Towards an automated and dynamic risk management response system

Gustavo Daniel Gonzalez Granadillo, Ender Yesid Alvarez Lopez, Alexander Motzek, Matteo Merialdo, Joaquin Garcia-Alfaro, Hervé Debar

Towards an Automated and Dynamic Risk Management Response System

Gustavo Gonzalez-Granadillo[1], Ender Alvarez[1], Alexander Motzek[2], Matteo Merialdo[3], Joaquin Garcia-Alfaro[1], and Hervé Debar[1]

[1] Institut Mines-Télécom, Télécom SudParis, CNRS UMR 5157 SAMOVAR
9 Rue Charles Fourier, 91011 Evry, France
{name.last_name}@telecom-sudparis.eu
[2] Universität zu Lübeck, Institute of Information Systems,
Ratzeburger Allee 160, 23562 Lübeck, Germany
motzek@ifis.uni-luebeck.de
[3] RHEA Group, Avenue Pasteur 23, 1300 Wavre, Belgium
m.merialdo@rheagroup.com

Abstract. Achieving a fully automated and dynamic system in critical infrastructure scenarios is an open issue in ongoing research. Generally, decisions in SCADA systems require a manual intervention, that in most of the cases is performed by highly experienced operators. In this paper we propose a framework consisting of a proactive management software that aims at anticipating the occurrence of potential attacks. It conducts an initial evaluation of reported proactive evidences based on a quantitative metric of monetary return on response investment. The framework evaluates and selects mitigation actions from a pool of candidates, by ranking them in terms of financial and operational impacts. The purpose of this process is to select an optimal set of mitigation actions from financial and operational perspectives and propose them to reduce the risk of threats against the monitored system, without sacrificing an organization's missions in favor of security. A real world case study of a SCADA environment shows the applicability of the model, from the analysis of the input data to the selection of the response plan.
Keywords: Dynamic Response System, RORI, Operational Impact, Automatic Response, Critical Infrastructures

1 Introduction

Critical infrastructures are systems and assets, whether physical or virtual (e.g., a company, an institution, an organization), which if disrupted, damaged, or destroyed, would have a serious impact on the health, safety, security, or economic well-being of citizens or the effective functioning of governments and other infrastructures depending on it [1]. Critical Infrastructures include sectors that account for substantial portions of national income and employment, such as energy (including nuclear), ICT, finance, healthcare, food, water, transport, safety, government. Most of these sectors use industrial control systems (ICS) in order to provide control of remote equipment [2].

Achieving a fully automated system in critical infrastructure scenarios is an ongoing research area. Generally, decisions in SCADA systems require a manual intervention, that in most cases is performed by highly experienced operators. However, it is possible to automate incident handling. For some threats, a system should be able to automatically select mitigation actions that provide the most suitable response possibilities to reduce identified risks below an admissible level while minimizing potential negative side effects of deliberately taken actions.

In this paper, we propose a dynamic risk management response system (DRMRS) that evaluates, ranks and selects optimal mitigation actions based on financial, operational and threat impact assessment functions. The selected actions are transformed into response plans that are automatically enforced by the system's policy enforcement points (PEPs). These latter are defined as security components that work as gateways or front doors to digital resources. PEPs are capable of applying security rules (e.g., permission, prohibition, obligation) over the triplet {subject, action, object}. Examples of PEP are web servers, portals, firewalls, LDAP directories, SOAP engines, and similar resources [3].

The contributions on this article are summarized as follows: **(1)** A model that automatically computes the input parameters of the financial impact metric and provides an indication of the feasibility of each evaluated action. **(2)** A process that dynamically generate and validate response plans. **(3)** The implementation and validation of the model. **(4)** The deployment of the model over a real scenario to perform automated responses in a critical infrastructure system.

The remainder of the paper is structured as follows: Sec. 2 introduces the return on response investment metric. Sec. 3 describes our proposed dynamic risk management response system. Sec. 4 details the tool implementation and validation. Sec. 5 depicts a case study to automate the response in a critical infrastructure system. Related work are presented in Sec. 6. Finally, conclusions and perspective for future work are presented in Sec. 7.

2 Dynamic Return On Response Investment (*RORI*)

The Return On Response Investment (RORI) is a cost sensitive metric used to assess, rank and select security countermeasures from a pool of candidates. The process undertaken by the DRMRS extends initial work reported in [4]. The approach proposes the combination of authorization models and quantitative metrics, for the selection of mitigation actions. The actions, modeled in terms of contextual rules, are prioritized based on a cost-sensitive metric that extends the return on investment (ROI) concept and all its variants [5–7]. The goal is finding an appropriate balance between the financial damages associated to a given threat, and the benefits of applying some mitigation actions to handle the threat, with respect to the loss reduction. The RORI metric is calculated for each mitigation action, according to Eq. 1.

