A Multi-Criteria Ranking of Security Countermeasures

Nicola Nostro, Ilaria Matteucci, Andrea Ceccarelli, Francesco Santini, Fabio Martinelli, Andrea Bondavalli

Abstract

We propose a multi-criteria framework for ranking controlling strategies based on several weights, such as delay-time, resource cost, and success-probability of attacks defined via quantitative threat analysis. Therefore, by assigning a different priority to weight-dimensions, we can rank controllers in an adaptive way. We exemplify our approach on the Customer Energy Management System, that acting as an interface among different systems, is open to attacks. We consider the Man in the Middle and Denial of Service attacks.

CCS Concepts

• Security and privacy → Security requirements; Formal security models;

Keywords

Security assessment; Semiring; Algebraic formalism

1. INTRODUCTION

This paper presents an adaptive multi-criteria framework for ranking controlling strategies to minimize the impact of attacks, thus helping in defining controllers that favour security, cost-effectiveness, or energy efficiency. We enhance the results in [12] by introducing a multi-criteria analysis to drive the countermeasures ranking.

The proposed framework consists of two main steps: i) a security analysis, performed by Adversary View Security Evaluation (ADVISE) formalism [8] to evaluate attack points and paths with respect to several criteria and to identify those that are feasible, and to rank attack weights, from the perspective of an attacker; ii) an evaluation of different run-time execution traces, corresponding to several countermeasures on the basis of the multi-criteria analysis results.

This work has been partially supported by the TENACE PRIN Project (n.20103P34XC), the H2020-MSCA-ITN-2015-NeCS 675320, and the FP7 Project SmartC2Net.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

SAC 2016, April 04-08, 2016, Pisa, Italy
© 2016 ACM. ISBN 978-1-4503-3739-7/16/04... $15.00
DOI: http://dx.doi.org/10.1145/2851613.2851878

2. RANKING SECURITY STRATEGIES VIA SECURITY ANALYSIS

System requirements are expressed in the form of a hierarchy, with stringent requirements at the top level, and less stringent ones at lower positions. System requirements are expressed in the form of a hierarchy, with stringent requirements at the top level, and less stringent ones at lower positions. In our framework, the ranking of controllers drives the selection of the best one with respect to the current hierarchy of requirements. In case of reorganization of the requirements hierarchy (e.g., in multiple-phased systems, whose operational life spans multiple phases characterized by different functional and non-functional requirements), a new ranking is easily provided without performing the analysis of the whole system again. The framework is composed by the following steps:

- the system specification in terms of its functional and non-functional requirements;
- once the system has been modelled, a security assessment is performed, thus providing a series of possible attacks that can be perpetrated on the system. The analysis considers several criteria and provides an estimation of each attack according to all criteria under investigation. Since the definition of the profile of an attacker is at the basis of the risk&threat evaluation processes [11], we defined two attackers’ profiles: hacker and civil activist;
- the exploitation of functional and non-functional system’s requirements to classify countermeasures according to possible trade-off among different criteria. Given the variety of potential attackers’ behaviour, we define several controllers that follow the attacker’s behaviour step by step;
- the adaptive ranking of countermeasures driven by the requirements’ hierarchy. Indeed, we use the information on the attack, obtained through the security analysis, to classify and rank countermeasures also according to the system’s requirements.

The classification is driven by the system’s requirements hierarchy and it is modelled by the order of the considered semiring [1]. We exemplify the proposed framework on the Customer Energy Management System (CEMS) [7], a service for an advanced energy management of low voltage grid.

The paper is structured as follows: Section 2 describes the multi-criteria framework for the ranking of countermeasures. Section 3 recalls controllers and formally defines the multi-criteria ranking. Section 4 exemplifies our approach on the CEMS reference scenario. Section 5 discusses related work and Sec. 6 draws conclusions and suggests future work.
3. MULTI-CRITERIA CLASSIFICATION OF QUANTITATIVE COUNTERMEASURES

We adopt semirings as the algebraic formalism to represent metrics used to rank the countermeasures.

