A Meta-heuristically Optimized Fuzzy Approach towards Multi-metric Security Risk Assessment in Heterogeneous System of Systems

Iñaki Eguia and Javier Del Ser
TECNALIA, 48170 Zamudio, Bizkaia, Spain

Keywords: Multi-metric Security Assessment, Fuzzy Logic, Meta-heuristics

Abstract: Security measurement of complex systems is a challenging task since devices deployed over the so-called System of Systems (SoS) are extremely heterogeneous and hence imply an interoperability effort in order to enable a common resilient security measurement language. Moreover, systems demand more features beyond security concept, require to preserve privacy and claim for dependable structures in order to seek a holistic and aggregated security and safety view. This paper addresses this need by capitalizing the availability of multiple security metrics through an hybrid meta-heuristic fuzzy aggregation and composition approach that takes into account the expertise compiled by the security manager, towards the generation of visual dashboards reflecting the SPD (Security, Privacy and Dependability) risk status of the system at hand.

1 INTRODUCTION

In the security field one of the most sounding paradigms resides in the security interoperability within a heterogeneous device landscape. In this scenario each of such devices performs with different protocols and scales. Interoperability is by itself a challenge for engaging the security paradigm as a built-in approach. Many efforts have been devoted to define security patterns (Yoshioka et al., 2008; Heyman et al., 2007; VanHilst & Fernandez, 2007; Fernandez et al, 2007) so as to develop and implement a understandable security backdrop.

Unfortunately, this background is usually quite complex. In this context, the setup elaborated by the nSHIELD initiative (NSHIELD, 2013) proposes a System of Systems representing a set of assets: subsystems, software components, protocols and devices and boards. These elements are configured along node, network and middleware-overlay layers. On the other hand, risks are denoted as the probability that a threat can become real impacting in a vulnerability of one or more components from those listed above. Threats are numerous and can be predictable or unpredictable. Those which can be predicted may be guarded by metrics, whereas those which are unpredictable could be challenged by composable, heuristics techniques. Therefore, metrics will be mapped to threats and problems to be measured. For example, if a problem of a given system is the network latency, the network latency must be measured. This obvious affirmation is the key for starting the process for selecting the correct metrics for any heterogeneous system. Consequently, risk analysis is the first process for creating a set of security metrics in scenarios with a diverse device spectrum.

This paper joins this research trend by outlining and sketching a novel multi-metric approach for heterogeneous systems capable of measuring risks impacting on different vulnerabilities in an interoperable and normalized fashion. This practical approach requires understanding and identifying beforehand security needs of the system at hand, as well as those of its constituent components. In other words, current vulnerabilities and threats must be identified so as to discriminate those vulnerabilities and threats more likely to take place in the future. To this end, this paper elaborates in advance of several evident, relevant observations: 1) systems' complexity yields an accordingly complex and also non-interoperable security management; and 2) without loss of generality, metrics considered in this approach are restricted to operational activities beyond security organizational metrics and measurements. Moreover, this paper depicts SPD metrics as resiliently built-in artifacts that are aggregatedly delivered from the engineering process to the operation phase, thus rendering a holistic SoS SPD view. Finally, a self-optimized hybrid meta-heuristic fuzzy system will be conceptualized as a de-

Eguia I. and Del Ser J..
A Meta-heuristically Optimized Fuzzy Approach towards Multi-metric Security Risk Assessment in Heterogeneous System of Systems.
DOI: 10.5220/0004876802310236
In *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems* (MeSeCCS-2014), pages 231-236
ISBN: 978-989-758-000-0

cision support system capable of providing the system security manager with an easy and understandable mechanism to tune and trigger security-related actions and rules based on fine-grained input metrics and measurements.

2 SPD METRICS IN HETEROGENEOUS DEVICE ECOSYSTEMS

The meaning of metric can be understood from a naive business standpoint in the sense that metrics should be made similar to human understanding because they need to be recognized and understood by both business and technical engineers operating on the systems. Informational SPD metrics are deemed an important factor when making reliable, well-grounded decisions about several aspects of security and dependability, ranging from the design of SPD architectures and controls to the effectiveness and efficiency of SPD operations. SPD metrics strive to offer a quantitative and objective basis for security assurance.

Given the application scope in Industrial Systems of Systems (SoS) environment tackled in this paper, we will analyze and combine traditional operational indicators with SPD metrics. Metrics in industrial operations (i.e. metrology) have always been regulated and certified by a higher authority. In the IT area this methodology has been applied in a less rigorously manner, since safety has always prevailed over security. However, SoS environments require both security and safety (part of dependability) requisites, as threats could proceed from both virtual and real (unpredicted/failure threats) worlds.

