Selecting optimal countermeasures for attacks against critical systems using the Attack Volume model and the RORI index

G. Gonzalez-Granadillo[1], J. Garcia-Alfaro[1], E. Alvarez[1], M. El-Barbori[1], H. Debar[1]

[a]*Institut Mines-Telecom, Télécom Sudparis, CNRS SAMOVAR UMR 5157*
9 rue Charles Fourier, 91011 EVRY, France
E-mails:{FirstName.LastName}@telecom-sudparis.eu

Abstract

The impact quantification of attacks and security countermeasures is an active research in the information and communications technology domain. Supporters of the Return on Investment (ROI), and all its variants, propose quantitative models that estimate their parameters based on expert knowledge, statistical data, simulation and risk assessment tools. Although results are used for relative comparisons, a great level of subjectivity is considered while estimating each parameter composing the model. In single attack scenarios, the use of cost sensitive metrics allows the evaluation and selection of security countermeasures. However, for attack attacks against critical infrastructures, this approach is not accurate enough to determine the impact of the equipment(s), subject(s), and/or action(s) that take part in a security incident. This paper proposes, therefore, a geometrical model that represents the volume of systems, attacks and countermeasures based on a three-dimensional coordinate system (i.e., user, channel, and resource). As a result, volumes are related to risks, making it possible to select optimal countermeasures against complex attacks based on a cost-sensitive metric. A case study on a critical infrastructure control process is provided at the end of the paper to show the applicability of our model in a scenario with two attacks.

Key words: Attack Volume, RORI, Countermeasure Selection, Security Metrics, Industrial Critical Control Systems, SCADA, Decision Support

1. Introduction

Innovation in Information Technology has brought numerous advancements but also some consequences. Cyber attacks have evolved along with technology, reaching a state of high efficiency and performance. Distributed Denial of Service (DDoS), Botnets and Low-rate attacks are just a few examples of this evolution. Attackers are becoming stronger and harder to detect, making the mitigation processes a big challenge for security analysts. The situation becomes even more complex with the dependency of critical infrastructures on information and communication technologies.

Critical infrastructure is a term used to describe assets (e.g., facilities for electricity generation, gas production, water supply, public health) that are essential for the functioning of a society and economy. Critical infrastructures are particularly important because of the functions or services they provide to a nation, and because they are complex systems: the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.

Critical infrastructures, such as the smart grid technology, involve distributed and embedded control and sensing equipment. More and more Supervisory Control and Data Acquisition (SCADA) systems are being connected directly or indirectly to the Internet. Both of these realities increase the potential for adversaries to cause significant damages to the safety and security of private citizens by exploiting weaknesses in these systems. Cyber defence capabilities should therefore improve defensive posture of critical infrastructure systems while ensuring that services are available and secure as widely as possible across the globe.

Most of the current research focus on approaches to detect complex cyber attacks, but only few of them concentrate in evaluating the countermeasures' efficiency in stopping the attack, and their ability to preserve, at the same time, the best service to legitimate users [1]. Supporters of the Return On Investment (ROI) [2, 3], and all its variants (e.g., ROA [4], ROSI [5, 6], ROISI [16]) propose quantitative models that estimate their parameters based on expert knowledge, statistical data, simulation and risk assessment tools. Although results are used for relative comparisons, a great level of subjectivity is considered while estimating each parameter composing the model.

Current approaches to mitigate cyber attacks consider one attack at a time [8, 9] by proposing security solutions to either stop its effects, or decrease its severity. However, very little effort is dedicated to the selection of countermeasures for multiple and complex attacks (e.g., attacks against critical infrastructures). We, therefore, need tools that could help security administrators in the assessment, evaluation and selection of security countermeasures for national and industrial critical infrastructures.

In this paper, we propose an improvement of the attack surface model [10] that represents graphically the volume of systems, attacks and countermeasures, based on a three-dimensional coordinate system (i.e., user, channel, and resource). The coordinates of each element are derived from a URI [11]. We compute the union and intersection of the different volumes by using geometrical operations. The CARVER methodology [12, 13] is used to give an appropriate weight to each element composing the axes in our coordinate system, making it possible to determine the coverage of multiple countermeasures with respect to a given security incident. Countermeasures are analyzed based on the Return On Response Investment (RORI), which evaluates multiple criteria (e.g., deployment cost, coverage, effectiveness, combination, restrictions) in order to select the countermeasure with the highest index, and thus, the highest benefit to the organization.

Paper Organization: Section 2 introduces the state of the art in cost sensitive metrics, and the attack surface model. Section 3 presents our proposed model and details the methodology to calculate the system, attack, and countermeasure volume. Section 4 describes each dimension composing our cooridnate system. Section 5 details the intra normalization of the elements composing the model. Section 6 presents the geometric approach to calculate the union and intersection of different volumes. Section 7 details the implementation of the decision support platform and discusses the main resulting geometrical figures. A case study on a critical infrastructure control process is provided in Section 8. Conclusions and future work are presented in Section 9.

2. State of the Art

This section introduces the two main concepts for the evaluation and selection of countermeasures: cost sensitive metrics and the attack surface model.

2.1. Cost Sensitive Metrics

Cost sensitive metrics are widely proposed as a viable approach to find an optimal balance between intrusion damages and response costs, and to guarantee the choice of the most appropriate response without sacrificing the system functionalities. This section introduces the Return On Investment (ROI) and its variants.

2.1.1. Return On Investment (ROI)

The simplest and most used approach for evaluating financial consequences of business investments, decisions and/or actions is the Return On Investment (ROI) metric. The ROI index is a relative measure that compares the benefits versus the costs obtained for a given investment [2, 3]. This metric supports decision makers to select the option(s) that have the highest return. The decision rule is that the higher the ROI value, the more interesting the investment.

2.1.2. Return On Attack (ROA)

The Return On Attack (ROA) is a relative measure that evaluates the gain the attacker expects from a successful attack over the losses that he sustains due to the adoption of countermeasures by his target [4]. As a result, the lower the ROA value, the more interesting the security investment.

2.1.3. Return On Security Investment (ROSI)

The Return On Security Investment (ROSI) is a relative metric that compares the differences between the damages originated by attacks (with and without countermeasures) against the cost of the countermeasure [5, 6].

The calculation of the parameter composing the ROSI equation has been widely discussed by Lockstep Consulting [14] and Kosutic [15]. The former proposes a methodology that considers different levels of likelihood and severity, which are then, respectively transformed into frequency and direct cost; the latter considers on the one hand, parameters associated to the incident (e.g. financial losses, costs, frequency, etc.), and on the other hand, parameters associated to the protection (e.g., cost, benefits, life expectancy of the security measure, etc.).

Similar to the ROI metric, the decision rule is that the higher the ROSI value, the more interesting the investment.

2.1.4. Return On Information Security Investment (ROISI)

Mizzi [16] proposes an adaptation to ROSI, which introduces the concept of motivation to an attack, successfulness of an attack, and viability of expenditure, making it possible to quantify the total cost of the portion of information assets that may be lost due to intrusions or attacks. However, according to Locher [17], ROSI would lead to proper results, if the risk mitigation effects are calculated properly with scenario analysis and expected values. It has been matured in various models trying to consider qualitative variables, but it is doubtful, if variables like criticality, exposure, and vulnerability, help to improve the ROSI concept.

2.1.5. Return On Response Investment (RORI)

The Return On Response Investment (RORI) was first introduced by Kheir et al. [8] as a service dependency model for cost sensitive response based on a financial comparison of the response alternatives. RORI is an adaptation of the ROSI index that provides a qualitative comparison of response candidates against an intrusion.

Gonzalez Granadillo et al. [9] propose an improvement of the RORI index that handles the choice of applying no countermeasure to compare with the results obtained by the implementation of security solutions (individuals and/or combined countermeasures), and provides a response that is relative to the size of the infrastructure. The improved index is calculated according to the following equation:

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100 \tag{1}$$

where:

- ALE is the Annual Loss Expectancy and refers to the impact cost obtained in the absence of security measures. ALE is expressed in currency per year (e.g., \$/year) and will depend directly on the attack's severity and likelihood.

- RM refers to the Risk Mitigation level associated to a particular solution. RM takes values between zero and one hundred percent (i.e. $0\% \leq \text{RM} \leq 100\%$). In the absence of countermeasures, RM equals 0%.

- ARC is the Annual Response Cost that is incurred by implementing a new security action. ARC is always greater than or equal to zero ($ARC \geq 0$), and it is expressed in currency per year (e.g., $/year).
- AIV is the Annual Infrastructure Value (e.g., Cost of equipment, Services for regular operations, etc.) that is expected from the system, regardless of the implemented countermeasures. ARC is greater than zero ($AIV > 0$), and it is expressed in currency per year (e.g., $/year).

2.2. Attack Surface

The attack surface is a model that measures quantitatively the level of exposure of a given system (i.e., the reachable and exploitable vulnerabilities existing on the system) [18].

2.2.1. Operating Systems Attack Surface

Measuring the attack surface has been initially considered by Howard et al. [19], who propose a method to identify the system's attack vectors (i.e., Target and enablers, Channels and protocols, and Access rights), compare it with other similar systems and use it as an indicator of the system's security. As a result, the more targets, the more channels and the more generous access rights, the larger the attack surface. However, this method presents the following shortcomings: the approach does not provide a systematic method to assign weights to the attack vectors; it focuses on measuring the attack surfaces of operating systems; and it is not possible to determine if all attack vectors have been identified.

2.2.2. Software Systems Attack Surface

Manadhata et al. [10] present an approach to systematically measure the attack surface of different software. The proposed approach measures the attack surface of a software system (e.g., IMAP server, FTP daemons and Operating Systems) based on the analysis of its source code, through three dimensions: methods, channels, and data. Not all resources are part of the attack surface, nor all of them equally contribute to the attack surface measurement.

The approach, however, presents the following shortcomings: the proposed methodology cannot be applied in the absence of source code. The damage potential estimation includes only technical impact (e.g., privilege elevation) and not monetary impact (e.g., monetary loss). The model only compares the level of attackability between two similar systems; no attempt has been made to compare the attack surface of different system environments. The method does not make assumptions about the capabilities of attackers or resources in estimating the damage potential-effort ratio. The methodology does not allow the security administrator to evaluate the impact of multiple attacks occurring simultaneously in a given system.

2.2.3. Other Attack Surface Approaches

Petajasoja et al. [20] propose an approach to analyse a system's attack surface using the Common Vulnerability Scoring System (CVSS). As a result, it is possible to identify most critical interfaces and help in prioritizing the test effort. However, this approach limits the attack surface to known vulnerabilities, it is not meant to be used as a reaction strategy and only compares relative security of similar infrastructures.

Microsoft also released an attack surface analyser tool [21] that identifies changes made to an operating system attack surface by the installation of new software. However the tool can only be used for Windows operating systems and does not measure a network attack surface.