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

In theory, all parameters composing the RORI metric should be given by expert knowledge, historical data, and/or a risk assessment methodology that evaluates all possible system's threats and gives directions about the most suitable mitigation actions to reduce risk levels down to acceptable values. In practice, however, the estimation of such parameters represents a big challenge and a time consuming task to security administrators. Depending upon the type of organizations, the RORI parameters can be more or less complex to estimate. For small and medium size organizations, the quantification of such parameters, is a process that could be performed within hours of discussions with use case providers and simple simulation runs [4]. For large and critical organizations, the process can take several weeks (and even months).

Based on the previous shortcomings, a first improvement has been made in the RORI expression to enhance the Risk Mitigation (RM) function. [8] extends the concept of attack surface used in previous versions of the RORI metric. It identifies authorization and contextual dimensions that may directly contribute to the exposition of system vulnerabilities. New properties associated to the vulnerabilities, 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) can now be included and combined with the RORI cost-sensitive metric.

An adaptation of the selection process, based on financial and operational assessment functions, has been presented in [9], which reports the combination of both assessment approaches, over a representative set of mitigation actions. The combination, based on a multi-dimensional minimization approach, proposes the choice of semi-optimal responses that, on the one hand, bear the highest financial attractiveness on return on investment; and, on the other hand, bear the lowest probability of conflicting with the organization's missions. This is seen as beneficial for its application in scenarios where highly critical missions and resources must be protected, without sacrificing missions in favor of security.

The remaining of this section details the parameters of the RORI metric and describes the process to automatically compute them in a dynamic system.

2.1 Description of the Dynamic *RORI* Model

Annual Loss Expectancy, ALE expresses the amount of money, e.g., €/year, that an organization may lose if a threat is realized on the system. It includes loss of assets, loss of data, loss of reputation, etc. ALE depends directly on the threat and it is independent on the mitigation actions and the policy enforcement points.

Annual Infrastructure Value, AIV depends directly on the policy enforcement point, and expresses the monetary value of the infrastructure, e.g., €/year, regardless of the threat and the implemented mitigation actions. AIV is greater than zero, i.e., $AIV > 0$, and includes costs of equipment, personal, service, etc.

Annual Response Cost, *ARC* provides the information about the amount of money (e.g., €) associated to the implementation of a mitigation action against a threat. *ARC* is always greater than or equal to zero, i.e., $ARC \geq 0$, and includes direct costs, such as cost of implementation, cost of maintenance, other direct and indirect cost, such as potential collateral damages. *ARC* depends on the mitigation action and the policy enforcement point, but it is independent on the threat.

Risk Mitigation, *RM* represents the level of reduction that is obtained after the implementation of a mitigation action. *RM* takes values between zero and one hundred, i.e., $0 \leq RM \leq 100$. *RM* depends on the threat, the mitigation action, and the policy enforcement point.

Each parameter depends on at least one of the following entities: (i) the threat affecting the system, (ii) the type of mitigation action to be implemented, and (iii) the type of policy enforcement point. Table 1 summarizes this information and details the level of complexity on the estimation of each parameter.

Table 1. Complexity level on the estimation of the RORI parameters

Parameter	Threat	MA_Type	PEP_Type	Complexity
AIV			✓	Low
ALE	✓			Low
ARC		✓	✓	Medium
RM	✓	✓	✓	High

2.2 Computation of the Dynamic *RORI* Parameters

In a dynamic environment, nodes can be active or inactive. Each snapshot of the system may provide a list of different nodes involved in the attack scenario. The evaluation process is therefore unique for each system's snapshot, and is discussed in the following definitions.

Definition 1 (ALE Computation). *Since the ALE parameter is associated to the threat, its value remains unchanged for each snapshot of the system. ALE is assessed first qualitatively, and then transformed into quantitative values. We follow the approach proposed in [10] that defines six qualitative levels of severity, and seven qualitative levels of likelihood with their corresponding quantitative values. ALE is calculated as the product of the severity transformed into probabilistic costs and the likelihood transformed into probabilistic frequency.*

Definition 2 (AIV Computation). *The AIV is computed as the sum of the Annual Equipment Cost (AEC) of all policy enforcement points that appears in the system's snapshot, as shown in Eq. 2.*

$$AIV = \sum_{i=0}^{n} AEC_i \tag{2}$$

Each PEP has an associated AEC that is estimated based on historical information and expert knowledge. Contrary to the ALE, the value of the AIV changes at each snapshot of the system. More details on its estimation can be found in [4].

Definition 3 (ARC Computation). *The ARC is associated to the implementation of a given mitigation action. The value depends directly on the type of mitigation action (e.g., reboot, shutdown, patching), and the PEP responsible of its implementation. More details on its estimation can be found in [4].*

Definition 4 (RM Computation). *The RM of an action is computed as the product of the effectiveness EF and the threat coverage COV, using Eq. 3.*

$$RM = EF \cdot COV \tag{3}$$

Effectiveness (EF) of a mitigation action represents the level at which a given action reduces the risk and/or consequences of an attack on the system. EF is intrinsic to the mitigation action type regardless of the threat it mitigates. For instance, a reboot action by itself provides a very low mitigation of a given threat, whereas a patching action provides a very high protection against it. Table 2 summarizes default values associated to mitigation action types. Each value has been assigned based on statistical data and expert knowledge. Coverage (COV) of a given mitigation action represents the number of nodes to which a mitigation action is being executed over the total number of vulnerable nodes, i.e.,

$$COV = \frac{Q_i \cdot WF_i}{\sum_{j=0}^{n} QT_j \cdot WF_j} \ , \tag{4}$$

where Q_i is the number of nodes from a PEP_type that are affected by a given mitigation action, WF_i is the weighting factor associated to the affected PEP_type, QT_j is the total number of active node types in the system, and WF_j is the weighting factor associated to each node type.