The spectrum of SPD metrics derived in nSHIELD constitute the first attempt in the related literature to correlate operational and SPD metrics so as to develop a business continuity approach for industrial sectors. It is important to highlight that control systems such as SCADAS or ICS (Industrial Control Systems) not only depend on the operational process (which is linked directly to business), but also is becoming progressively more dependent on robustness, resilience and security factors that preserve operation from malicious attacks and large failures. Indeed, the dependability concept guarantees this fact: dependability mechanisms deal with availability (e.g. threats against DDoS), which is the most important feature for industrial operations. However, security may also be threatened in terms of integrity; for instance, a man-in-the-middle attack for value modification in the communications link from smart meters to concentrators could cause less profit to electric vendors and an unequal operation for distribution system operators when balancing energy offering & demand. On the other hand, the notion of privacy implies confidentiality and anonymity, and is becoming essential as Big Data gets involved within industrial and large organizational settings. Therefore, nSHIELD metrics are set towards business continuity: 1) heterogeneous but measurable; 2) understandable by the human being with comprehensible, possibly fuzzy glossary; and 3) composable since inputs are aggregated through an expert system. This envisaged portfolio of requirements makes the nSHIELD view fulfill with the so-called Security by Design (SbD) principles (Cavoukian & Dixon, 2013): nSHIELD SPD metrics apply to security, privacy and dependability built-in concepts and functionalities within the whole engineering process. Furthermore, such functionalities are not seen as the final patch but as an intrinsic conceptualization of the whole and holistic engineering and operation procedure. SPD metrics are extracted from a set of SPD requirements and risks statements within SoS scenarios.

Bearing this rationale in mind, the nSHIELD multi-metric approach follows a quantitative focus. This approach provides a metric template for metrics identification and gathering process. In the first specification approach more than 60 metrics were identified and structured in layers $\{\text{SPD}, L_x\}$. Metrics identified as heterogeneous sometimes overlap in different layers. The result of measurements according to these metrics has to be described quantitatively. The following list oversees some of the most relevant metrics concluded after this study[1]:

1. Code execution (Node Layer): verification that only authorized code (booting, kernel, application) runs on the system.
2. Network delay (Network Layer): this is a performance metric used for measuring the delay induced by a node in retransmitting incoming data.
3. Network Capacity (Network Layer): this is a performance metric used for measuring the networks capacity, which shall be large enough to allow the necessary traffic to go through. As a rule of thumb, at normal operation, the traffic should be about 60-70% of the network capacity, so as to avoid bottlenecks when there will be traffic peaks.
4. Discovery frequency (Middleware Layer): amount of discovery events per protocol and unit

[1]Upon its acceptance a more detailed list of metrics will be presented and discussed, along with their corresponding *formulae*.

of time.

5. Metric Composition statistics (Middleware Layer): statistics on the availability of the composition service: queue length (momentarily count of outstanding composition requests); Thread count (count of threads serving composition requests); used memory (amount of heap memory reserved by the service); wait time (time from arrival to sending, averaged for all requests per interval); and response time (time from start of sending to receiving response, averaged for all requests per interval).
6. Profit per agent type (Middleware Layer): it stands for the profit that each agent type (namely, evil or malicious, disturbing, selfish and honest) can obtain according to its behaviour. The profit is higher if an agent cheats on another agent.
7. Uptime (Overlay Layer): this metric denotes the uninterrupted system availability.
8. Attack surface (Overlay Layer): used to count the number of data inputs to an overlay node.
9. Failed authentication (Overlay/Middleware Layer): used to count the number of data inputs to an overlay node.
10. Detection accuracy (Overlay Layer): Measure of the detection accuracy as the ratio of the number of undetected attacks to the total amount of detected attacks.
11. Total attack impact (Overlay Layer): quantifies the impact of the attack as the ratio of the number of nodes attacked to the total amount of nodes.

2.1 Design of the proposed Multi-metric Decision Making Approach

Once the overall set of metrics under consideration has been defined, a multi-metric decision making approach is applied to infer and trigger security actions rules based on the values of the metrics in a understandable fashion. Such expert system builds upon the following design steps:

A. Selection of Metrics: system operators will select specific security metrics according to the requirements and risk factors of the scenario at hand. In particular, the nSHIELD approach addresses more than 60 types of SPD metrics structured in 4 layers: node, network, middleware and overlay. System operators must decide which metrics refer better to their business operation: some might prioritize integrity to availability, whereas other could trade reliability for privacy, etc.

