higher than the impact measurement of the security incident (e.g., $M(E_2)$), it means that event E_1 affects more system's elements than event E_2, but it does not mean that event E_2 is totally covered by event E_1. Computing the event coverage allows us determining the portion of the system under attack and the level of mitigation.

Implementing two or more security controls simultaneously generally increases the coverage area of the incident, which reduces the residual risk and makes the solution look more attractive than their individual implementation. However, the implementation of a set of security controls may require modifications (e.g., change configuration) on system's elements that are not under attack. Such action originates potential collateral damage (PCD) to the system. A higher PCD generally implies higher impact on the system. We should, therefore, search for solutions with the highest incident coverage and the lowest potential collateral damage.

One important aspect of our model is the fact that it only considers a percentage of affected elements to plot the impact contribution on each polygonal axis. It is therefore possible to fall into a situation where two disjoint events are graphically plotted as joint. For instance, if event E_1 covers 50% of the system's users and resources with 50% of the attacker's knowledge, and event E_2 covers 25% of the same axes, assuming that both events are disjoint (they have no affected elements in common), the graphical representation of both events will show that event E_2 is totally covered by event E_1. Whereas, in reality, if both events are disjoint, they should be treated separately, by making a comparison on the impact size of both events (in this case, event E_1 is two times bigger than event E_2), and the coverage should be zero. To avoid the previous issues, we need to calculate the event coverage and plot the graphical representation of events only if they are partially or totally joint.

VII. Related Work

Determining the impact of cyber security events is an open issue in the TIC domain. Several research works rely on metrics to quantitatively measure such impacts. Howard et al., [23], [24] and Manadhata et. al. [25], [26], for instance, propose a model to systematically measure the attack surface of different software. However, the approach presents the following shortcomings: it cannot be applied in the absence of source code; it includes only technical impact; it cannot be used to compare different system environments; and it does not evaluate the impact of multiple attacks occurring simultaneously in the system.

Some researchers rely on simulations to analyze and estimate the impact of cyber events. Dini et. al [5], [6], for instance, present a simulative approach to attack impact analysis that allows for evaluating the effects of attacks, ranking them according to their severity, and provides valuable insights on the attack impact since during the design phase. As a result, the approach supports designers in deciding which attacks to address and which countermeasures to select. However, the simulation does not provide quantitative analysis on the impact of countermeasures while evaluating the impact of attacks.

Other approaches use frameworks to model the cyber physical attack space. Texeira et al. [27], [28], for instance, propose a framework to classify attacks in a cyber-physical system using a three dimensional taxonomy, whose main axes are the adversary's knowledge, disclosure and disruption of resources. The main drawback of this research is that authors concentrate only on the adversary a priori knowledge leaving aside the a posteriori knowledge. In addition, Krautsevich et al. [17] and Sarraute et al. [29] propose adversary models that allow understanding the attacker's behavior. The main shortcoming of these researches is that their analysis is based on the adversary's point of view. Our proposed model considers the main aspects of these models to analyze both, the attacker's a priory and a posteriori knowledge.

Based on the aforementioned shortcomings, we propose a geometrical approach to project the impact of cyber events as an n-dimensional prism. The approach uses geometrical operations to compute the size of the polygon, and thus the impact of the represented event. As a result, we are able to project multiple events (e.g., attacks, countermeasures), in a variety of dimensions (e.g., users, channels, resources, Confidentiality, Integrity, Availability, time, etc.), which provides the means to propose security countermeasures as a reaction strategy to mitigate the detected attacks.

VIII. Conclusion

In this paper we proposed a novel approach that considers internal vulnerabilities and the attacker's knowledge to model the impact of cyber security events as geometrical prisms. The approach considers internal information about the assets

that compose the information system (e.g., users, IP addresses, communication protocols, physical and logical resources, etc.), and external information, about the attacker's knowledge (a priori and a posteriori).

Each element composing the model is assigned a quantitative value (depending on their relevance, priority, or impact over the system). Similar elements are regrouped to form one axis of the model. The projection of all axes (internal and external) results into an n-sided prism, whose base is represented by the internal axes and the height is represented by the external axis. It is therefore possible to plot multiple events (attacks and countermeasures) over the same system which allows the comparison of their size, and thus, their associated impact.

We propose a quantitative approach to compute the area and volume of each geometrical instance, making it possible to compute the coverage of events with respect to the system, the residual risk, and the potential collateral damage that may occur out of the implementation of the security countermeasures. As a result, our model is seen as a tool that helps organizations to make the most cost-effective decisions in minimizing the risk of the studied cyber events.

Acknowledgements: The research in this paper has received funding from the PANOPTESEC project, as part of the Seventh Framework Programme (FP7) of the European Commission (GA 610416).

REFERENCES

[1] Computer Emergency Response Team, *Common Cyber Attacks: Reducing the Impact*. White Paper, CERT UK, 2015.