Table 2. Default effectiveness values associated to mitigation action types.

Mitigation Action Type	**Protection**	**EF**
Reboot	Very Low	1.00 %
Shutdown	Low	10.00%
Backup	Medium	50.00%
Change Configuration	High	80.00%
Patching	Very High	100.00%
Install Software/Hardware	Very High	100.00%

3 Dynamic Risk Management Response System

The Dynamic Risk Management Response System (DRMRS) handles identified threats, authorized mitigation actions and strategic policies (i.e., default and

contextual policy rules, as well as contextual definitions). It extracts concrete entities from reported threats, and infers concrete policy instances to eventually guide the system into new updates and reconfigurations. These are provided as concrete response plans on a long-term proactive perspective. Response plans are validated by human operators, prior final enforcement. The goal of the DRMRS is the automated administration of policy-related activities, including addition of new rules, removal of unnecessary conditions, and activation of strategic responses (i.e., activation of new mitigation and response plans).

The DRMRS is a dynamic process that involves information coming from different sources of an environment, which are notated and defined as follows.

Abstract Security Policies contain the security policies of the target organization. They include details of the threat (e.g., threatID, attack vector, severity, frequency); details of the Policy Enforcement Point (e.g., name, annual equipment value, PEPType, quantity); and details of the mitigation actions (e.g., ID, ARC, coverage, nodeID, restrictions, effectiveness).

Proactive Risk Profile includes information about assets, supporting assets, attack scenarios and detrimental events. These latter are defined as the fact of harming the accomplishment of an organization's objective or mission.

Network Inventory contains information of all active devices of the emulation environment providing various attributes, e.g., the PEP_Type.

Mission Dependency Model contains information about business processes and devices, consequences and requirements. It contains information about entry points, critical resources, and their dependencies and impact to the mission of the organization.

Network Dependency Model contains information about direct dependencies between individual resources of an organization or mission. The model is used to identify indirect dependencies and cover transitive impacts to the mission of the organization from widespread events.

Attack Graph contains information about all possible attack scenarios. The information includes details of the target and source nodes, as well as the attack paths and its associated likelihood.

Authorized Mitigation Actions contain a list of mitigation actions that are authorized to be executed as a reaction to a given threat.

Based on these input data, response plans are generated and evaluated as elaborated in the following sections.

3.1 Response Plan Generation Process

The process, as depicted in Fig. 1, starts by obtaining information of the threat scenarios coming from the Abstract Security Policies (ASP) and the information of Detrimental Events (DE) coming from the Proactive Risk Profile (PRP). We compare predefined conditions in both input files. We compare, e.g., if the likelihood of the threat scenario is greater than or equal to the likelihood of the detrimental event (Step 1). In such a case, we collect all attack path IDs that

will be used in the attack graph parsing process (Step 2a). If the condition is not met, the process generates an empty response plan (Step 2b).

Given the most updated information of the network inventory and the attack vector from the ASP, we generate a concrete attack vector (Step 3). A determination is made on whether there is a partial concrete attack vector (i.e., for each path of the attack vector, we search all active nodes from the network inventory). If at least one concrete attack vector is found, the process searches for a match of entry points and business devices from the obtained attack vector and the mission dependency model (Step 4a). Otherwise, an empty response plan is generated (Step 4b).

Following, we search paths matching the attack graph file and the attack vector (Step 5). A determination is made on whether there is a final concrete attack vector (i.e., for each path of the attack vector, there is a node that matches with the attack graph). If at least one matching node is found, the process collects the set of nodes from the attack vector involved in the attack graph (Step 6a), otherwise, an empty response plan is generated (Step 6b).

Given the list of authorized mitigation actions, a determination is made on whether or not there are involved nodes in the process. If it is the case, the process extracts all mitigation actions associated to the PEP type of the nodes obtained from the Attack Graph (Step 7a), otherwise, an empty response plan is generated (Step 7b). The RORI evaluation is performed on the extracted mitigation actions and response plans are generated accordingly (Step 8).

The output of this module is a set of response plans, which are vectors of mitigation actions, representing individual actions to be performed as a response to an adversary or threat opposed to an organization. A response plan contains an ID, mitigation action IDs and types, a policy enforcement point and the RORI index. Response plans are of two types: individual, when only one mitigation action is proposed; and combined, when two or more mitigation actions are proposed to be implemented. In such a case, a new parameter called "probability of conflict" is included in order to manage restrictions among the proposed actions.