B. Normalization and Regression: Each of the metrics identified previously may feature different units and value range. This means that such values must be normalized in order to have a common value range domain and not to bias subsequent processing stages of the decision making engine. This is of utmost importance in order to define a common value range for their mutual comparison, and is indeed one of the purposes of the SPD metric triplet: to homogenize the representation of metrics in a threefold risk-valued domain. In other words, metrics quantify phenomena of very diverse nature, and therefore samples can be represented in different units (e.g. seconds, KW or Celsius) and within distinct numerical ranges (i.e. from discrete sets such as key par length – 64, 128, 256, 512 – to continuous-valued quantities such as time lapse in nanoseconds). For instance, if one assumes that the network latency takes on valid values from a positive region between 4 and 10 milliseconds, *correct* SPD values for this metric will be declared if all fall within this range. This axiom shall only be valid in a particular domain concerning a certain business process. If is hence between 4 and 10 milliseconds, the valid range for the network latency could be set to $[0, 10]$.

At this stage it must be pointed out that although time is an objective and measurable concept, the S level (Security Threat Level) is a subjective, experience-earned concept that the system operator in the nSHIELD approach must set up. The same conclusion holds for the P and D levels as they correspondingly relate to privacy and dependability. The S level represents the security threat level that will be bounded by its valid value range and its normal performance region. All these subjective SPD indicators must be determined by expert engineers and system operators who have the operational experience and who are in the position to shape universal security principles to the specific scenario under operation. Therefore, the decision making approach proposed in this work not only takes into account the experience of the operator, but also learns from past decisions in order to set up the best indicators for the considered metrics.

Table 1: Example of S level values for a temporal variable mapped by an expert.

Time	0	1	2	3	4	5	6	7
S level	0	2	4	6	8	11	14	17
Time	8	9	10	11	15	25		
S level	20	23	26	32	44	58		

Returning to the aforementioned example, the S level associated to the first time values $[0, 3]$ could be labeled as *unlikely to happen* under the criterion

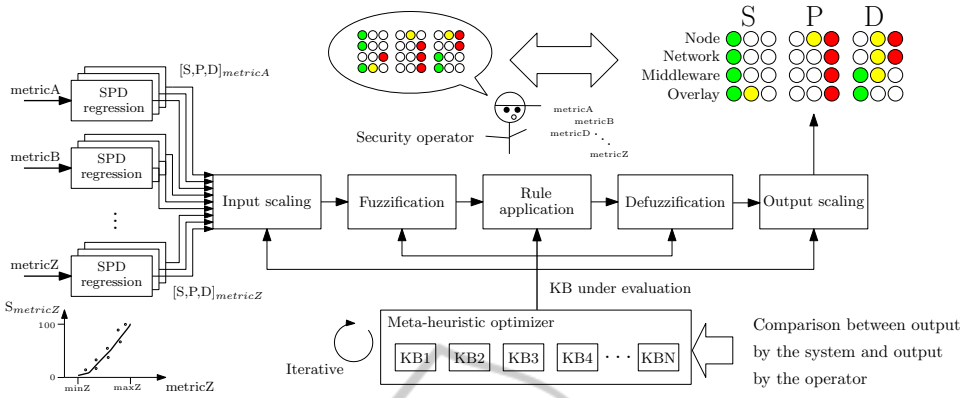

Figure 1: Overview of the proposed meta-heuristic fuzzy multi-metric aggregation scheme. The term KB (Knowledge Base) stands for any set of ruleset, scaling and membership functions within the population tuned by the meta-heuristic solver.

and experience of the system administrator. Correct values fall between $[4, 10]$, within where the threat level is kept linear to reflect that systems are able to handle this security context in an scalable fashion. However, the mapped level of security context is set to grow exponentially beyond 10 milliseconds and logarithmically above 15 miliseconds in order to represent a sharp increase of the severity of the security context. A similar methodology should be adopted for privacy and dependability concepts referring to each of the considered metrics.