Definition 3.1 (c-semiring [1]). A c-semiring is a five-tuple \( \mathbb{K} = (\mathbb{K}, +, \times, \bot, \top) \) such that \( \mathbb{K} \) is a set, \( \bot, \top \in \mathbb{K} \), and \( +, \times : \mathbb{K} \times \mathbb{K} \to \mathbb{K} \) are binary operations making the triples \((\mathbb{K}, +, \bot)\) and \((\mathbb{K}, \times, \top)\) commutative monoids (semi-groups with identity), satisfying i) \((\text{distributivity})\) \( \forall a, b, c \in \mathbb{K}. a \times (b + c) = (a \times b) + (a \times c) \), ii) \((\text{annihilator})\) \( \forall a \in \mathbb{A}. a \times \bot = \bot \), and iii) \((\text{top element})\) \( \forall a \in \mathbb{K}. a + \top = \top \).

The idempotency of + leads to the definition of a partial ordering \( \leq_{\mathbb{K}} \) over the set \( \mathbb{K} \) (\( \mathbb{K} \) is a poset). Such complete partial order is defined as \( a \leq_{\mathbb{K}} b \) if and only if \( a + b = b \), and + becomes the least upper bound \((\text{lub})\) of the lattice \((\mathbb{K}, \leq_{\mathbb{K}})\). Thus \( b \) is “better” than \( a \). Therefore, we can use + as an optimisation operator and always choose the best available solution. Other derived properties are [1]: i) both \( + \) and \( \times \) are monotone over \( \leq_{\mathbb{K}} \), ii) \( \times \) is intensive (i.e., \( a \times b \leq_{\mathbb{K}} a \)), iii) \( \times \) is closed (i.e., \( a \times b \in \mathbb{K} \)), and iv) \( \{K, \leq_{\mathbb{K}}\} \) is a complete lattice where \( \bot \) and \( \top \) are its bottom and top elements, respectively. A countermeasure (controlling strategy) [3] is a run-time execution trace of a controller \( E \) that follows the behaviour of a target \( F \) step by step based on control rules in Tab. 1. The resulting behaviour is denoted by \( E_{\times K}^{\leq_{\mathbb{K}}} F \), where \( \mathbb{K} \) is the semiring used to specify quantities to quantitatively estimate the contribution of each countermeasure on the system. The alphabets of \( E, F \), and of the resulting process \( E_{\times K}^{\leq_{\mathbb{K}}} F \) are different, as \( E \) may perform control actions of the form \( a, \forall a, b, \exists a \) for \( a, b \in \text{Act} \), denoting respectively the actions of acceptance, that means that the action of \( F \) is accepted by the controller \( E \), suppression, that means that the action of \( F \) is hidden (becomes \( \tau \)) by \( E \), and insertion, that introduces correct action in front of the action of \( F \). Each action of controller and target is associated to a value of the semiring \( \mathbb{K} \), i.e., we have a pair \((a, k)\) as label, where \( k \in \mathbb{K} \) is a quantity related to the effect \( a \). Given an execution trace \( t = (a_1, k_1) \ldots (a_n, k_n) \), we define label \( l(t) = a_1 \cdots a_n \), and run weight \( |t| = k_1 \times \ldots \times k_n \). Hence, we are able to rank different strategies and, eventually, select the “best” one as follows.

Definition 3.2. [3] Given an agent \( F \), and a semiring \( \mathbb{K} \), a controller \( E_2 \) is better than a controller \( E_1 \), w.r.t. \( F \), \( E_1 \leq_{\mathbb{K}, F} E_2 \), iff \( \|E_1 \times_{\mathbb{K}} F\| \leq_{\mathbb{K}} \|E_2 \times_{\mathbb{K}} F\| \). \( E_2 \) is always better than \( E_1 \), \( E_1 \leq_{\mathbb{K}} E_2 \), iff \( E_1 \leq_{\mathbb{K}, F} E_2 \), for any \( F \).

Since the Cartesian product of semirings is a semiring, we can rank countermeasures using various criteria by exploiting the lexicographic order among the considered semirings.

Definition 3.3. Let \( \{K_1, +_1, \times_1, \bot_1, \top_1\} \) and \( \{K_2, +_2, \times_2, \bot_2, \top_2\} \) be c-semirings. Then, the associated lexicographic order \( \leq_{\mathbb{K}} \) on \( K_1 \times K_2 \) is given by:

\[
\langle k'_1, k'_2 \rangle \leq (k''_1, k''_2) \quad \text{if} \quad \left\{ \begin{array}{l}
k'_1 \leq k''_1 \\
k'_2 \leq k''_2 \land k'_1 = k''_1 \wedge k'_2 \leq k''_2
\end{array} \right.
\]