3.2 Response Selection and Visualization

This module obtains the generated response plans and performs an operational evaluation in order to select the best response plan in financial and operational terms. We consider that response plans, while highly effective, could lead to operational negative side-effects inside the network and therefore onto a mission. Response plans are therefore evaluated based on local impact and assessments of dependencies inside an organization's business. We perform such an operational impact assessment based on a locally validatable probabilistic approach as proposed by Motzek et al. in [11]. The operational impact assessment is based on a probabilistic graphical model obtained from a mission- and network dependency model through probabilistic inference and is detailedly discussed in [11] and [9]. As a result, response plans are enriched with operational information that indicates the impact over the organizational mission(s) in three dimensions: a short-term impact (OI_0), mid-term (OI_1) and long-term impact (OI_2). Based

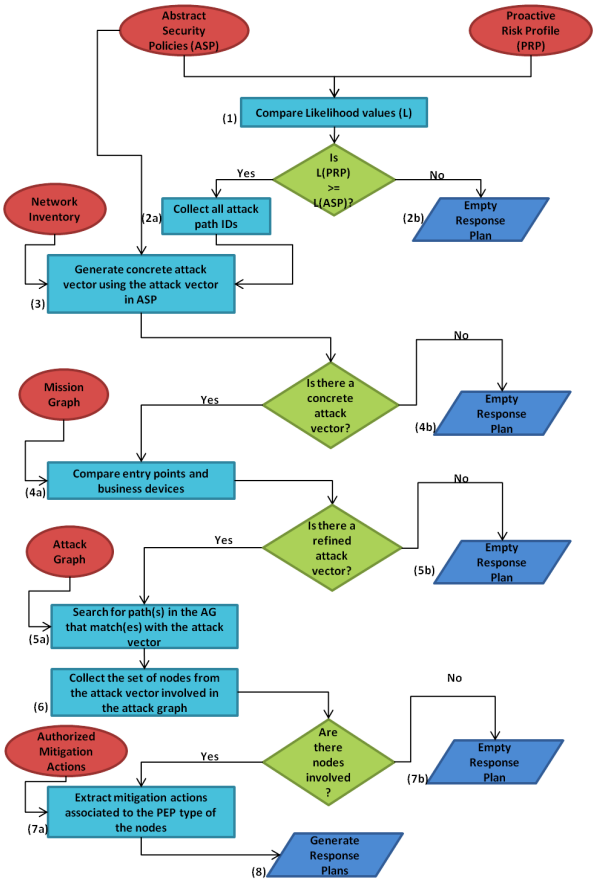

Fig. 1. Workflow for generating potential response plans.

on [9], the number of response plans is reduced to a single response plan that is optimal in each dimension: the financial and the operational impact. Their method searches for a semi-optimal response plan with the lowest operational impact assessment and the highest RORI index.

A response plan is said to be semi-optimal since it might not be the best solution neither in financial nor in operational terms, but it proposes a set of mitigation actions that on the one hand, bear the highest financial attractiveness on return on investment, and, on the other hand, bear the lowest probability of conflicting with a company's mission. This is beneficial for applications, where highly critical missions and resources must be protected, without sacrificing missions in favor of security.

The approach searches for a boundary of acceptable elements (acceptable as a compromise). This boundary is a numerical value representing a normalized deviation (ε) of the optimum. For instance, with ε=0.1, we accept 10% deviation of the optimum in each dimension based on the dimensions absolute scale. The acceptance criteria for the financial and operational impact are different. For the

financial impact, we keep response plans whose RORI index are greater or equal to 90% of the highest (best) RORI value. For the operational impact, we keep response plans whose OI_i are up to 10% of the lowest (best) OI_i value. Then, we check if there is a match in all evaluated response plans. If there is a match, we stop the process; otherwise, we increase the ε value until we find a tuple that matches. In particular, we search the ε where we obtain the smallest set of values. Once a semi-optimal response plan is found, the information is sent to the visualization module, which depicts such results to the security operator.

4 System Testing and Experimentation

Testing and experimentation consists of demonstrating accomplishment of different functional and non-functional requirements defined for the DRMRS. More specifically, we focus on defining a set of tests that are conducted to verify that each requirement is covered by the component implementation. In summary, functional requirements are used to test the syntactical and semantical correct behavior to input data, i.e., correct computation of ALE, ARV, AIV and RM values. All tests have been conducted by manual code inspection, as well as automatically performed tests on artificial data testing syntactical errors, as well as, real data (see Sec. 5) testing correct semantic behavior. In summary all tests were executed without errors or exceptions.

Additionally, several test cases are executed in order to evaluate the computation time in the combined evaluation of mitigation actions. The number of combination for a set of non-restrictive candidates is given by the expression $X = (2^N)(N + 1)$. Since the total number of combinations grows exponentially, we measure the time at which the system is able to perform the evaluation of multiple candidates. An existing non-functional requirement demands the evaluation of multiple response plans in the range of minutes. Results plotted in Fig. 2 show that a combination of 12 restrictive mitigation actions results into 796 combinations that are obtained in less than one second. For 12 non-restrictive mitigation actions, a total of 4 082 combinations exists, which are performed in less than 10 seconds. Given 24 restrictive mitigation actions, 590 464 combinations are evaluated in almost three hours. Therefore, to keep the evaluation process within a reasonable time (less than one minute), the system processes up to 14 non-restrictive mitigation actions (16 369 combinations). Beyond this threshold more than one minute is required, but the approach scales linearly with the number of processed combinations as evident from Fig. 2.