The behavior of the SPD metrics with respect to any given value of the input metric can be analytically characterized in terms of the expected risk for each of such values. To this end, a function $f_\lambda^\alpha : x_\lambda \rightarrow r_\alpha$ can be inferred by regressing the values x_λ taken by metric λ to a risk value $r_\alpha \in [0, 100]$ for SPD metric $\alpha \in \{\mathrm{S}, \mathrm{P}, \mathrm{D}\}$. The analytical expression for this function f_λ^α can be obtained by performing a piecewise regression (not necessarily linear) over a set of metric-risk pairs input by the security manager of the system at hand. As a result of the overall processing step, one obtains a numerical triplet $[\mathrm{S}, \mathrm{P}, \mathrm{D}]$ for every security metric input to the system, which is then processed via a decision making engine to produce visual indicators of the level of SPD risk for every layer of the system based on the expertise of the manager for security operations.

C. Multi-metric Aggregation based on Expert Systems and Meta-heuristically Optimized Fuzzy Systems: The last step of the envisaged multi-metric security approach consists of an aggregation and decision making engine that processes the numerical values of the monitored security metrics (part of which are shown in the enumerated list of Section 2) towards providing a fuzzy representation of the risk level of the heterogeneous device ecosystem at hand. The aggregation system should 1) comprise a set of human understandable linguistic rules (in the form of IF-THEN-ELSE conditional statements) to ease their supervision and manual crafting; 2) automatically infer optimized rule sets based on a performance index that reflects the error between the produced decision and that provided by security experts; and 3) tailor the mapping between the numerical and linguistic domains corresponding to the SPD values of the considered metric with their fuzzy representation and processing through the rule set. These specifications are deemed of utmost importance in our attempt at avoiding black-box decision engines that provide no further benefit than the blind automation of the decisions to be made.

These specifications call for the adoption of a specific class of fuzzy systems that incorporates stochastic solvers to optimize the scaling factors and membership functions that specify the meaning of the numerical SPD inputs in the linguistic domain, as well as the collection of fuzzy rules that best matches the decisions taken by security experts (see Figure 1). Traditionally tackled via evolutionary algorithms (mostly, genetic optimizers (Cordon et al., 2004, 2001)), we plan to analyze and benchmark the performance – in the context of optimizing fuzzy rule-based systems – of more recent meta-heuristic solvers. In particular we will focus on Harmony Search (Geem et al., 2001), a population-based optimization algorithm that has been proven to outperform their genetic counterparts in a plethora of application fields such as engineering optimization, routing, resource allocation, economics and operations research (see (Manjarres et al., 2013) for a thorough survey). This algorithm resembles the way musicians in an orchestra improvise with their instruments before playing a piece of music in order to reach an aesthetically well-sounding harmony. This mimicking has implications in the def-

$$\mu(x) = \begin{cases} 0 & \text{if } S_{metricA} < a, \\ 2^{\lambda-1}\left(\frac{S_{metricA}-a}{b-a}\right)^{\lambda} & \text{if } a \leq S_{metricA} \leq (a+b)/2, \\ 1-2^{\lambda-1}\left(\frac{b-S_{metricA}}{b-a}\right)^{\lambda} & \text{if } (a+b)/2 < S_{metricA} < b, \\ 1-2^{\beta-1}\left(\frac{S_{metricA}-b}{c-b}\right)^{\beta} & \text{if } b \leq S_{metricA} < (b+c)/2, \\ 2^{\beta-1}\left(\frac{c-S_{metricA}}{c-b}\right)^{\beta} & \text{if } (b+c)/2 \leq S_{metricA} \leq c, \\ 0 & \text{if } S_{metricA} > c. \end{cases} \quad (1)$$

inition of the operators driving the search procedure of the algorithm, which ultimately leads to a better adaptability of the explorative and exploitative capabilities with respect to the problem to be optimized.

Back to the pursued aggregation system, the goal is to produce an intensity, colored, real-valued indicator of the level of risk for the S, P and D components at each of the considered layers (node, network, middleware, overlay), in the form of an output matrix. To this end, the expert would be first asked to provide, by means of e.g. questionnaires, their estimated output to a series of eventual metric values so as to lay decisional baseline information. This would permit to compare the output of the system under differently optimized fuzzy systems and extract therefrom a performance index (integer from the range [0-100], in %) quantifying the level of compliance of the optimized decision maker with the expected output by the security expert(s). This performance index would measure the fitness of every combination of rule set/membership function/scaling factor iteratively refined by the harmony search optimizer. In particular, parameterized membership functions and rules will be jointly optimized by means of a Pittsburg approach where the population of the algorithm is formed by separately encoded variable domains.