[2] Ponemon Institute, *State of the Endpoint Report: User-Centric Risk*. Technical Paper, 2015.

[3] Verizon Enterprise Solutions, *2015 Data Breach Investigations Report*. Research report, 2015.

[4] B. Roberts, *The macroeconomic impacts of the 9/11 attack: Evidence from real-time forecasting*. Working Paper, Homeland Security, Office of Immigration Statistics, 2009.

[5] G. Dini and M. Tiloca, *On simulative analysis of attack impact in wireless sensor networks*. Conference on Emerging Technologies & Factory Automation, 2013.

[6] G. Dini and M. Tiloca, *A simulation tool for evaluating attack impact in cyber physical systems*. International Workshop MESAS, pages 77-94, 2014.

[7] G. Gonzalez-Granadillo, J. Garcia-Alfaro, E. Alvarez, M. El-Barbori, and H. Debar, *Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the rori index*. Computers and Electrical Engineering Journal", 47:13-34, 2015.

[8] G. Gonzalez-Granadillo, J. Garcia-Alfaro, and H. Debar, *Using a 3D geometrical model to improve accuracy in the evaluation and selection of countermeasures against complex cyber attacks*. 11th EAI International Conference on Security and Privacy in Communication Networks, pages 538-555, 2015.

[9] P. Mardziel, *Modeling, Quantifying, and Limiting Adversary Knowledge*. PhD Thesis, University of Maryland, College Park, USA, 2015.

[10] D. Buckshaw, G. Parnell, W. Unkenholz, D. Parks, J. Wallner, S. Saydjari, *Mission oriented risk and design analysis of critical information systems*. Military Operations Research, Vol. 10, number 2, pp.19–38 , 2005.

[11] L. Krautsevich, A. Yautsiukhin, *Evaluation of Adaptive Attacker Models*. ESSoS Doctoral Symposium, 2014.

[12] M. Libicki, *Brandishing Cyberattack Capabilities*. National Defense Research Institute, white paper, 2013.

[13] A. A. E. Kalam, R. E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, *Organization based access control*. International Workshop on Policies for Distributed Systems and Networks, 2003.

[14] N. Li and M. Tripunitara, *Security analysis in role-based access control*. ACM Transactions on Information and System Security, 9(4):391-420, 2006.

[15] F. Cuppens and N. Cuppens-Boulahia, *Modeling contextual security policies*. International Journal of Information Security, 7(4):285-305, 2008.

[16] F. Cuppens, N. Cuppens-Boulahia, and A. Miege, *Modelling contexts in the or-bac model*. 19th Annual Computer Security Applications Conference, 2003.

[17] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, *Towards modelling adaptive attacker's behaviour*. 5th International Symposium, FPS, pages 357-364, 2013.

[18] S. R. P. Mell, and K. Scarfone, *A complete guide to the common vulnerability scoring system version 2.0*. Technical Paper, 2007.

[19] M. Bielecki and G. Quirchmayr, *A prototype for support of computer forensic analysis combined with the expected knowledge level of an attacker to more efficiently achieve investigation results*. International Conference on Availability, Reliability and Security, pp. 696-701, 2010.

[20] D. Shinder, *Scenes of the cybercrime. computer forensics handbook*. Syngress Publishing Inc., 2002.

[21] T. L. Norman, *Risk Analysis and Security Countermeasure Selection*. CRC Press, Taylor & Francis Group, 2010.

[22] F. of American Scientists, *Special operations forces intelligence and electronic warfare operations, appendix D: Target analysis process*. Available at: http://www.fas.org/irp/doddir/army/fm34-36/appd.htm, 1991.

[23] M. Howard, *Mitigate security risks by minimizing the code you expose to untrusted users*. In MSDN Magazine, 2004.

[24] M. Howard and J. Wing, *Measuring relative attack surfaces*. Computer Security in the 21st Century, pages 109-137, 2005.

[25] P. Manadhata and J. Wing, *An attack surface metric*. IEEE Transactions on Software Engineering, 2010.

[26] P. Manadhata, J.Wing, M. Flynn, and M. McQueen, *Measuring the attack surfaces of two ftp daemons*. 2nd ACM Workshop on Quality of Protection, 2006.

[27] A. Teixeira, I. Shames, H. Sandberg, and K. Johansson, *Attack Models and Scenarios for Networked Control Systems*. Conference on High Confidence Networked Systems HiCoNS, pp. 55–64, 2012.

[28] A. Teixeira, I. Shames, H. Sandberg, and K. Johansson, *A secure control framework for resource-limited adversaries*. Automatica, vol.51, pp. 135–148, 2015.

[29] C. Sarraute, O. Buffet, J. Hoffmann, *POMDPs make better hackers: Accounting for uncertainty in penetration testing*. arXiv preprint arXiv:1307.8182, 2013.