In addition, several integration tests have been performed to verify and validate the appropriate communication of all the components of the DRMRS framework. Such tests rely on the generation of response plans. The communication between the financial and the operational impact assessor modules is an example of integration among the system's components. The set of response plans generated by the financial impact module is sent for evaluation to the operational impact module, making it possible to generate a single response plan that best satisfies the financial and operational impact assessments.

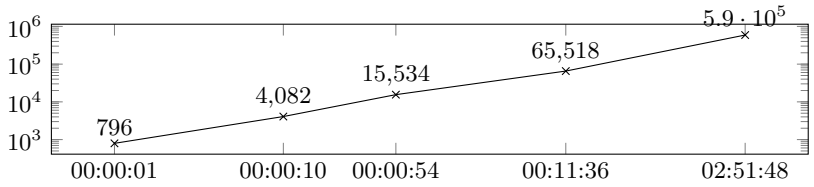

Fig. 2. Computation time (abscissa) to evaluate all combinations of mitigation actions is linear in the number of combinations (ordinate) *(double logarithmic plot)*.

5 Case Study: Automated Response in a Critical Infrastructure System

We study the infrastructure environment of an Energy Distribution organization. The environment consists of a distributed network of Remote Terminal Units (RTU) in energy stations of medium voltage (MV) and high voltage (HV), that acquire data from electrical devices (e.g., PLC, sensors, etc), and send them to the Supervisor Terminal Unit (STU) of the headquarters. The system uses Supervisory Control and Data Acquisition (SCADA) protocols.

5.1 Threat Scenario

The threat to analyze is a denial of service against a high voltage node of the C&C infrastructure with the objective of taking the C&C offline. More precisely, the threat will cause an out of service condition on Front End Servers (e.g., FE-X1) which breaks communication path from SCADA Servers to RTUs. There exists an attack vector via ICT Network (via VR-08) targeting first the file server (i.e., File-SRV), second, the archive server (i.e., Archive-SRV), and third, the high voltage Front End devices (i.e., FE-X1, FE-X2).This threat has a severity defined as "grave," which corresponds to a single loss expectancy SLE = 10 000 000 €, and a likelihood defined as "medium," equivalent to an annual rate of occurrence $ARO = 2$. The Annual Loss Expectancy is therefore equivalent to ALE = 20 000 000 €/year.

5.2 Input Information

After receiving input information, the system checks for active PEPs in the simulation environment in order to obtain the AIV. For this threat scenario, the current snapshot shows that there are 17 active PEPs with an AIV equivalent to 6 925 555€, as shown in Table 3. Note that AIV corresponds to the value obtained out of the sum of all PEP's cost, i.e., AEC, that are active at the time of the snapshot. The AIV parameter is a variable value that depends on the time of the evaluation and the PEP that are detected by the system.

Following, the system compares the likelihood values of detrimental events in the proactive risk profile against the threat scenario threshold values. For this threat scenario, three detrimental events have greater likelihood values

Table 3. Input Values of the AIV parameter

PEP	PEP_Type	Description	AEC
PEP16	FWCEDET	Logical Firewall and IPS working in CEDET	105 000
PEP2	SRVMSCADA	Medium Voltage Server	355 000
PEP1	SRVXSCADA	High Voltage Server	355 000
PEP3	FEXSCADA	High Voltage Front End	1 320 000
PEP13	FTPSRV	FTP Server	3 000
PEP11	HMISCADA	Human-Machine Interface	80 000
PEP15	NTPSRV	NTP Server	2 000
PEP20	VRTX	Edge Router on Remote Sites	206 796
PEP14	USERPC	User PC	1 000
PEP5	GWMSCADA	Medium Voltage Gateway	410 532
PEP6	GWXSCADA	High Voltage Gateway	615 800
PEP17	FWDR	Firewall IPS/DR	105 000
PEP10	WEBCADA	Web Server	45 000
PEP18	MGMSRV	Management Server	3 000
PEP9	RTUSCADA	Remote Terminal Unit	2 621 927
PEP4	FEMSCADA	Medium Voltage Front End	660 000
PEP7	VGROUTER	Virtual Router	36 500
Annual Infrastructure Value (AIV)			6 925 555

than those associated to the threat scenario, the system therefore retrieves a concrete attack vector for Threat $AS01HV$: 'EntryPoint=VGROUTER; Target1=WEBSCADA; Target2=FTPSRV; BusinessDevice=FEXSCADA'

Based on the information from the mission dependency model, we have retrieved the nodes in paths pointing to Business Devices for threat $AS01HV$. Each node has a unique identifier, a host name that corresponds to an instantiated device, a PEP_Type which corresponds to the abstraction class of the PEP, and a Node_Type, which indicates whether the node is an entry point, an intermediate node, a target node or a business device. Please note that business devices are the most critical node types from the emulation environment. They are required to accomplish a business process within the organization. Table 4 summarizes this information.