4. RANKING OF COUNTERMEASURES IN THE CEMS CASE STUDY

The CEMS is an application service or device of low voltage grids for an advanced energy management; it is based on tariff information and an integration of Distributed Energy Resources (DER) for a more balanced grid stability. A basis for this control network is established by the deployment of a comprehensive Advanced Metering Infrastructure (AMI) for Automated Meter Reading (AMR), able to monitor the electricity consumption of households collected by smart meters (see [7]). Since CEMS may operate in a very hostile environment, our security analysis focuses on two well-known attacks potentially harmful for the CEMS functionalities, namely: 1) a Denial of Service (DoS) attack, consisting in the introduction of relevant quantity of noise in the bi-directional flow of information between CEMS and the AMR gateway. This may lead to a halt failure of the AMR gateway or CEMS or to a delay of the Energy Management Gateway (EMG) activity, thus reducing availability of the energy distribution system; 2) a Man in the Middle (MiM) attack, capturing messages exchanged between EMG and CEMS or between CEMS and the higher control layer. For instance, the attacker can delay the messages or alter their content to produce an undesired effect, or simply collect data, thus causing a violation of integrity or confidentiality.

The first step of the Security Model Based Assessment is the definition of the profile of an attacker. We assume two profiles, a hacker and a civil activist, in which the hacker has high technical skill, and might operate on commission driven by gain, while the civil activist, moved by ideological motivations, has a lower technical skill with respect to the hacker. We exploit the ADVISE formalism and the related simulator. Fig. 1 shows the ADVISE Attack Execution Graph (AEG) of both the DoS and MiM attacks, which aim at achieving the three attack goals: availability, confidentiality, and integrity violations. The AEG represents the sequence of attack steps (rectangles in the figure) the attacker has to perform in order to realize the goal (the three ovals in figure). Squares represent different access domains owned and triangles are the attacker skills regarding the next attack step. Circles denote the knowledge the attacker acquires while perpetrating the attack. We also define a set of access domains, knowledge, attack skills, and attack preferences, initially owned by different profiles of attackers, which represent the input to the ADVISE model. Moreover, the attack steps of the model have a specific time duration, cost, success probability, and detection probability, which are dif-

![Figure 1: ADVISE AEG for MiM and DoS attacks.](image-url)
Table 1: Semantics definitions for quantitative control rules.

<table>
<thead>
<tr>
<th>Time Unit</th>
<th>Success Prob.</th>
<th>Cost Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Civil activist</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 2: DoS attack: total average time (T), success probability (P), and cost (C).

<table>
<thead>
<tr>
<th>Time Unit</th>
<th>Success Prob.</th>
<th>Cost Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Civil activist</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3: Corrupt Messages attack.

<table>
<thead>
<tr>
<th>Time Unit</th>
<th>Success Prob.</th>
<th>Cost Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Civil activist</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 4: Read Messages attack.

<table>
<thead>
<tr>
<th>Time Unit</th>
<th>Success Prob.</th>
<th>Cost Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Civil activist</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

4.1 Evaluation of Countermeasures on CEMS

The execution of the ADVISE model provides information related to: i) cost, ii) time, and iii) success probability to achieve a specific attack goal by one of the two attackers as shown in Tab. 2, Tab. 3, and Tab. 4. The cost measure is modelled by the weighted semiring $W = (\mathbb{R}^+ \cup \{\infty\}, \min, +, \infty, 0)$. This cost represents the total amount of hardware/software resources spent by the attacker (to attack) and by the defender (to defend). The delay suffered by the system (again, considering attacks and countermeasures) needs to be reduced as much as possible. To accomplish this, if $t$ is the time-cost of an action, then we model it as $1/t$ and we adopt the fuzzy semiring $\mathbb{F} = ([0,1], \max, \times, 0, 1)$. We suppose always $t \neq 0$. In this way, we compose two delays $t_2 > t_1$ by selecting the higher one ($1/t_2$ with respect to $t_1$) and we prefer the lower delay ($1/t_1$ with respect to max). Hence we minimize the bottleneck delay during the system execution. Finally, the success probability of an attack is represented by the probabilistic semiring $\mathcal{P} = ([0,1], \max, \times, 0, 1)$. On the attacker’s side, such score represents the probability to be successful, while on the defender’s side it models the effectiveness probability of stopping the relative attack: if the countermeasure is 100% effective, then the probability $p$ of an attack is annihilated, i.e., $p \times 0 = 0$ (equal to $\bot$).