Once the fuzzy engine is optimized after a given number of iterations of the Harmony Search heuristic, the aggregation system is ready to receive outputs from the different security metrics and fuzzify them through the optimized scaling and membership functions $\mu(x)$, which could be parametrized to yield the generic function formulation in Expression (1) to be optimized by means of the aforementioned meta-heuristic solver, where $S_{metricA}$ denotes the S component of metric A (the same holds for the rest of SPD components and metrics), and $\{\lambda, \beta, a, b, c\}$ are the parameters to be optimized. It should be obvious that λ and β define the shape of right and left slopes of the membership function at hand, i.e. $\lambda = \beta = 1$ would correspond to the well-known triangular functions with center b and upper and lower extremes a and c, respectively.

Next the engine would apply the simultaneously optimized rule set and combine their outputs into a linguistically encoded output SPD matrix (by means of conventional methods for accumulating fuzzy outputs of individual rules, such as normalized and bounded sums), which is finally defuzzified (via e.g. the center of gravity method (Van Leekwijck & Kerre, 1999)) into colored intensity indicators so as to yield a more intuitive security assessing information of increased visual understandability. This 4×9 output matrix of integer entries between 0 (low intensity) and 10 (high intensity) facilitates a global perspective of the Security, Privacy and Dependability risk status at node, network, middleware and overlay layers. All in all, this visual information provides an holistic understanding of aggregated metrics in a SoS scenario.

3 CONCLUDING REMARKS

This manuscript has outlined the main design principles of a metric aggregation engine technically envisaged as a fuzzy expert system hybridized with a novel meta-heuristically optimized learning mechanism. The paper has gravitated, from a theoretical perspective, on the feasibility of measuring metrics in an heterogeneous complex systems environment. Mainly motivated by the lack of universal security guidelines for highly heterogeneous systems, the proposed aggregation approach regards system expert knowledge as an essential basis for security decision making. However, we foresee that this dependency could also be circumvented by a *learn-as-it-goes* approach, i.e. by supervising the SPD levels of successively held security incidences and feeding this information back to the decision making tool for its autonomous adjustment. Next steps will be oriented towards implementing and validating this procedure in diverse application scenarios.

REFERENCES

Yoshioka, N., Washizaki, H., Maruyama, K., 2008, *A Survey on Security Metrics*, Progress Informatics, N. 5, pp. 35-47.

Heyman, T., Yskout, K., Scandariato, R., Joosen, W., 2007, *Analysis of the Security Patterns Landscape*, International Workshop on Software Engineering for Secure Systems. Washington, DC, USA, p. 3.

VanHilst, M., Fernandez, E. B., 2007, Reverse Engineering to Detect Security Patterns in Code. Proceedings of the International Workshop on Software Patterns and Quality. Information Processing Society of Japan, pp. 25-30.

Fernandez, E. B., Yoshioka, N., Washizaki, H., 2007, *Using Security Patterns to Build Secure Systems*, Proceedings of the International Workshop on Software Patterns and Quality. Information Processing Society of Japan, pp. 47-48.

NSHIELD Artemis project, 2013, http://www.newshield.eu/.

Cavoukian, A., Dixon, M., 2013, *Privacy and Security by Design: An Enterprise Architecture Approach*, retrieved from http://www.ipc.on.ca.

Cordon, O., Gomide, F., Herrera, F., Hoffmann, F., Magdalena, L., 2004, *Genetic Fuzzy Systems: New Developments*, Fuzzy Sets and Systems, Vol. 141 (1), pp. 1-3.

Cordon, O., Herrera, F., Gomide, F., Hoffmann, F., Magdalena, L., 2001, *Ten Years of Genetic-Fuzzy Systems: A Current Framework and New Trends*, Proceedings of Joint 9th IFSA World Congress and 20th NAFIPS International Conference, pp. 1241-1246, Vancouver, Canada.

Geem, Z. W., Kim, J.-H., Loganathan, G. V., 2001, *A New Heuristic Optimization Algorithm: Harmony Search*, Simulation, Vol 76 (2), pp. 60-68 (2001)

Manjarres, D., Landa-Torres, I., Gil-Lopez, S., Del Ser, J., Bilbao, M. N., Salcedo-Sanz, S., Geem Z. W., 2013, *A Survey on Applications of the Harmony Search Algorithm*, Engineering Applications of Artificial Intelligence, Vol. 26 (8), pp. 1818-1831.

Van Leekwijck, W., Kerre, E. E., 1999, *Defuzzification: Criteria and Classification*, Fuzzy Sets and Systems, Vol. 108 (1999), pp. 159–178.