Table 4. Retrieved node information.

Node Identifier	Host Name	PEP_Type	Node_Type
b992e600-0de2-496c-kkk0-...	mferp1	FEXSCADA	Business Device
718bc323-9d78-4ada-9629-...	dorete	FTPSRV	Target2
e06496d2-6120-4c9d-a310-...	LANGUARD	MGMSRV	Intermediate Node
94d37c8d-bc68-47bf-ad60-...	ARCHIVESRV	FTPSRV	Target2
19b2bb1e-9f23-4fe8-902e-...	KALI	MGMSRV	Intermediate Node
e470baab-5d88-4b20-ac28-...	FTPSRV01	FTPSRV	Target2
876hhezq-77tg-4897-665g-...	xferp2	FEXSCADA	Business Device
d3480ddc-fe4a-4b94-9dc5-...	mferp2	FEXSCADA	Business Device
b54b235d-116a-49b4-9052-...	xferp1	FEXSCADA	Business Device
c9fa4086-d979-4794-9b6e-...	STWEB	WEBSCADA	Target1
c6dd8687-c791-4f91-bf58-...	TPT2000-T2	RTUSCADA	Intermediate Node

As shown in Table 4, the PEP types of nodes involved in paths leading to critical devices are: WEBSCADA, FEXSCADA, MGMSRV, RTUSCADA, and FTPSRV. Note that none of the nodes are defined as entry points, and those associated to the PEP_Type MGMSRV do not have pre-defined authorized mitigation actions. In such a case, they are discarded from our analysis.

5.3 Dynamic *RORI* Evaluation

For the RORI evaluation, we obtain the list of authorized mitigation actions associated to threat AS01HV. Table 5 summarizes this information.

Table 5. Authorized mitigation action information.

PEP_Type	WF	Affected Node	Q	COV	MA_Type	EF	ARC (€)
WEBSCADA	3	STWEB	1	0.09	Shutdown	0.15	15.00
					Reboot	0.01	15.00
					Patching	1.00	25.00
FEXSCADA	4	mferp1, mferp2	4	0.50	Shutdown	0.15	200.00
		xfep1, xferp2			Reboot	0.01	200.00
MGMSRV	1	LANGUARD, KALI	2	0.00	No action	0.00	0.00
RTUSCADA	5	TP2000-T2	1	0.16	Shutdown	0.15	15.00
					Reboot	0.01	15.00
FTPSRV	2	ARCHIVESRV,	3	0.19	Shutdown	0.15	15.00
		FTPSRV01,			Reboot	0.01	15.00
		dorete			Patching	1.00	25.00

As shown in Table 5, each PEP_type has an associated weighting factor (WF) that indicates the level of priority or criticality inherent to the type of PEP in the execution of a mission. For instance, management servers (e.g., MGMSRV) are assigned a WF=1, FTP servers (e.g., FTPSRV) are assigned a WF=2, Web servers (e.g., WEBSCADA) are assigned a WF=3, Front End devices (e.g., FEXSCADA) are assigned a WF=4, and Remote Terminal Units (i.e., RTU) are assigned a WF=5. The *COV* value is computed using Eq. 4.

To each PEP_type none, one or more of the following mitigation actions can be applied: **(1)** Patching, refers to a piece of software designated to update a computer program or its supporting data, to fix or improve it. This includes fixing or removing security vulnerabilities and other bugs and improving the usability or performance. **(2)** Reboot, refers to the process of restarting a device or a computer program. **(3)** Shutdown, refers to completely remove any possibility to access a device by powering off a device.

Each type of mitigation action has an associated effectiveness (EF) and cost (ARC). The EF value is assigned automatically using the information from Table 2, whereas the ARC value is assigned by expert knowledge and statistical data. Using Eq. 1, we compute the RORI value for individual and combined mitigation actions in Table 6. Each response considers the ARC and EF to calculate the risk mitigation value (RM), using Eq. 3, and take into account restrictions among the candidates (e.g., shutdown a given device is totally restrictive to all other actions that could be executed to such device).

Table 6. RORI evaluation results for individual mitigation actions.

MA	MA_Type	PEP_Type	RM	Restrictions	RORI
MA_1	Shutdown	WEBSCADA	0.0141	MA_2, MA_3	4.07
MA_2	Reboot	WEBSCADA	0.0009	MA_1	0.26
MA_3	Patching	WEBSCADA	0.0937	MA_1	27.09
MA_4	Shutdown	FEXSCADA	0.0750	MA_5	21.66
MA_5	Reboot	FEXSCADA	0.0050	MA_4	1.44
MA_6	Shutdown	RTUSCADA	0.0234	MA_7	6.76
MA_7	Reboot	RTUCADA	0.0016	MA_6	0.46
MA_8	Shutdown	FTPSRV	0.0281	MA_9, MA_{10}	8.11
MA_9	Reboot	FTPSRV	0.0019	MA_8	0.55
MA_{10}	Patching	FTPSRV	0.1875	MA_8	54.15

The mitigation action with the highest RORI index is MA_{10}, which requires to install a patch for the PEP_Type "FTPSRV". More specifically, the node "dorete" requires a patching against two vulnerabilities (i.e., CVE-2008-4250, and CVE-2006-3439). Considering the previous information about mitigation actions, a total of 214 combinations have been performed to evaluate the RORI metric. Table 7 presents the top 5 combination results.