3. Our Approach: The Attack Volume Model

In single attack scenarios, the use of cost sensitive metrics allows the evaluation and selection of security countermeasures. However, for multiple and complex attack scenarios, this approach does not allow security administrators to determine the equipment(s), subject(s), and/or action(s) that take part in a security incident, making it difficult to accurately assess the damage of a complex incident and/or the effectiveness of a group of security countermeasures.

We propose therefore, to extend the surface model into a volume model that will represent systems, attacks and countermeasures in a three dimensional coordinate system representing the user, channel, and resource dimensions.

Similar to the Cartesian Coordinate System, the coordinate system is composed of three dimensions with the following characteristics:

- The system is composed of three orthogonal axes, any two of them being perpendicular,
- There exists a single unit of length for all three axes,
- There exists a single orientation for each axis.

The three axes are bounded by the size of the system. The volume encompassed by the three axes represents the maximum risk at which the system is exposed, and corresponds to the system volume. Inside this volume, we define sub-volumes that correspond to the attacks and/or countermeasures applied on the system.

As a result, the graphical representation of multiple attacks and countermeasures makes it possible to determine not only the impact of each attack and countermeasure (or the impact of a group of them), but also, the residual risk (i.e., the volume of the system that is being attacked but is not covered by any countermeasure), as well as, the potential collateral damage (i.e., the volume of the system that is not being attacked but is covered by a countermeasure, and whose implementation could cause a damage over the target element).

3.1. Volume Definition

A volume is the quantity of three-dimensional space enclosed by some closed boundary. We study three types of volumes: the system volume (the maximal space susceptible to be attacked), the attack volume (part of the system volume that is compromised), and the countermeasure volume (part of the system volume that is protected by a given countermeasure). For each element we define the system dimensions (discussed in Section 4), and we assign a weighting factor depending on the contribution of each axis to the calculation of the volume. This weighting factor corresponds to the criticality of each element represented on the axis. Figure 1 depicts the graphical representation of each type of volume.

3.1.1. System Volume (SV):

It represents the maximal space a given system (e.g., S1) is exposed to users and attackers. This volume includes tangible assets (e.g., PCs, mobile phones, network components, etc.), as well as intangible assets (e.g., confidential information, business reputation, etc) that are vulnerable to known and unknown threats. Each of these assets is represented in the system volume according to three dimensions: user accounts, channels, and/or resources.

3.1.2. Attack Volume (AV):

Within the complete system volume exposed to attackers (including all possible vulnerable resources of the given system), we concentrate on a given attack to identify the portion of the volume being targeted based on the vulnerabilities it can exploit. These vulnerabilities are related to all the dimensions that comprise the system volume (i.e.,user accounts, channels, and resources).

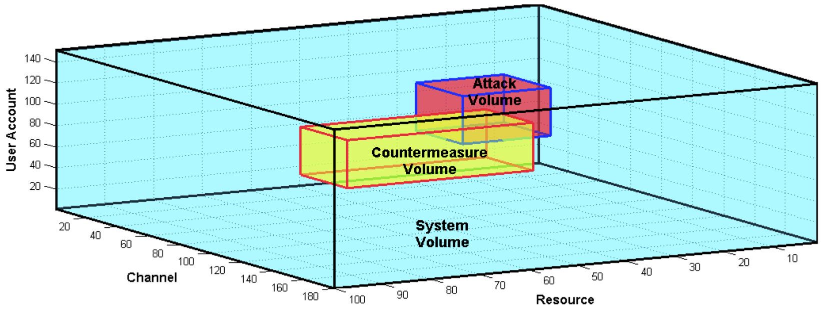


Figure 1: Volume Graphical Representation

3.1.3. Countermeasure Volume (CV):

The countermeasure volume represents the level of action that a security solution has on a given system. In other words, the countermeasure volume is the percentage of the system volume that is covered and controlled by a given countermeasure. An attack is covered by a countermeasure if their volumes overlap. The countermeasure can exceed the attack volume and cover part of the system that is not covered by the attack. Two cases are distinguished:

- Total Coverage, where all exploitable vulnerabilities associated to a given attack A_1 are controlled by a given countermeasure (e.g., C_1), in this case we have a perfect mitigation (100% of the attack volume coverage);
- Partial Coverage, where only a portion of the exploitable vulnerabilities associated to a given attack A_1 is controlled by a given countermeasure (e.g., C_1).

3.2. Volume Calculation

The projection of the three axis in our coordinate system generates a parallelepiped. The volume of such geometric figures is the product of the area of its base 'A' and its height 'h'. The base is any of the six faces of the geometric figure, whereas the height is the perpendicular distance between the base and the opposite face.

The volume calculation requires the computation of the contribution of each axis represented in the coordinate system. The axis contribution is determined as the sum of each set of axis elements of each different type (user account type, resource type, etc.) times its associated weighting factor in the system S, as shown in Equation 2.

$$Co_{Axis}(S) = \sum_{i=0}^{n} Count(E \in Type(Axis)) \times WF_{Type} \tag{2}$$

The remaining of this section details the calculation of the different volumes defined in Section 3.1.

3.2.1. System Volume (SV) Calculation

Consider a system S, which is a vector composed of three elements: a set of user accounts (Acc), a set of IP address and open ports (Ip-Port), and the system's resource (Res). The volume of system S is represented by the vector SV(S) = ($Co_{Acc}(S)$, $Co_{Ip-Port}(S)$, $Co_{Res}(S)$). The system volume is calculated as the product of the axis contribution, as shown in Equation 3.

$$SV(S) = \prod_{Axis \in AXES} Co_{Axis}(S) \tag{3}$$

3.2.2. Attack Volume (AV) Calculation

Consider A as a given attack, $AV_{Acc}(A)$ as the A' user account-based volume, $AV_{Ip-Port}(A)$ as the A' Channel-based volume, and $AV_{Res}(A)$ as the A' resource-based volume. The volume of attack A is represented by the vector: $AV(A) = (Co_{Acc}(A)$, $Co_{Ip-Port}(A)$, $Co_{Res}(A))$. The attack volume is calculated as the product of the axis contribution, as shown in Equation 4.

$$AV(A) = \prod_{Axis \in AXES} Co_{Axis}(A) \tag{4}$$

The coverage (Cov) of a given attack A in the system S is computed as the ratio between the attack volume overlapping with the system volume (AV($A \cap S$)) and the system volume (SV(S)), as shown in Equation 5.

$$Cov(A, S) = \frac{AV(A \cap S)}{SV(S)} \times 100 \tag{5}$$

3.2.3. Countermeasure Volume (CV) Calculation

Consider a given countermeasure C, a set of user accounts as the attack vector 'Acc', a set of IP address and ports as the attack vector 'Ip-Port', and the system's resource as the attack vector 'Res'. The volume of countermeasure C is represented by the vector: $CV(C) = (Co_{Acc}(C)$, $Co_{Ip-Port}(C)$, $Co_{Res}(C))$. The countermeasure volume is calculated as the product of the axis contribution, as shown in Equation 6.

$$CV(C) = \prod_{Axis \in AXES} Co_{Axis}(C) \tag{6}$$

The coverage (Cov) of a given countermeasure (C) respect to a given attack (e.g., A) is calculated as the ratio between the countermeasure volume overlapping with the attack volume (CV($C \cap A$)) and the attack volume (AV(A)), as shown in Equation 7.

$$Cov(C/A) = \frac{CV(C \cap A)}{AV(A)} \times 100 \tag{7}$$

From Equation 7, the higher the ratio, the greater the mitigation level.

4. System Dimensions

In analogy with access control models (e.g., ABAC [22], RBAC [23], OrBAC[24]), we identified three main dimensions that contribute directly to the execution of a given attack: User account (subject), Resource (object), and Channel (the way to execute actions, e.g., connect, read, write, etc). This latter is represented as the transitions between subjects and objects. For instance, in order to access a web-server (object) of a given organization, a user (subject) connects to the system by providing a login and password (action).

4.1. User Account

A user account is a unique identifier for a user in a given system that allows him/her to connect and interact with the system's environment. A user account is associated to a given role in the system, from which his privileges and rights are derived (i.e., system administrator, standard user, guest, internal user, or nobody).

- Super Administrator: Also called *root user*, is the account with the highest level of access within the system (i.e.,permission to view and modify all fields on the system). There are as many super administrators as required in the system.
- System Administrator: It is created by the root user and it is able to view and modify most fields of the system. There are as many systems administrators as required.
- Standard User: It is a limited user account that is granted the right to use most software and system settings that do not affect other users. There are as many standard users as required.
- Guest: This is a user account with a temporary access to the system. Guest accounts have the same access as standard users but it is further restricted by not being able to install software, hardware or change settings. There are as many guests as required.
- Internal User: It is used for a person who has a member status and uses this account to access and interact with the system. An internal user has restricted rights (e.g., it cannot access the administrator interface, but it can perform simple edit operations on the interface). There are as many local users as required.
- Nobody: It is a user account that owns no files, is in no privileged groups, and has no abilities except those which every other user has.

Table 1 presents the different categories of user accounts according to their associated rights and privileges.

Table 1: User Account Categories

User Account	**Rights and Privileges**			
	Read	**Write**	**Modify**	**Admin Access**
Super Admin	all	all	all	yes
System Admin	all	most	most	yes
Standard User	all	some	some	no
Guest	all	few	few	no
Internal User	all	few	few	no
Nobody	all	none	none	no

4.2. Channel

In order to have access to a particular resource, a user must use a given channel. This section considers the IP address and the port number to represent channels in TCP/IP connections. However, each organization must define the way its users connect to the system and have access to the organization's resources.

4.2.1. IP Address

The Internet Protocol (IP) address is a unique numerical label assigned to each device on a network (e.g., PC, printer). The IP address offers two main functions: (i) Identification of the host or network interface, and (ii) Location addressing [25]. There are two versions of the IP addresses: IPv4 [26]; and IPv6 [27]. IP address can be either public, private, or reserved for special purposes [29, 28]. Examples of IP addresses are depicted in Table 2.

Table 2: IP Address Categories

IP Address Types	**Characteristics**	**Examples**
Public	any address or number assigned to a device accessible over the Internet	1.0.0.0/8, 9.0.0.0/8, 129.0.0.0/8
Private	any address or number assigned to a device accessible only within a LAN	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
Reserved/ Special purpose	any address or number reserved for a specific purpose e.g., loop-back, broadcast, etc	127.0.0.0/8, 255.255.255.255/32, 240.0.0.0/4

4.2.2. Port Number

A port is an application-specific or process-specific software construct, serving as a communication end-point in a computer's host operating system.

Port numbers are divided into 3 ranges: well-known ports, from 0 through 1023 (e.g., 20: File Transfer Protocol, 25: Simple Name System Protocol, etc.); registered ports, from 1024 through 49151; and dynamic or private ports, from 49152 through 65535 [29]. Table 3 presents the different categories of port numbers according to their use by applications [30].