Depending on which measure is prioritized, we have the following categories. Secure countermeasures: the controllers are ordered based on their security, measured as the probability of being attacked, modelled by the probabilistic semiring. Economical countermeasures: a controller can be said to be economical when the priority is given to the dimension of cost, modelled by the weighted semiring.

Economical countermeasures: the fuzzy semiring models the measure of consumed time, interpreted as ecological impact. Hence the optimal controller is the lowest with respect to the amount of consumed energy. Referring to the attacks’ graph in Fig. 1, the action GainNetworkAccess represents a possible first step of an attack. Hence, the controlling strategies has a hook before this action in such a way to be prepared to activate a possible countermeasure. Let us consider three countermeasures:

$C_1 = \langle \text{GainNetworkAccess} \rangle$

$C_2 = \langle \text{SendAccessRequest}, (z_1, y_1, z_1) \rangle C'$

$C_3 = \langle \text{GainNetworkAccess}, (x_2, y_2, z_2) \rangle C'_2$

where both $C'$ and $C'_2$ behave according to the suppression rule on all the other attacker’s action, while $C'_2$ behaves by suppressing the NetworkScanning action. Then we consider that also this countermeasure works by accepting all the other actions. $C_1$ and $C_2$ act differently only on the first action GainNetAccess: $C_1$ modifies the behaviour by intro-
MiM attack. Let us consider \( \langle t, c, p \rangle \in K \) where \( K \) is the Cartesian product of \( \mathcal{F}, \mathcal{W} \) and \( \mathcal{P} \) (ecological controller) as lexicographic order to rank countermeasures. Let us also consider the MiM attacker corrupts the message \((\text{Tab. 3})\), countermeasure \( C \) according to the probability of attack, then the criteria under analysis. As a result, we can adaptively rank the criteria under analysis.

Let us now compare \( C_2 \) and \( C_3 \). Since \( C_3 \) accepts all the actions, (\( X_2, Y_3, Z_3 = (\lambda, \lambda, \lambda) \)), \( C_3 \) is more ecological (less cost) than \( C_2 \). Hence \( C_3 \) is more ecological than \( C_2 \).

Let us now consider the hierarchy of requirements by privileging those about the probability of attack, then time, and finally cost requirements, \( (p, t, c) \) (secure countermeasure).

The new ranking leads to a new classification of countermeasures. Being \( Z_2 \times C_1 \succ P \perp \), we have \( C_3 \preceq_{K, A_{MIMC}} C_2 \). The new classification is made starting from the existing evaluation (no need to perform it again).

DoS attack. \( C_3 \) is again always worse than \( C_2 \), due to the monotonicity of the semiring. \( C_2 \) suppresses all the actions of the DoS attack while \( C_3 \) suppresses the NetworkingAccess action. This increases the probability to prevent attack, time, and cost of the trace. Hence,

\[
\begin{align*}
C_2 & \preceq_{K, A_{MIMC}} A_{DoS} \\
C_3 & \preceq_{K, A_{MIMC}} A_{DoS}
\end{align*}
\]

In this case, the hierarchy of requirements is crucial for ranking countermeasures. For example, let us consider the first line of Tab. 3 for the civil activist profile: \( C_1 = 1/180, C_e = 45.4275, \) and \( C_p = 0.6170 \). If \( X_4 \prec\prec 1/180 \) and \( X_3 \prec\prec 1/180 \) then \( \min(X_2, C_1) = X_2 = \min(X_1, C_1) \). Hence, if \( X_2 \prec\prec X_3 \) then \( C_3 \) is more ecological than \( C_2 \), otherwise, if the vice versa holds then \( C_3 \) is more ecological than \( C_3 \). Finally, if \( X_2 \approx X_3 \) then they are equally ecological, and we have to rank them according to their costs. The same reasoning can be done for the cost as well: if their cost is the same, we compare their probability.

6. CONCLUSION AND FUTURE WORK

This work presents an adaptive multi-criteria framework for the ranking of countermeasures to select the one that satisfies the system requirements (arranged in a hierarchy) in presence of an attack. We exemplified the approach in terms of the CEMS use case. As future work, we plan to introduce countermeasures as part of the system model in order to evaluate their impact on the initial system based on the criteria under analysis. As a result, we can adaptively change the ranking according to the obtained measurements.

7. REFERENCES