Table 7. RORI evaluation results for combined mitigation actions.

MA	ARC	RM	RORI
$MA_{2,3,4,6,9,10}$	295.0	0.3085	89.07
$MA_{3,4,6,9,10}$	280.0	0.308	88.94
$MA_{2,3,4,6,10}$	280.0	0.3075	88.80
$MA_{3,4,6,10}$	265.0	0.3071	88.67
$MA_{2,3,4,7,9,10}$	295.0	0.2975	85.91

As shown in Table 7, the highest RORI index corresponds to the combination of mitigation actions MA_2, MA_3, MA_4, MA_6, MA_9, and MA_{10} which proposes the following six concrete actions: ***(1)*** *Reboot node STWEB.* ***(2)*** *Install patches to the node STWEB against CVE-2008-4250, and CVE-2006-3439.* ***(3)*** *Shutdown the node mferp2.* ***(4)*** *Shutdown the node TPT2000-T2.* ***(5)*** *Reboot nodes ARCHIVESRV and FTPSRV01* ***(6)*** *Install patches to the node dorete against CVE-2008-4250, and CVE-2006-3439.*

5.4 Response Plan Generation

For each evaluated mitigation action (including all possible combinations), a response plan has been generated. Each response plan contains the identification of the mitigation action(s), the PEP responsible for its enforcement, and the associated RORI index. The Response Plans contain mitigation actions applied only to the nodes obtained in the Attack Graph parsing (e.g., STWEB, ARCHIVESRV, FTPSRV01, dorete, etc). For the previous scenario, a total of 224 response plan were generated.

5.5 Response Plan Selection and Visualization

To select a semi-optimal response plan, all proposed response plans based on RORI values are evaluated based on their short-, mid-, and long-term impacts onto the company from an operational perspective, i.e., operational impacts OI_0, OI_1, OI_2. These values are derived as described in [11], where a mission dependency model was created by business experts to the company, and a network dependency model was automatically learned from network traffic analyzes. Table 8 shows a comparison of a selected subset of all 224 evaluated response plans.

Table 8. Financial and operational impact comparison.

MA	RORI	OI_0	OI_1	OI_2
RP_1	4.07	0.1407	0.1407	0.1407
RP_2	0.26	0.137	0.0799	0.0
RP_3	27.09	0.0247	0.0	0.0
RP_4	21.66	0.0989	0.0989	0.0989
RP_5	1.44	0.9995	0.8247	0.0
RP_6	6.76	0.1855	0.1855	0.1855
RP_7	0.46	0.1745	0.1051	0.0
RP_8	8.11	0.0756	0.0756	0.0756
RP_9	0.55	0.0731	0.0478	0.0
RP_{10}	54.15	0.038	0.0	0.0

The semi-optimal response plan that matches the criteria is RP_{46}, with a deviation of ϵ=0.2, a RORI index equivalent to 71.34%, and the following operational impacts: $OI_0 = 0.2724$, $OI_1 = 0.2161$, and $OI_2 = 0.1781$. As a result, the selected response plan is displayed in the visualization module, proposing the enforcement of mitigation actions MA_3, MA_6, MA_9, and MA_{10} which correspond to the following four concrete actions: ***(1)*** *Install patches to the node STWEB against CVE-2008-4250, and CVE-2006-3439.* ***(2)*** *Shutdown the node TPT2000-T2.* ***(3)*** *Reboot nodes ARCHIVESRV and FTPSRV01.* ***(4)*** *Install patches to the node dorete against CVE-2008-4250, and CVE-2006-3439.*

6 Related Work

Dynamic systems that automatically evaluate and select the actions to mitigate complex attack scenarios is an open research that represents a big challenge to critical infrastructures. Some research works has been conducted in the assessment of security measures. Kotenko et al. [12,13], e.g., propose a framework for cyber attack modeling and impact assessment based on attack graph generation, real-time event analysis techniques, prognosis of future malefactor steps, attack impact assessment, and anytime approach for attack graph building and analysis. We differ from these research as we do not propose new algorithms or methods of attack graph construction, instead, we propose a novel framework that processes input data to generate response plans for pre-defined threat scenarios.

Agosta et al. [14] propose a software countermeasure framework based on the combination of a cryptographic algorithm implementation with a polymorphic engine which dynamically and automatically transforms the binary code to be protected. The approach enables the generation of multiple versions of the code, to prevent an attacker from recognizing the exact point in time where the observed operation is executed and how such operation is performed. We differ from the previous work since it can only be applied to an algorithm or to a subset of vulnerable instructions, ours is a modular framework that is applied in a whole network to automatically analyze the impact of possible attacks and provide an appropriate response based on multiple criteria.