Table 3: Port Number Categories

Class	**Characteristics**	**Port Numbers**
1	Well-known and widely used	20, 21, 22, 23, 25, 53, 80, 110, 119, 143, 161, 443
2	Well-known and not widely used	From 0 to 1023 except ports from Class 1
3	Registered official ports that are used by multiple applications	1109, 1200, 1337, 1521, 1550, 1761, 2049, 2082, 2083, 2086, 2105, 2210, 2211, 2212, 2399, 2809, 4662, 5000, 5001, 5150, 5228, 5281, 6005, 6100, 6112, 6888, 6969, 7787, 7788, 7937, 8000, 8008, 8080, 8880, 8887, 8888, 9001, 9080, 9800, 9898, 15000, 20000, 26000
4	Registered official ports and not widely used	From 1024 to 49151 except ports from Class 3
5	Private ports	From 49152 to 65535

4.3. Resource

A resource is either a physical component (e.g., host, server, printer) or a logical component (e.g., files, records, database) of limited availability within a computer system. We identify three elements from the URI generic syntax (i.e., path, query, and fragment) that can be exploited to have access to a given resource. It is important to recall that the path section of a URI contains data organized in hierarchical form, that along with the non-hierarchical query component, serves to identify a resource. In addition, the query and fragment sections of a given URI allow indirect identification of a secondary resource [11].

We defined two levels of privileges (i.e., kernel, user), and seven level of transitions (i.e., read, write, execute, and their combinations), and we assigned numerical values to each privilege and transitions based on their characteristics. Table 4 summarizes these values.

Table 4: Privilege and Access Right Values for Resources

Privilege	**Characteristic**	**Value**	**Transition**	**Characteristic**	**Value**
Kernel	Complete access to all files and commands, including the system's kernel.	3	R	Read file names without additional information (e.g., content, size, type)	9
User	Limited access to files and applications.	1	W	Modify a file or entries in a directory (e.g., create, delete, rename)	6
			X	Execute and access files.	6
			R-W	Read and write	4
			R-X	Read and execute	4
			W-X	Write and execute	4
			R-W-X	Read, write and execute	3

5. Unit Volume Construction

As previously stated, a bijection between the URIs and the coordinate system is required in order to make the appropriate transformations. A bijection is a function giving an exact pairing of the elements of two sets. To have an exact pairing between X and Y (where Y needs to be different from X), four conditions must hold:

1. each element of X must be paired with at least one element of Y,
2. no element of X may be paired with more than one element of Y,
3. each element of Y must be paired with at least one element of X,
4. no element of Y may be paired with more than one element of X.

In formal mathematical terms, the function f: X→Y is bijective if and only if for all y∈Y there is a unique x∈X such that f(x)=y.

Each axis contributes differently in the volume calculation. This contribution represents the impact of a given element in the execution of an attack. Following the CARVER methodology [12, 13], we assign a weighting factor to each element represented in our coordinate system. The remaining of the section details this methodology and the intra-dimension normalization.

5.1. Carver Methodology

Norman[12] and the Federation of American Scientists[13] propose a methodology to measure the priority of each element in a given system, based on the following factors:

- **Criticality (C):** measures the impact that an asset has on carrying out the organization's mission. A target is said to be critical when its destruction or damage has a significant impact on production or service. Criticality depends on several factors such as: time (e.g., the speed at which the impact of a target affects operations), quality (e.g., the level of damage caused to output, production or service), surrogate (e.g., effect in the output, production or service), relativity (e.g., number of targets, position, relative value).
- **Accessibility (A):** refers to the ability and means to communicate or interact with a system, use system resources to handle information, gain knowledge of the information the system contains, or control system components and functions.
- **Recuperability (R):** measures the time that a target needs to replace, repair, or bypass destruction or damage. Recuperability varies with the available sources and type of targeted components.
- **Vulnerability (V):** is a weakness in an information system, system security procedures, internal controls, or implementation that can be exploited or triggered by a threat source. A target is vulnerable if the operational element has the means and expertise to successfully attack the target.
- **Effect (E):** measures all significant impact (whether desired or not), at the target and beyond, that may result once the selected target is attacked.
- **Recognizability (R):** is the degree to which a target can be recognized by an operational element. Factors such as the size and complexity of the target, the existence of distinctive signatures, the presence of masking or camouflage influence the level of recognizability of a given target.

The methodology assigns numerical values on a scale of 1 to 10 to each considered factor and places them in a decision matrix. The sum of the values indicate the severity of a given dimension.

5.2. Intra-dimension Normalization

Each category within the axis contributes differently to the volume calculation. The weighting factor corresponds to the severity of a given category based on CARVER. The remaining of this section details the weighting factor assigned to each category of the coordinate system's dimensions.

5.2.1. User Account

We have previously defined six categories of user accounts (i.e., super administrator, system administrator, standard user, guest, internal user, and nobody). Each user account category has an associated weighting factor that corresponds to the CARVER analysis, as shown in Table 5.

5.2.2. Channels

We have previously defined the most commonly used channels in TCP/IP connections (i.e., IP address and port numbers). This section presents the normalization of these channels according to their contribution in the volume measurement.

IP Address. We assigned a weighting factor to each category of IP address. As a result, public IP addresses are assigned a weighting factor of 3 units, since they are more likely to be used in the execution of an attack. Private IP addresses are assigned a weighting factor of 1 unit, and reserved/special purpose IP address are assigned a weighting factor of 0 units, since they are not very likely to be used in the execution of an attack.

Table 5: Intra-dimension Weighting Factor

	Dimension	C	A	R	V	E	R	Total	WF
User Account	Super Admin	10	9	8	10	10	9	56	5
	System Admin	8	8	7	9	8	7	47	4
	Standard User	6	7	6	7	7	5	38	3
	Internal User	4	5	4	6	5	5	29	2
	Guest	3	3	2	5	4	2	19	1
	Nobody	1	1	1	1	1	1	6	0
IP-Port	Class 1	10	9	8	8	7	8	50	4
	Class 2	8	7	6	5	5	6	39	3
	Class 3	7	8	5	7	5	6	38	3
	Class 4	3	2	3	4	3	5	20	1
	Class 5	2	1	1	3	1	1	9	0
	Public	8	7	5	7	6	5	37	3
	Private	5	1	4	3	4	3	20	1
	Reserved/ Special purpose	2	1	3	1	1	1	9	0
Resource	Kernel & R-W-X	10	10	9	9	9	9	56	5
	Kernel & W-X/R-X/R-W	8	9	9	9	7	8	50	4
	Kernel & R/W/X	6	7	7	8	7	5	40	3
	User & R-W-X	5	5	7	7	6	6	36	3
	User & W-X/R-X/R-W	5	5	6	5	4	5	30	2
	User & W/X	3	3	5	3	2	3	19	1
	User & R	1	2	2	1	1	3	10	0

Port Number. We assigned a weighting factor that ranges from 0 to 4 to each of the 5 previously defined categories of port numbers. Class 1 ports are more likely to be used in the execution of an attack, representing a weighting factor of 4 units. Class 2 and 3 ports are less likely to be used in the execution of an attack, representing a weighting factor of 3 units. Class 4 ports represent a weighting factor of 1 unit, and Class 5 Ports are not very likely to be used in the execution of an attack, representing a weighting factor of 0 units.

The resulting IP-Port couple is then represented as the sequence of affected IP address, followed by the active port numbers in ascending order (e.g., IP_1, IP_2, ..., IP_n, $Port_1$, $Port_2$, ..., $Port_n$).

5.2.3. Resource

Resources are used to attack a given system only if the attacker has the appropriate access rights and privileges. However, in order to acquire the required permissions, attackers must spend some effort. We assigned a weight to each resource based on the effort to obtain the access rights and privileges associated to a given resource, as shown in Table 5.

The index that results from the division between the Privilege (PR) value and the Transition (TR) value (i.e.,$\frac{PR}{TR}$) represents the level of access assigned to a given resource on the system.

As a result, a compromised resource with a kernel privilege and Read-Write-Execute transition is assigned a weight of 5 units; a kernel privilege and Read-Write, Read-Execute, or Write-Execute transition is assigned a weight of 4 units; a kernel privilege with Read, Write or Execute transition is assigned a weight of 3 units. Similarly, a compromised resource with a user privilege and Read-Write-Execute transition is assigned a weight of 3 units; a user privilege with Read-Write, Read-Execute, or Write-Execute transition is assigned a weight of 2 units; a user privilege with Write or Execute transition is assigned a weight of 1 unit; and a user privilege with a Read-only transition is assigned a weight of 0 units.

6. Attack Volume Union and Intersection

The calculation of the Attack Volume (AV) for multiple attacks requires the identification of their union and intersection. The union of two or more attack volumes is bounded and ranges from the maximum volume of the group of attacks in its lower bound, to the sum of the individual volumes in its upper bound (Equation 8). The intersection of two or more attack volumes ranges from zero in its lower bound, to the minimum volume of the group of attacks in its upper bound (Equation 9).

$$AV(A_1 \cup ... \cup A_n) \in \Big[max(AV(A_1), ..., AV(A_n)) - \sum AV(A_1), ..., AV(A_n)\Big] \tag{8}$$

$$AV(A_1 \cap ... \cap A_n) \in [0 - min(AV(A_1), ..., AV(A_n))] \tag{9}$$

Two cases can be distinguished in the calculation of the volume union and intersection: joint and disjoint attack volumes.

6.1. Disjoint Attack Volumes

The volume of one attack is disjoint from another attack volume if they have no elements in common. Therefore, having n number of disjoint attacks $(A_1, ..., A_n)$, the volume of their union and intersection is calculated using Equations 10 and 11 respectively.

$$AV(A_1 \cup ... \cup A_n) = \sum_{i=1}^{n} AV(A_i) \tag{10}$$

$$AV(A_1 \cap ... \cap A_n) = 0 \tag{11}$$

From the previous equations, we derive the following definition:

Given two attacks (A_1, A_2), Attacks A_1 and A_2 are disjoint if their combined volume has no element in common, therefore, the attack volume of the union is calculated as the sum of their individual volumes, and the attack volume of the intersection is equal to 0, as shown in Equation 12:

$$\text{iff } A_1 \cap A_2 = \varnothing \begin{cases} AV(A_1 \cup A_2) = AV(A_1) + AV(A_2) \\ AV(A_1 \cap A_2) = 0 \end{cases} \tag{12}$$

6.2. Joint Attack Volumes

The Volume of one attack is partially or totally covered by another attack if they share some or all of their elements. For n number of partially covered attacks (e.g., $A_1, ..., A_n$), the union is calculated as the sum of the individual attack volumes minus their intersections (Equation 13), and the intersection volume is calculated as the sum of the individual attack volumes minus their union (Equation 14).

$$\begin{aligned} AV(A_1 \cup ... \cup A_n) \quad &= \textstyle\sum_{i=1}^{n} AV(A_i) - \sum_{i,j=1}^{n} \binom{n}{2} AV(A_i \cap A_j) \\ &+ \textstyle\sum_{i,j,k=1}^{n} \binom{n}{3} AV(A_i \cap A_j \cap A_k) + ... + \\ &(-1)^{n+1} AV(A_i \cap ... \cap A_n) \end{aligned} \tag{13}$$

$$\begin{aligned} AV(A_1 \cap ... \cap A_n) \quad &= \textstyle\sum_{i=1}^{n} AV(A_i) - \sum_{i,j=1}^{n} \binom{n}{2} AV(A_i \cup A_j) \\ &+ \textstyle\sum_{i,j,k=1}^{n} \binom{n}{3} AV(A_i \cup A_j \cup A_k) + ... + \\ &(-1)^{n+1} AV(A_i \cup ... \cup A_n) \end{aligned} \tag{14}$$

From the previous equations, we derive the following definitions:

Given two attacks (A_1, A_2), Attacks A_1 and A_2 are joint if their combined volume has at least one element in common, therefore, the attack volume of the union is calculated as the sum of their individual volumes minus their intersection, and the attack volume of the intersection is calculated as the sum of their individual volumes minus their union, as shown in Equation 15.

$$\text{iff } A_1 \cap A_2 \neq \varnothing \begin{cases} AV(A_1 \cup A_2) = & AV(A_1) + AV(A_2) - AV(A_1 \cap A_2) \\ AV(A_1 \cap A_2) = & AV(A_1) + AV(A_2) - AV(A_1 \cup A_2) \end{cases} \tag{15}$$

Given two attacks (A_1, A_2), Attack A_1 is a subset of Attack A_2 if the volume of A_1 is a subset of the volume of A_2 (AV(A_1)$\subseteq$ AV(A_2)), therefore, the attack volume of the union is equal to the attack volume of the bigger attack, and the attack volume of the intersection is equal to the attack volume of the smaller attack, as shown in Equation 16.

$$\text{iff } A_1 \subseteq A_2 \begin{cases} AV(A_1 \cup A_2) & = AV(A_2) \\ AV(A_1 \cap A_2) & = AV(A_1) \end{cases} \tag{16}$$

Given two attacks (A_1, A_2), Attacks A_1 and A_2 have the same volume if Attack A_1 is a subset of Attack A_2 and Attack A_2 is a subset of Attack A_1, therefore, the attack volumes of the union and the intersection are the same as their individual attack volume (Equation 17).

$$\text{iff } A_1 \subseteq A_2 \wedge A_2 \subseteq A_1 \rightarrow AV(A_1 \cup A_2) = AV(A_1 \cap A_2) = AV(A_1) = AV(A_2) \tag{17}$$

Given two attack volumes as introduced in Equation 4 (e.g., $AV(A_1) = (Co_{Acc}(A_1), Co_{Ip-Port}(A_1), Co_{Res}(A_1))$; $AV(A_2) = (Co_{Acc}(A_2),\ Co_{Ip-Port}(A_2),\ Co_{Res}(A_2))$, the attack volume intersection is calculated as the sum of all elements 'E' that are included in both set of volumes times their corresponding weighting factor, as shown in the following equation:

$$AV(A_1 \cap A_2) = Co_{Acc}(A_1 \cap A_2) \times 2 \times Co_{Ip-Port}(A_1 \cap A_2) \times 1 \times Co_{Res}(A_1 \cap A_2) \times 1,5 \tag{18}$$

where:

$Co_{Acc}(A_1 \cap A_2) = \sum_{i=0}^{n}(E_i \times WF(E_i) \mid E_i \in A_1 \wedge E_i \in A_2)$.
$Co_{Ip-Port}(A_1 \cap A_2) = \sum_{i=0}^{n}(E_i \times WF(E_i) \mid E_i \in A_1 \wedge E_i \in A_2)$.
$Co_{Res}(A_1 \cap A_2) = \sum_{i=0}^{n}(E_i \times WF(E_i) \mid E_i \in A_1 \wedge E_i \in A_2)$.

From the previous equations, 'E' represents the elements associated to each attack dimension (i.e., IP address, channel, and resource) that are compromised during the execution of a given attack, and 'WF(E_i)' corresponds to the weighting factor of the element E_i as proposed in Section 5.1.

6.3. Dimension-based Attack Volume Calculation

The calculation of the attack volume union and intersection based on a given dimension derives Equations 19 and 20.

$$Co_{Vec}(A_1 \cup A_2) = Co_{Vec}(A_1) + Co_{Vec}(A_2) - Co_{Vec}(A_1 \cap A_2) \tag{19}$$

$$Co_{Vec}(A_1 \cap A_2) = \sum_{E \in Vec_1 \cap Vec_2} WF(E) \tag{20}$$

Given two attacks (A_1, A_2), a set of elements Vec_1=\{E_1, E_2, ...E_n\} that are targeted by A_1 in this dimension, and a set of elements Vec_2=\{E_a, E_b, ...E_x\} that are targeted by A_2, the contribution of the union to the volume is calculated as the sum of each individual volumes minus their intersection. The intersection of both attacks is calculated as the sum of the elements that belong to both dimensions (Vec_1, Vec_2) times their corresponding weighting factor.

The remaining of this section details the methodology to calculate the attack volume union and intersection for each attack dimension.

6.3.1. User Account

Given two attacks (A_1, A_2), a set of user accounts UA_1=$\{Acc_1,\ Acc_2,\ ...Acc_n\}$ that are targeted by A_1, and a set of user accounts UA_2=$\{Acc_a,\ Acc_b,\ ...Acc_x\}$ that are targeted by A_2, the volume intersection of both attacks based on the user account dimension is calculated as the elements that belong to both set of user accounts (UA_1, UA_2) times their corresponding weighting factor, as shown in Equation 21.

$$\begin{aligned} Co_{Acc}(A_1 \cap A_2) = \quad & Count(admin \in UA_1 \wedge UA_2) \times WF(admin) + \\ & Count(std\_user \in UA_1 \wedge UA_2) \times WF(std\_user) + \\ & Count(int\_user \in UA_1 \wedge UA_2) \times WF(int\_user) + \\ & Count(guess \in UA_1 \wedge UA_2) \times WF(guess) \end{aligned} \tag{21}$$

6.3.2. Channel

As previously presented, the contribution of the channel dimension ($Co_{Ip-Port}$) in the volume calculation is determined as the sum of the contributions of the IP address and the Port number. The remaining of this section defines the calculation of each channel element.

IP Address. Given two attacks (A_1, A_2), a set of IP address I_1=$\{IP_1,\ IP_2,\ ...,\ IP_n\}$ that are targeted by A_1, and a set of IP address I_2=$\{IP_a,\ IP_b,\ ...IP_x\}$ that are targeted by A_2, the volume intersection of both attacks based on the IP address is calculated as the elements that belong to both set of IP addresses (I_1, I_2) times their corresponding weighting factor. The contribution (Co) of the IP address is shown in Equation 22.

$$\begin{aligned} Co_{Ip}(A_1 \cap A_2) = \quad & Count(Public\_IP \in I_1 \wedge I_2) \times WF(Public\_IP) + \\ & Count(Private\_IP \in I_1 \wedge I_2) \times WF(Private\_IP) \end{aligned} \tag{22}$$

Port Number. Given two attacks (A_1, A_2), a set of port numbers P_1= $\{Port_1,\ Port_2,\ ...Port_n\}$ that are targeted by A_1, and a set of IP address P_2= $\{Port_a,\ Port_b,\ ...Port_x\}$ that are targeted by A_2, the volume intersection of both attacks based on the port number is calculated as the elements that belong to both set of port numbers (P_1, P_2) times their corresponding weighting factor, as shown in Equation 23.

$$\begin{aligned} Co_{Port}(A_1 \cap A_2) = \quad & Count(class1 \in P_1 \wedge P_2) \times WF(class1) + \\ & Count(class2 \in P_1 \wedge P_2) \times WF(class2) + \\ & Count(class3 \in P_1 \wedge P_2) \times WF(class3) + \\ & Count(class4 \in P_1 \wedge P_2) \times WF(class4) \end{aligned} \tag{23}$$

6.3.3. Resource

Given two attacks (A_1, A_2), a set of resources R_1=$\{Res_1,\ Res_2,\ ...Res_n\}$ that is targeted by A_1, and a set of resources R_2=$\{Res_a,\ Res_b,\ ...Res_x\}$ that is targeted by A_2, the volume intersection of A_1 and

A_2 based on the resource dimension is calculated as the sum of the elements that belong to both set of resources (R_1, R_2) times their corresponding weighting factor, as shown in Equation 24.

$$Co_{Res}(A_1 \cap A_2) = \sum_{R \in R_1 \cap R_2} WF(R) \tag{24}$$

7. Implementation and Results

We developed a software application (cf. `http://j.mp/3d-rori`) to generate the graphical representation of multiple attacks and countermeasures within a particular system, and to evaluate, rank, and select optimal countermeasures against complex attacks.

This section describes the Decision Support platform and the resulting geometrical figures, as well as, the process of selecting optimal countermeasures.

7.1. Platform Description

The decision support platform is composed of two main modules: The Attack Volume application, and the RORI application. These two modules are described next.

7.1.1. Attack Volume Application

This module is composed of three elements: a graphical interface, an AV engine and an AV database, whose mission is to graphically represent attacks and countermeasures in a three-dimensional system and calculate the monetary impact of individual and multiple attacks (i.e. ALE), as well as the coverage of single and multiple countermeasures (i.e., Cov(CM)).

- **AV Graphical Interface:** This element requests the AV Engine to perform the volume evaluation of particular systems, attacks, and/or countermeasures to display their graphical representation. Results of these evaluation (e.g., ALE, Cov(CM), AV(A)) are then transmitted to the RORI application for further analysis.
- **AV Engine:** This element receives a request either from the AV graphical interface or from the RORI application to evaluate the volume of one or several systems, attacks or countermeasures. The AV Engine requests the input data to particular services (e.g., LDAP, databases, ACL, servers) and retrieves the associated RCU (Resource-Channel-User) information in order to calculate its volume and plot its graphical representation. The retrieved RCU data is stored in the AV database.
- **AV Database:** It contains the RCU information related to the system, including the attacks at which the RCU elements are vulnerable,and the countermeasures that could be implemented to protect them in case of a security incident. Each RCU element is assigned a unique identifier and a weight factor based on the CARVER methodology. Information about resources contains the resource ID, type, privilege, transition, weight factor, vulnerabilities, and countermeasures. Information about channels contains channel ID, type, weight factor, vulnerabilities, and countermeasures. Information about users contains the user ID, role, rights, privileges, weight factor, vulnerabilities, and countermeasures.

7.1.2. RORI Application

This module is composed of three elements: a decision-related user interface, a RORI engine and a RORI database, whose mission is to perform the evaluation of individual and combined countermeasures and propose the optimal candidate based on the RORI index.