Ossenbuhl et al. [15], introduce a response selection model that allows mitigating network-based attacks based on an intuitive response selection process that evaluates negative and positive impacts associated with each countermeasure. The model overcomes several challenges in automated response selection, however, several other challenges are left uncovered (e.g., scalability and performance issues, i.e., no alert correlation mechanism has been developed to handle large amount of alerts, security issues, i.e., lack of secured communication channel among the system's components, and applicability issues, i.e., lack of applying responses in more advanced attack scenarios).

7 Conclusions and Future Work

We introduce a Dynamic Risk Management Response System that evaluates, ranks and selects optimal mitigation actions based on financial, operational and threat impact assessments. The system generates response plans containing mitigation actions and corresponding financial and operational evaluations. There are two main improvements of this approach: (i) the dynamic evaluation performed by the system, and (ii) the automation of the response plan generation.

In terms of dynamicity, the system operates on snapshots of a target system with a regular frequency within minutes. At each snapshot, the current condition are assessed. Upon reception of a risk profile, indicating a possible exploitation of a given threat, the system requests input information and performs corresponding analyses. Input data may vary at each snapshot, indicating, e.g., that one or more PEPs are detected on the system, or that one or more mitigation actions are not authorized for the current snapshot. As a result, every time a system snapshot is performed, values of parameters, such as AIV and RM, dynamically change, which in turn changes RORI indexes for the set of evaluated responses.

In terms of automation, the system performs the process in an automatic chain, from the detection of the threat, to the visualization of the selected response plan. The process is automated to assist security administrators in the decision making process. It does not enforce the mitigation action automatically, but provides an assessment of the current system conditions in order to highlight the appropriate response strategies to administrators. For critical infrastructures, selection of mitigation actions generally requires manual intervention by an operator, an approval by supervisors, or more advanced system operator.

Future work will concentrate on managing conflicts among restrictive actions. It is possible that the best response plan suggests an enforcement of mutually exclusive mitigation actions. In such a case, the system should assign priorities to each action being able to discard those with low priority rate.

Acknowledgements: This work received funding from the PANOPTESEC project, as part of the 7th Framework Programme (FP7) of the European Commission (GA 610416).

References

1. E. Filiol, C. Gallais, "Critical Infrastructure: Where we stand today?", *9th International Conference on Cyber Warefare and Security*, (2014).
2. K. Gordon, M. Dion, "Protection of Critical Infrastructure and the role of investment policies relating to National Security", *OECD*, Whitepaper, (2008).
3. Y. Ben Mustapha, H. Debar, G. Blanc. "Policy Enforcement Point Model", *Conference on Security and Privacy in Communication Networks*, pp. 278–286, (2014)
4. G. Gonzalez-Granadillo, M. Belhaouane, H. Debar, G. Jacob. "RORI-based countermeasure selection using the OrBAC formalism", *International Journal of Information Security*, Vol. 13(1), pp. 63–79, (2014)
5. Schmidt, M. Return on Investment (ROI): Meaning and Use, *Encyclopedia of Business Terms and Methods*, (2011)
6. 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, (2006)
7. Mizzi, A. "Return on Information Security Investment: the Viability of an Anti-Spam Solution in a Wireless Environment", *International Journal of Network Security*, vol. 10, number 1, pp. 18–24, (2010)
8. G. Gonzalez-Granadillo, J. Garcia-Alfaro, H. Debar. "A Polytope-based Approach to Measure the Impact of Events Against Critical Infrastructures", *Journal of Computer and System Sciences*, (2016)
9. G. Gonzalez-Granadillo, A. Motzek, J. Garcia-Alfaro, H. Debar. "Selection of Mitigation Actions Based on Financial and Operational Impact Assessments". *International Conference on Availability, Reliability and Security*, (2016)
10. Lockstep Consulting. "A Guide for Government Agencies Calculating Return on Security Investment", Available at: http://lockstep.com.au/library/return_on_investment, (2004)
11. A. Motzek, R. Moller, M. Lange, S. Dubus. "Probabilistic Mission Impact Assessment based on Widespread Local Events", *NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact*, (2015)
12. I. Kotenko, A. Chechulin "A Cyber Attack Modeling and Impact Assessment Framework", *5th International Conference on Cyber Conflict*, (2013)
13. I. Kotenko, E. Doynikova. "Dynamical Calculation of Security Metrics for Countermeasure Selection in Computer Networks", *24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing*, (2016).
14. G. Agosta, A. Barenghi, G. Pelosi. "A Code Morphing Methodology to Automate Power Analysis Countermeasures", *49th Annual Design Automation Conference*, pp. 77-82, (2012)
15. S. Ossenbuhl, J. Steinberger, H. Baier. "Towards Automated Incident Handling: How to Select an Appropriate Response Against a Network-based Attack?", *Conference on IT Security Incident Management & IT Forensics*, (2015)