- **Decision-related user interface:** This element requests the RORI Engine to perform the countermeasure evaluation evaluation (e.g., individual and combined) for a given attack scenario. Countermeasures are ranked based on the RORI index. The RORI results are displayed in the user interface to help security administrators in the decision making process.
- **RORI Database:** It contains the information related to the organization (e.g., security equipment name, type, cost), to the security incident (e.g., name, severity, likelihood), and to the countermeasure (e.g., name, effectiveness, coverage, cost).
- **RORI Engine:** This element receives a request from the decision-related user interface to evaluate, rank and select optimal countermeasures against a given attack. The RORI Engine requests the input parameters (i.e., ALE, AIV, ARC, RM) to the RORI database through a get command. If the ALE or the RM are missing for that particular security incident, the RORI engine will request the AV Engine to perform the attack volume evaluation and to provide the corresponding values. Upon reception of all the parameters, the RORI engine stores them in the RORI database through a push command, and performs the individual evaluation of all the countermeasures. Non-restrictive candidates are selected to be combined in groups of up to n elements.

7.2. Input Data

For testing purposes, we stored in the AV database the RCU information of 2 stations, i.e., Control Station (CS), and Visualization Station (VS), from a Critical Infrsatructure Control System. The data presented in Table 6 have been selected to illustrate the deployment of our tool.

Table 6: RCU Summary Information

Dimension	**Type**	**Range**	**Q**	**WF**	**Start**	**End**	**Station**
Resource	Sensor	R1:R150	150	5	0	750	all
	Actuator	R151:R215	65	3	750	945	all
	RTU	R216:R255	40	2	945	1025	all
	Gateway	R256:R257	1	5	1025	1030	all
	MTU	R257:R258	1	5	1030	1035	all
	Server	R258:R262	5	4	1035	1055	CS
	Database	R263:R266	4	4	1055	1071	CS
	Workstation	R267:R284	18	2	1071	1107	CS
	Server	R285:R288	4	4	1107	1123	VS
	Database	R289:R291	3	4	1123	1135	VS
	Workstations	R292:R304	12	2	1135	1159	VS
Channel	Public IP	Ch1:Ch215	215	3	0	645	CS
	Public IP	Ch216:Ch421	206	3	645	1263	VS
User Account	Admin	U1:U6	6	5	0	30	CS
	Standard user	U7:U31	25	3	30	105	CS
	Internal user	U32:U65	34	2	105	173	CS
	Admin	U66:U78	13	5	173	238	VS
	Standard user	U79:U100	22	3	238	304	VS
	Internal user	U101:U138	38	2	304	380	VS

The information is organized by dimension (i.e., resource, channel, user), and type (e.g., server, public IP, standard user), from which we know the range of elements, the quantity (Q), and the associated weighting factor (WF). Each element is represented as a segment in the coordinate system with a start point (Start) and an end point (End). The length of the segment is determined by the weighting factor.

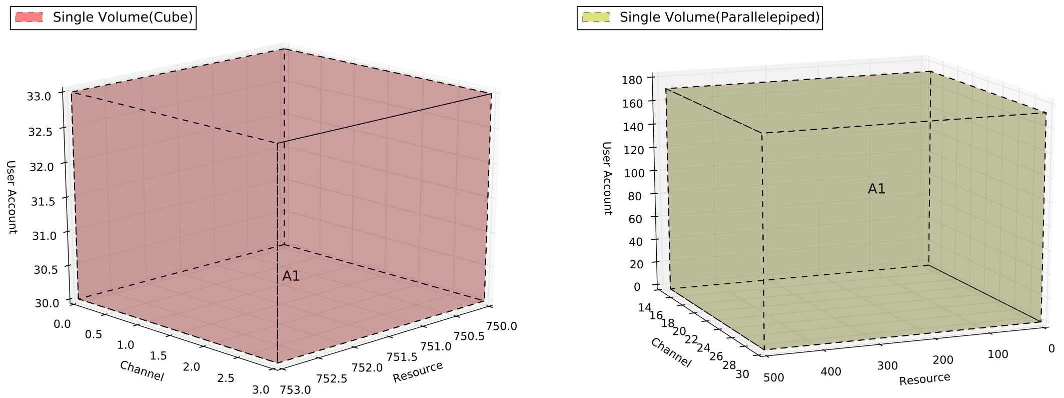
Elements either belong to a single department (e.g., CS, VS) or to all departments of the organization (all).

7.3. Resulting Geometrical Figures

A variety of cases results from the analysis of the RCU elements included in a system, an attack or a countermeasure. The remaining of this section details all the different cases.

7.3.1. Single Volumes

A volume results from the projection of at least one element from the 3 axes of our coordinate system. Two types of volumes are generated: cubes and parallelepipeds.



(a) Single Volume (cube)

(b) Single Volume (parallelepiped)

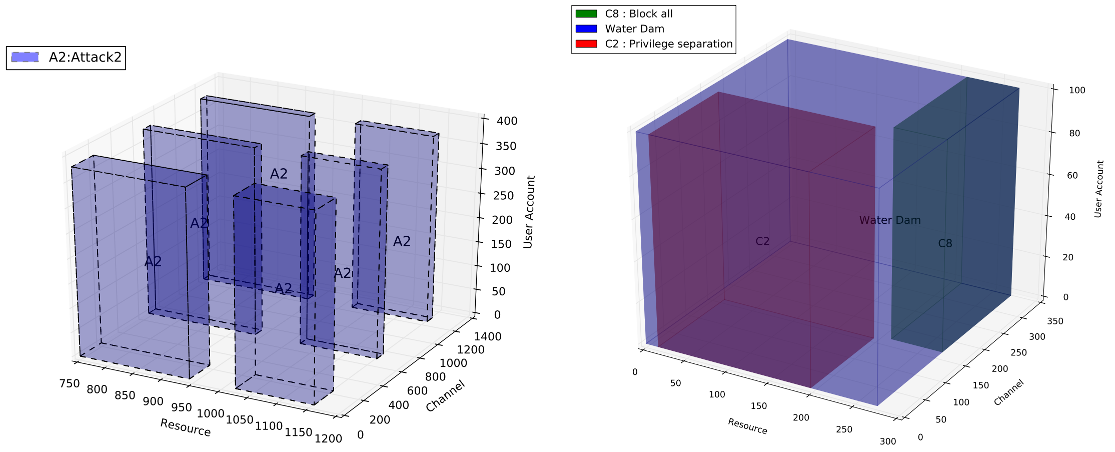
Figure 2: Single Volumes

Figure ??(a) shows the graphical representation of a single resource (i.e., R151:R151), a single channel (i.e., Ch1:Ch1), and a single user (i.e., U7:U7). Since there is an equal number of elements affected in each axis with the same weighting factor, its projection results into a cube. Figure ??(b) depicts the graphical representation of a group of consecutive resources (i.e., R1:R100), channels (i.e., Ch5:Ch10), and users (i.e., U1:U65) affected to a particular incident. The projection of these axes results into a parallelepiped.

7.3.2. Multiple Volumes

Multiple volumes result either when plotting a range of non consecutive RCU elements that belong to the same incident, or when plotting simultaneously several systems, attacks and/or countermeasures. For instance, if a given attack (e.g., A2) has as target the following resources (R151:R215 & R256:R304), channels (Ch1:Ch65 & Ch216:239 & Ch401:421), and users (U1:U138), its graphical representation will result into six disjoint parallelepipeds (all with the same colors), as shown in Figure 3(a). When plotting multiple volumes (i.e., systems, attacks, and/or countermeasures) simultaneously, each figure is assigned a unique color, as shown in Figure 3(b).

Three cases are distinguished when multiple volumes are analysed simultaneously: totally joint, totally disjoint, and partially joint volumes.



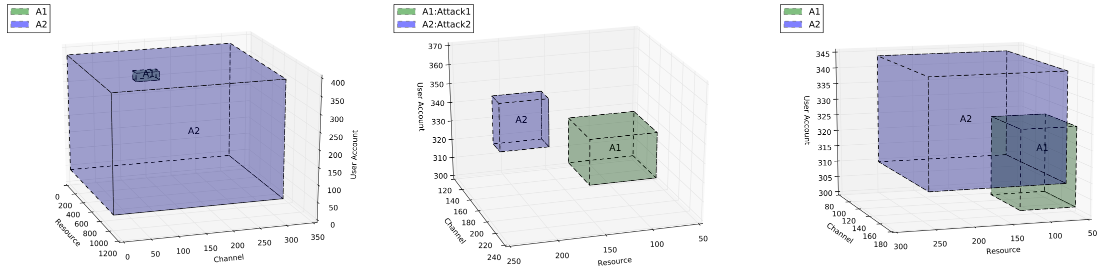
(a) Single Incidents

(b) Multiple Incidents

Figure 3: Multiple Volumes

Totally Joint Volumes. Figure 4(a) depicts the graphical representation of two totally joint volumes (i.e., the volume of one element is totally covered by the volume of a second element). For instance, let us suppose that attack A_1 has as target [R10:R25, Ch40:Ch55, U100:U111] and attack A_2 has as target [R1:R250, Ch1:Ch105, U10:U138]. Attack A_2 targets a wider range of RCU elements (including the target of attack A_1), therefore, only Attack A_2 is analysed and countermeasures for this latter are proposed to face both attacks.

Totally Disjoint Volumes. Figure 4(b) depicts the graphical representation of two totally disjoint volumes (i.e., they affect different RCU elements). For instance, given an attack A_1 that targets [R10:R25, Ch40:Ch55, U100:U111], and attack A_2 that targets [R40:R50, Ch70:Ch75, U120:U131], their volumes are disjoint since they have no target in common, therefore, they are treated individually, assuming that countermeasures for A_1 do not generate conflicts with those for A_2. The volume of attack A_1 is therefore independent of the volume of attack A_2.



(a) Totally Joint

(b) Totally Disjoint

(c) Partially Joint

Figure 4: Joint/Disjoint Volumes

Partially Joint Volumes. Figure 4(c) depicts the graphical representation of two partially joint volumes (i.e., they share some of the RCU elements). For instance, let us suppose that attack A_1 has as target

[R10:R25, Ch40:Ch55, U100:U111], and attack A_2 has as target R20:R51, Ch29:Ch59, U109:U120. Both attacks share only a portion of the RCU elements (i.e., R20:R25, Ch40:Ch55, U109:U111).

7.4. Countermeasure Analysis

The selection of the appropriate countermeasure requires the analysis of all candidates and their combinations. In order to combine multiple countermeasures, we need to compute the portion of the attack volume that is covered by a given countermeasure. We perform geometrical operations to determine the union and intersection of multiple volumes, making it possible to compute the coverage of each alternative.

7.4.1. Countermeasure Coverage:

Each countermeasure is represented as a geometrical figure that covers a set of resources, channels, and users (RCU) from a given system. Such coverage is calculated using Equation 7. For this, it is necessary to determine the RCU elements that belong to both: the attack and the selected countermeasure.

For instance, considering that A_1 affects resources R1:R6, channels Ch1:Ch91, and users U1:U25 (AV(A_1) = 712,530 $units^3$); and countermeasure C_1 protects resources R3:R15, channels Ch51:Ch101, and users U1:U10 (CV(C_1)= 417,690 $units^3$), the RCU elements that are covered by C_1 respect to A_1 are the following: resources R3:R6, channels Ch51:Ch91, and users U1:U10. The coverage volume of C_1 with respect to A_1 is therefore equivalent to

$$CV(C_1 \cap A_1)= [(4 \times 5) \times (41 \times 3) \times ((6 \times 5) + (4 \times 3))]= 103{,}320\ units^3.$$

The countermeasure coverage of C_1 with respect to A_1 is calculated as:

$$Cov(C_1/A_1) = \frac{103{,}320 units^3}{712{,}530 units^3} \times 100 = 14.50\%$$

As a result, only 14.50% of the total volume of A_1 is covered by C_1. The remaining 85.50% of the attack is considered as a residual risk. In addition, Since the volume of C_1 is equal to 417,690 $units^3$ and the coverage volume of C_1 with respect to A_1 is equivalent to 103,320 $units^3$, the difference of these two parameters results into a potential collateral damage (i.e., RCU elements that need to be affected by a particular countermeasure even though they are not vulnerable to a given attack). The resulting collateral damage is equivalent to 314,370 $units^3$, which represents 75,26% of the total countermeasure volume.

7.4.2. Countermeasure Evaluation

The process starts with the selection of all security measures to evaluate and the calculation of their RORI index using Equation 1. The quantification of the parameters composing the RORI model is a task that can be achieved within 3 to 4 hours of discussion with system administrators and use case providers. A complete methodology to estimate each RORI parameter is proposed in [9].

The RORI platform stores all the security information regarding the organization (e.g., cost of the security infrastructure), the attacks (e.g., severity, likelihood), and the countermeasures (e.g., cost, benefit). If all the RORI parameters are known, the RORI engine performs the evaluation by using Equation 1. However, if one or more parameters are missing, the RORI engine requests the administrator to provide them manually or to request them to the AV platform. This latter performs the attack volume evaluation and to provide the corresponding values of ALE and Cov(CM).

Upon reception of all the RORI parameters, the RORI engine evaluates all individual candidates and ranks them in descendant order based on their associated RORI index. Each countermeasure is presented along with the RCU elements it covers and their possible associated restrictions.

A combined evaluation is then performed among all selected candidates (those that are not totally restrictive), making it possible to select the countermeasure or group of countermeasures with the highest RORI index, thus the highest benefit to the organization.

Selected countermeasures are then translated into their corresponding actions for implementation in the system. For instance, blocking a particular channel may be translated into a command to deny all traffic coming/going through a given port (e.g., 8080) in the system's firewall.

8. Use Case: Critical Infrastructure Process Control

This section describes a use case provided by a telecommunication enterprise operating in the field of Information and Communication Technology (ICT) services. The case study responds to the needs of improving the security of a system whose mission is to control a critical infrastructure, specifically a dam. The following subsections describe the case study and detail two scenarios of attack, as well as the general operations required to rank, select and deploy optimal countermeasures.

8.1. General Description

The features of a dam infrastructure are strictly related to the aims they are conceived for. Mostly dams are used for water supplying, hydroelectric power generation, water activities and wildlife habitat granting.

The reference system architecture involves SCADA components (i.e., Supervisory Control And Data Adquisition system targeted to monitoring and controlling infrastructure, and industrial facility based processes). Three main groups of components are identified in the system: control devices (e.g., workstations, databases, HMI, shared resources); I/O devices (e.g., sensors and actuators components), and a SCADA gateway.

The monitoring relies on typical Automated Data Acquisition System (ADAS) components with Remote Terminal Unit (RTU) devices. The supervisor gathers and delivers data from and to a Control and a Visualization Station. The Control Station allows on-line and real time data analysis as well as data and event storing. The Visualization Station presents historical data stored in a database through a web server interface. Sensors and actuators are responsible for retrieving measurements related to specific physics phenomena. The SCADA gateway is responsible for evaluating, processing, storing retrieved measurements and elaborating proper commands for the actual system.

8.2. Attack Scenarios

This section describes two scenarios of attack against a critical infrastructure process control and its corresponding risk analysis.

8.2.1. Attack 1 - Control Station Hacking

A machine connected to the visualization station succeeds in controlling remotely a machine in the control station (through password theft, bug exploit, and other techniques). Consequently, the malicious user modifies sensor settings (e.g., policies and alerting thresholds) and sends commands to the actuators, asking them to maintain the monitoring values under the new thresholds.

The hypothesis is that the attacker has access to the remote machine with a stolen password, he does not install any malicious software, but he knows packet format, and generates well-formed packets. The visualization station is located in a DMZ branch of the LAN, while the control station is in a protected branch of the LAN. The traffic between the two subnets passes through a firewall. A constraint of the system is that the commands to drive the actuators can be made only from the control station.

A control station hacking attack has an estimated *Serious* severity level (equivalent to 1M€) since, if the attack is realized, an extended part of the system can be damaged, and an extended loss of business confidence can be experienced. Likewise, the damage is not estimated to permanently destroy the system, but a large amount of service is estimated to be compromised.

The likelihood for this attack can be estimated as *Negligible* (equivalent to 0.05 times per year), since the control station is highly protected. The estimated value is very indicative because the probability of occurrence of an attack depends on many factors such as: motivation, ability of the attacker, type of the attacker (i.e. employee or external user, etc). Finally, due to the recent shift in technology used for Critical Infrastructures, there is not a rich statistic to be used to extract realistic values about the likelihood of occurrence of the attacks. However, it is worth noting that depending on socio-political events (e.g. during a period of terrorism attacks) this figure is supposed to quickly take higher values.

The annual loss (ALE) for a control station hacking attack is expected to be 50k€/ year and the annual infrastructure value (AIV) is calculated as the value of all the Policy Enforcement Points (PEP) that are needed to be deployed in the preliminary phase of the system architecture. Table 7 lists the PEPs for this scenario and provides information regarding their costs and threats that mitigate.

Table 7: Security Equipments for a Critical Infrastructure Process Control

PEP	**Description**	**AIV**	**Threats that mitigate**							
			T1	T2	T3	T4	T5	T6	T7	T8
PEP.1	Stronger Cryptography	2,000€					✓	✓	✓	✓
PEP.2	Wireless Sensor Network	1,000€	✓	✓			✓	✓	✓	
PEP.3	Back-up Power Supply	1,500€					✓			
PEP.4	IDS-IPS	2,500€	✓	✓	✓	✓	✓	✓	✓	✓
PEP.5	Firewall	2,000€	✓	✓	✓	✓	✓	✓	✓	✓
PEP.6	Antivirus/Antimalware	500€	✓	✓						✓
PEP.7	Access Control Mechanisms	1,500€	✓	✓	✓	✓	✓	✓	✓	✓
PEP.8	System Behaviour Monitoring	1,200€	✓	✓	✓	✓	✓	✓	✓	✓
PEP.9	Communication Protocols	500€	✓	✓		✓	✓		✓	

T1 Water Level Sensor Compromise
T2 Tilmeter Compromise
T3 Administration Password Theft
T4 Hazardous Water Release
T5 Hydroelectric Power Plant Hacking
T6 Visualization Station Misuse
T7 Control Station Hacking
T8 Other threats (e.g., malwares, virus)

From the list of equipments proposed in Table 7, we selected Wireless Sensor Network, IDS/IPS, Firewall, Access Control Mechanisms, System Behaviour Monitoring and Communication Protocols (e.g., DNP3, ICCP) as the security solutions to deploy for a Critical Infrastructure Process Control, since a combination of all of them provide a wider and more complete coverage of the different threats to which the system is exposed. The Annual Infrastructure Value is therefore estimated as 8,700€(the cost of all the selected solutions).

8.2.2. Attack 2 - Hydroelectric Power Plant Hacking

In case of a hydroelectric power plant islanding event (e.g., a blackout), the dam should immediately stop feeding the hydraulic turbines with water. However, an attacker may intercept and hide the request to the dam control station (using for instance a man-in-the-middle attack to counterfeit and/or delete the request messages). As a result, the dam gates remain open and continue to feed the hydroelectric turbines with water, causing their failure.

In particular, the attacker may alter some nodes in the WSN in order to return false measurements to the control station; i.e., the sensor measuring the dam gate openness is hijacked. Therefore, when an islanding event occurs, the control station sends a request to close the gates, but they already seem to be closed because of the hijacked sensor. The consequence is that nothing is done to stop the discharging water on the penstocks and the failure cannot be avoided.

A hydroelectric power plant hacking attack has an estimated *Serious* severity level (equivalent to 1,000,000€). The damage is not estimated to permanently destroy the system, but a large amount of service is estimated to be compromised. The likelihood for this attack can be estimated as *Negligible* (equivalent to 0.05 times per year). Italian laws provide the dams to be 24/7 under surveillance. Therefore, an attack from an internal network is very unlikely to occur. There is no established taxonomy to extract realistic values about the likelihood of occurrence of the attacks. This is because the use of computer technology to control dams has been recently introduced. It is worth noting that depending on socio-political events (e.g. during a period of terrorism attacks) this figure is supposed to quickly take higher values.

The annual loss (ALE) for a hydroelectric power plant hacking attack is expected to be 50k€/year and the annual infrastructure value (AIV) as estimated in the previous subsection is expected to be 8,700€/year.

8.3. Countermeasure Selection

This section evaluates different countermeasures for each of the attack scenario previously described, and aims at demonstrating how the RORI index helps in the selection of countermeasures. The list of proposed countermeasures was agreed with use case providers and contains the most common reactions to be considered in order to mitigate the detected attack.

8.3.1. Individual Countermeasure Selection

Each countermeasure candidate is analysed and evaluated individually based on the trade-off between their cost and benefit.

Attack 1 - Control Station Hacking. The following are the countermeasures that could best mitigate a control station hacking attack.

C1.1 NOOP: This candidate considers to accept the risk by doing no operation. This action does not require any modifications, therefore the cost and risk mitigation level are equal to zero.

C1.2 Privilege Separation: Enforce separation of privileges is useful by preventing users to perform actions they are not allowed.

C1.3 Active Alert Mode: This alternative proposes to fire an alert indicating that the control station is suspected to be under attack.

C1.4 Disable Remote Connections to the Control Station: Allow only local connections to the control station to authorized users (Switch from *remote* to *not-remote*).

C1.5 Enable Multiple Monitoring Indication: This countermeasure activates two or more monitoring systems to verify the water level indication obtained by the sensors.

C1.6 Restart Sensor Settings: It erases the current sensor values and request for new thresholds.

C1.7 Activate Back-up Sensors: Switch *off* current sensors and *on* back-up sensors.

Each countermeasure affects directly or indirectly a set of RCU elements, which generates a geometrical figure, as described in Section 7. Each countermeasure volume is interposed with the attack volume represenation in order to calculate, through geometrical operations, its corresponding coverage. An Example of this geometrical representation is shown in Figure 5.

As depicted in Figure 5, Countermeasure 1.2 covers only a portion of Attack 1. Such a coverage is calculated by selecting the RCU elements that belong to both attack 1 and countermeasure 1.2. As a result, 60% of attack 1 is controlled by countermeasure 1.2. This coverage is used to calculate the risk mitigation value (RM) of each security candidate, which in turn is used to calculate the RORI index. Table 8 summarizes this information.

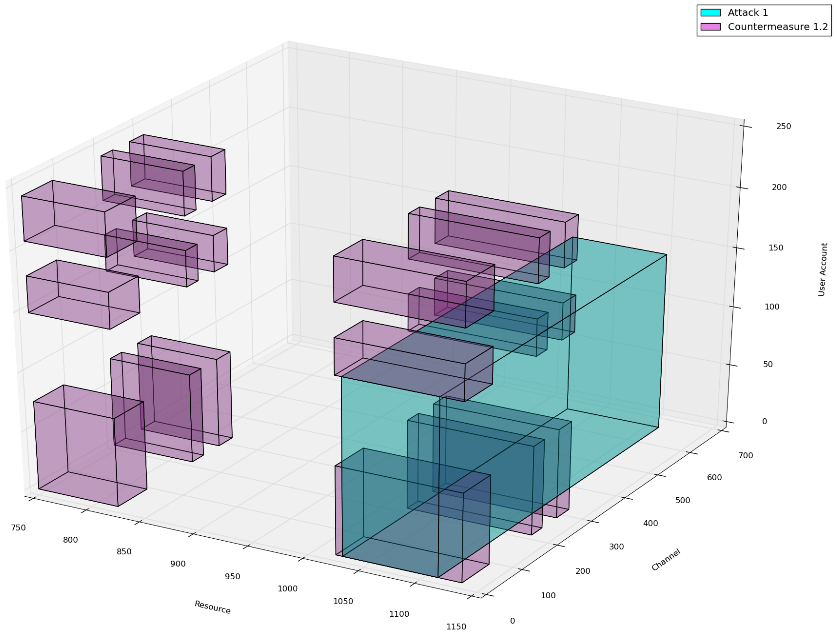


Figure 5: Volume Representation of Attack 1 and Countermeasure 1.2

From the set of proposed countermeasures, the highest RORI value corresponds to alternative C1.7 (Activate Back-up Sensors), with a cost of 400€, a risk mitigation of 63%, and a benefit of 341.76%. This candidate solution requires the manipulation of PEP.2 (i.e., Wireless Sensor Network) and it can be combined with any other countermeasure of the list except for C1.1. Countermeasure C1.7 becomes the selected single countermeasure for a control station hacking attack.

Attack 2 - Hydroelectric Power Plant Hacking. The following are the countermeasures that could best mitigate a hydroelectric power plant hacking attack.

C2.1 NOOP: This solution considers to accept the risk by performing no operation. The cost and risk mitigation level are equal to zero.

C2.2 Received Signal Strength: Depending on the position of the attacker, this alternative can be useful to indicate an abnormal behaviour on the system.

C2.3 Sensor Tamper Resistance: Activate tamper resistance on each sensor improves effectiveness to prevent hydroelectric power plant hacking attacks.

C2.4 Activate Protocol Analysis on the Firewall: Analyse the packets that go in/out the network and verify if the parameters are correct according to specific protocol norms, and stop them if they are classified as suspicious.

C2.5 Activate the Block-all Option: Block all unknown requests if the application is closed.

C2.6 Activate Back-up Sensors: Switch *off* current sensors and *on* back-up sensors.

Table 9 summarizes the information regarding each countermeasure. The parameters on the table are estimated according to the following assumption: an attacker replaces the sensor for gate openness with a fake one. The hijacked sensor can successfully authenticate itself and it always says that the dam gate is closed.

Table 8: Individual Countermeasure Evaluation for Attack 1

Countermeasures	**PEP**[1]	**ARC**[2]	**Cov**[3]	**EF**[4]	**RM**[5]	**RORI** [6]	**Restriction**
C1.1 NOOP	-	0€	0.00	0.00	0.00	0.00%	all
C1.2 Privilege Separation	PEP.7	200€	0.60	0.80	0.48	267.42%	C1.1
C1.3 Active Alert Mode	PEP.4	300€	0.45	0.60	0.27	146.67%	C1.1
C1.4 Disable Remote Connect.	PEP.5	500€	0.85	0.70	0.60	317.93%	C1.1
C1.5 Enable Mult. Monitoring	PEP.8	700€	0.75	0.85	0.64	331.65%	C1.1
C1.6 Restart Sensor Settings	PEP.2	200€	0.55	0.70	0.39	214.04%	C1.1
C1.7 Activate Back-up Sensors	PEP.2	400€	0.70	0.90	0.63	341.76%	C1.1

[1] Policy Enforcement Point [2] Annual Response Cost [3] Countermeasure Coverage
[4] Effectiveness Factor [5] Risk Mitigation Level [6] Return On Response Investment

Table 9: Individual Countermeasure Evaluation for Attack 2

Countermeasures	**PEP**[1]	**ARC**[2]	**Cov**[3]	**EF**[4]	**RM**[5]	**RORI** [6]	**Restriction**
C2.1 Do nothing	-	0€	0.00	0.00	0.00	0.00%	all
C2.2 Received Signal Strength	PEP.8	500€	0.40	0.75	0.30	157.61%	C2.1,C2.5
C2.3 Sensor Tamper Resistance	PEP.2	200€	0.75	0.70	0.53	292.70%	C2.1,C2.5
C2.4 Protocol Analysis	PEP.9	200€	0.75	0.85	0.64	355.90%	C2.1,C2.5
C2.5 Block Unknown	PEP.5	300€	0.80	0.80	0.64	352.22%	all
C2.6 Back-up Sensors	PEP.2	400€	0.70	0.90	0.63	341.76%	C2.1,C2.5

[1] Policy Enforcement Point [2] Annual Response Cost [3] Countermeasure Coverage
[4] Effectiveness Factor [5] Risk Mitigation Level [6] Return On Response Investment

From the set of proposed countermeasures, the highest RORI value corresponds to alternative C2.4 (Protocol Analysis), with a cost of 200€, a risk mitigation of 64%, and a RORI of 355.90%. This candidate solution requires the manipulation of PEP.9 (i.e., Communication protocols), and it can be combined with all other countermeasures except for C2.1 and C2.5. Countermeasure C2.4 becomes the selected single countermeasure for a hydroelectric power plant hacking attack.

8.3.2. Combined Countermeasure Evaluation

A combined countermeasure results from the simultaneous implementation of two or more countermeasures to mitigate a given attack. A combined solution is therefore analysed as a single countermeasure with a combined cost and a combined risk mitigation.

Attack 1 - Control Station Hacking. We know that all countermeasures can be combined except for C1.1 (NOOP), because this is a totally restrictive solution. We select therefore, C1.2, C1.3, C1.4, C1.5, C1.6, and C1.7 as the candidates to combine.

The coverage of multiple countermeasures is calculated by interposing the graphical representation of several countermeasures against that one of the attack scenario. As a result, we are able to determine the union and intersection of different volumes, as proposed in Section 7.4.1. An example of this geometrical representation is depicted in Figure 6.

Using Equation 7, we compute the volume coverage of each group of countermeasures with respect to the volume of attack A1. By interposing the geometrical figures of the detected attack against the volume of the countermeasures, we are able to determine the RCU elements that belong to both, attack and countermeasures. Such intersection is needed to compute the risk mitigation (RM) of all combined candidates.

Figure 6 shows that a portion of C1.4 and C1.7 covers attack A1. In this example, the intersection coverage results into 63%, which in turn results into a risk mitigation of 79% and a RORI index of

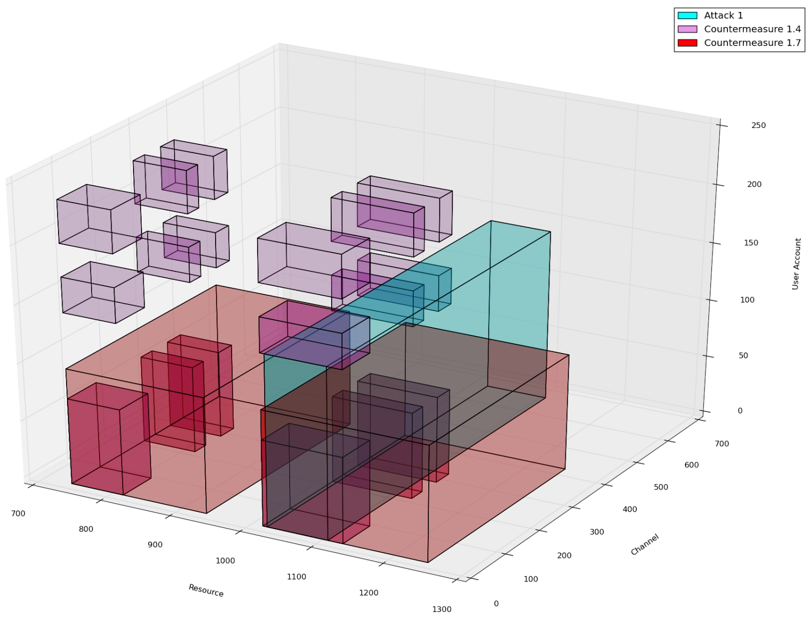


Figure 6: Volume Representation of Attack 1 and Countermeasures 1.2 and 1.4

400.78%. Table 10 summarizes the top ten results on the evaluation of all combined countermeasures for a Control Station Hacking Attack.

Table 10: Combined Countermeasure Evaluation for Attack 1

CM	Combination	C_ARC[1]	C_Cov[2]	C_EF[3]	C_RM[4]	RORI
1	C1.2+C1.3+C1.6+C1.7	1100€	0.23	0.60	0.88	436.48%
2	C1.2+C1.3+C1.7	900€	0.23	0.60	0.82	420.31%
3	C1.3+C1.6+C1.7	900€	0.23	0.60	0.82	420.31%
4	C1.2+C1.6+C1.7	800€	0.28	0.70	0.80	413.95%
5	C1.4+C1.7	900€	0.63	0.70	0.79	400.78%
6	C1.2+C1.3+C1.5+C1.6	1400€	0.23	0.60	0.83	398.27%
7	C1.2+C1.4+C1.7	1100€	0.38	0.70	0.80	398.21%
8	C1.2+C1.7	600€	0.45	0.80	0.75	396.77%
9	C1.3+C1.5+C1.6	1200€	0.23	0.60	0.80	391.92%
10	C1.2+C1.3+C1.5	1200€	0.23	0.60	0.798	390.66%

[1] Combined Annual Response Cost [2] Combined Intersection Coverage
[3] Combined Effectiveness Factor [4] Combined Risk Mitigation

From Table 10, we select C1.2, C1.3, C1.6, and C1.7, as the best combination of countermeasures, which proposes to enforce separation of privileges, activate alert mode, restart sensor settings, and activate back-up sensors. By doing this, the system is able to secure the control and visualization station network and ensure the authentication of messages. Furthermore, the risk is expected to be reduced 88%, resulting in a RORI index of 436.48%. This group of candidates becomes the selected combined countermeasure for a Control Station Hacking Attack in the scenario of critical infrastructure process control.

Attack 2 - Hydroelectric Power Plant Hacking. We select C2.2, C2.3, C2.4, and C2.6 as the candidates to combine (they are not totally restrictive). Table 11 summarizes the results obtained on the evaluation of all combined countermeasures for a Hydroelectric Power Plant Hacking Attack.

Table 11: Combined Countermeasure Evaluation for Attack 2

CM	**Combination**	**C_ARC**[1]	**C_Cov**[2]	**C_EF**[3]	**C_RM**[4]	**RORI**
1	C2.2+C2.4+C2.6	1,100€	0.20	0.75	0.83	414.80%
2	C2.4+C2.6	600€	0.57	0.85	0.78	412.23%
3	C2.2+C2.3+C2.6	1,100€	0.20	0.70	0.81	403.32%
4	C2.3+C2.4+C2.6	800€	0.45	0.70	0.78	401.45%
5	C2.3+C2.6	600€	0.57	0.70	0.75	398.12%
6	C2.3+C2.4	400€	0.63	0.70	0.72	393.96%
7	C2.2+C2.3+C2.4	900€	0.20	0.70	0.77	389.71%
8	C2.2+C2.4	700€	0.28	0.75	0.73	381.52%
9	C2.2+C2.3+C2.4+C2.6	1,300€	0.20	0.70	0.78	378.25%
10	C2.2+C2.6	900€	0.25	0.75	0.74	377.34%
11	C2.2+C2.3	700€	0.28	0.70	0.63	328.99%

[1] Combined Annual Response Cost
[2] Combined Coverage
[3] Combined Effectiveness Factor
[4] Combined Risk Mitigation

From Table 11, we determine that the best solution to implement is the combination of C2.2, C2.4, and C2.6, which proposes to analyze received signal strengh, activate protocol analysis and activate back-up sensors. As a result, the risk is expected to be reduced 83%, and the RORI index is expected to be 414.80%. This group of candidates becomes the selected combined countermeasure for a Hydroelectric Power Plant Hacking Attack in the critical infrastructure process control scenario.

9. Conclusion

We introduced the attack volume as an improvement of the attack surface model [19, 10]. Based on the several limitations derived by the implementation of the attack surface model, we propose an approach to model the information retrieved by a URI into a three-dimensional coordinate system (i.e., user, channel, and resource).

We propose to measure the volume of multiple elements by using geometrical operations to calculate their union and intersection. The approach considers joint and/or disjoint volumes, and proposes equations for their corresponding evaluation. The proposed model provides a clear representation of attacks and countermeasures in a given system, and the possibility to identify priority areas (e.g., those with the highest attack volume, or where multiple attacks intersect). Consequently, it is possible to detect the users, channels, and resources that are the most vulnerable in the system, in order to define the reaction strategies to apply.

In addition, we propose an accurate and quantitative methodology to evaluate countermeasures for complex attack scenarios. Countermeasure volumes are analysed and compared, making it possible to determine the coverage of each countermeasure over each of the studied attacks.

Future work will concentrate in integrating other axes (e.g., time, contexts) into the coordinate system. Considering that the number of axis could change in the proposed model, the system should be flexible enough to model the information retrieved by a URI into more than three dimensions, resulting in a variety of geometrical figures (e.g., hyperrectangle, hypercube) that are not initially considered in the calculation of the attack volume.

Acknowledgements: The research in this paper has received funding from the Information Technology for European Advancements (ITEA2) within the context of the ADAX Project (Attack Detection and Countermeasure Simulation), and the PANOPTESEC project, as part of the Seventh Framework Programme (FP7) of the European Commission (GA 610416). We graciously acknowledge support received from the Spanish Ministry of Science and Innovation (project TIN2011-27076-C03-02 CO-PRIVACY). Authors would also like to thank the MAnagement of Security information and events in Service InFrastructures (MASSIF) projet and the use case providers for their contribution of a real case study.

References

[1] Vetillard, E., Ferrari, A.: Combined Attacks and Countermeasures, International Federation for Information Processing, Smart Card Research and Advanced Application, pp. 133–147, (2010)

[2] Jeffrey, M.: Return on Investment Analysis for e-Business Projects, Internet Encyclopedia, First Edition, Hossein Bidgoli Editor, vol. 3, pp. 211–236, (2004)

[3] Schmidt, M.: Return on Investment (ROI): Meaning and Use, Encyclopedia of Business Terms and Methods, (2011)

[4] Cremonini, M., Martini, P.: Evaluating Information Security Investment from Attackers Perspective: the Return-On-Attack (ROA), 4th Workshop on the Economics on Information Security, (2005)

[5] Sonnenreich, W., Albanese, J., Stout, B.: Return On Security Investment (ROSI) – A Practical Quantitative Model, Journal of Research and Practice in Information Technology, vol. 38, number 1, pp. 45-46, (2006)

[6] Brocke, J., Strauch, G., Buddendick, C.: Return on Security Investment — Design Principles of Measurement System Based on Capital Budgeting', Conference of Information Systems Technology and its Applications, pp. 21–32, (2007)

[7] Mizzi, A.: Return on Information Security Investment: the Viability of an Anti-Spam Solution in a Wireless Environment, In International Journal of Network Security, vol. 10, number 1, pp. 18–24, (2010)

[8] Kheir, N., Cuppens-Boulahia, N., Cuppens, F., Débar, H.: A Service Dependency Model for Cost-Sensitive Intrusion Response, Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS), pp. 626–642, (2010)

[9] Gonzalez-Granadillo, G., Belhaouane, M., Debar, H., Jacob, G.: RORI-based countermeasure selection using the OrBAC formalism, International Journal of Information Security, vol. 13, number 1, pp. 63–79, (2014)

[10] Manadhata, P., Wing, J.: An Attack Surface Metric, IEEE Transactions on Software Engineering, vol. 37, number 3, pp. 371–386, (2011)

[11] Berners-Lee, T., Fielding, R., Masinter, L.: Uniform Resource Identifier (URI): Generic Syntax, RFC3986 (2005)

[12] Norman, T.: Risk Analysis and Security Countermeasure Selection, CRC Press, Taylor & Francis Group (2010)

[13] Federation 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)

[14] Lockstep Consulting: A Guide for Government Agencies Calculating Return on Security Investment, Available at: http://lockstep.com.au/library/return_on_investment (2004)

[15] Kosutic, D.: Is it possible to calculate the Return on Security Investment (ROSI)?, Available at: http://blog.iso27001standard.com/2011/06/13/is-it-possible-to-calculate-the-return-on-security-investment-rosi/ (2011)

[16] Mizzi, A.: Return on Information Security Investment: the Viability of an Anti-Spam Solution in a Wireless Environment, In International Journal of Network Security, vol. 10, number 1, pp. 18–24, (2010)

[17] Locher, C.: Methodologies for Evaluating Information Security Investments - What Basel II Can Change in the Financial Industry, 2005 European Conference on Information Systems, paper 122, Available at: http://aisel.aisnet.org/ecis2005/122 (2005)

[18] Northcutt, S.: The Attack Surface Problem, SANS technology Institute Document, Available at: http://www.sans.edu/research/security-laboratory/article/did-attack-surface, (2011)

[19] Howard, M., Wing, J.: Measuring Relative Attack Surfaces, In Computer Security in the 21st Century, pp. 109–137, (2005)

[20] Petajasoja, S., Kortti, H., Takanen, A., Tirila, J.: IMS Threat and Attack Surface Analysis using Common Vulnerability Scoring System, 35th IEEE Annual Computer Software and Applications Conference Workshops, pp. 68–73, (2011)

[21] Krill, P.: Microsoft Releases Attack Surface Analizer for secure development, Available at: http://www.techworld.com/news/security/microsoft-releases-attack-surface-analyzer-for-secure-development-3257260/ (2011)

[22] Hu, V., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K.: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162 (2014)

[23] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., Youman, C. E.: Role-based access control models, IEEE Computer, Vol. 29, pp. 38–47, (1996)

[24] Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G.: Organization based access control, 8th International Workshop on Policies for Distributed Systems and Networks, (2003)

[25] Information Sciences Institute University of Southern California: DOD Standard Internet Protocol, Available at: http://tools.ietf.org/html/rfc760 (1980)

[26] Touch, J.: Updated Specification of the IPv4 ID Field, Available at: http://tools.ietf.org/html/rfc6864 (2013)

[27] Deering, S., Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, Available at: http://tools.ietf.org/html/rfc1883 (1995)

[28] Cotton, M., Vegoda, L., Bonica, R., Haberman, B.: Special-Purpose IP Address Registries, Available at: http://tools.ietf.org/html/rfc6890 (2013)

[29] Cotton, M., Eggert, L., Touch, J., Westerlund, M., Cheshire, S.: Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry, Available at: http://tools.ietf.org/html/rfc6335 (2011)

[30] Touch, J. Kojo, M., Lear, E., Mankin, A., Ono, K., Stiemerling M., Eggert, L.: Service Name and Transport Protocol Port Number Registry, Available at: `http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml` (2013)

Short Bios

Gustavo Gonzalez Granadillo is a postdoctoral fellow at Telecom SudParis. He holds an engineering degree from Yacambu University, Venezuela; an MS in Computer and Communication Networks from Telecom SudParis, France; and a Ph.D. in Informatics from Paris 6 University. His research interests include security information and event management, critical infrastructures, risk analysis and attack impact models.

Joaquin Garcia-Alfaro is Professor at Telecom SudParis. He holds a double PhD degree in Computer Science and Network Security, and a full research and professorship habilitation. His interests are on areas related to the management of security policies, analysis of threats, enforcement of mitigation and evaluation of countermeasures.

Ender Alvarez is a research engineer at Telecom SudParis. He holds a Bachelor degree in Informatics from Universidad Nacional Experimental del Tachira, Venezuela, and a MS in Computer and Communication Networks from Telecom SudParis, France. He is currently focused on the development of applications to improve ICT security areas, with interest in TCP/IP Networks and GNU/Linux System administration.

Mohammed El Barbori is a research engineer at Telecom SudParis. He did a Master of Science in algorithms and optimization, and a Specialization in security information and cryptography from Limoges University. His research interests include the detection and analysis of complex cyber attacks, software development, and the integration of security solutions in critical platforms.

Hervé Debar is Professor at Telecom SudParis, and the Head of the Networks and Telecommunication Services Department. His activity is related to the information and communication technology (ICT) security area. He has been involved in intrusion detection research, and he is currently focusing on security information and event management (SIEM), with an emphasis on automated threat mitigation.