chist-era SUCCESS

D2.3: Final prototype

Grant Agreement:	N/A
Project Acronym:	SUCCESS
Project Name:	SecUre aCCESSibility for the internet of things
Instrument:	CHIST-ERA Call 2015
Thematic Priority:	SPTIoT
Start Date:	1 December 2016
Duration:	36 months
Document Type[1]:	T (Technical Report)
Document Distribution[2]:	CO (Confidential)
Document Code[3]:	SUCCESS-UGA-PR-001
Version:	v1.0
Editor (Partner):	M. Bozga (UGA)
Contributors:	M. Bozga, F. Kammüller, Ioana-Domnina Cristescu
Workpackage(s):	WP2
Reviewer(s):	F. Kammüller (MU)
Due Date:	Month 36
Submission Date:	Nov 2019
Number of Pages:	8

Funded by EPSRC Engineering and Physical Sciences Research Council, ANR, NWO Netherlands Organisation for Scientific Research

[1]MD = management document; TR = technical report; D = deliverable; P = published paper; CD = communication/dissemination.
[2]PU = Public; PP = Restricted to other programme participants (including the Commission Services); RE = Restricted to a group specified by the consortium (including the Commission Services); CO = Confidential, only for members of the consortium (including the Commission Services).
[3]This code is constructed as described in the H2020 Project Handbook.

D2.3: Final prototype

M. Bozga[1]

[1]UGA

REVISION HISTORY

Date	Version	Author	Modification
17.1.2020	1.0	F. Kammüller	Started the document
17.1.2020	1.1	M. Bozga	Draft outline and content for prototypes
27.1.2020	1.	F. Kammüller	Approval

APPROVALS

Role	Name	Partner	Date
Project Manager	F. Kammüller	MU	27.1.2020

Contents

1 Executive Summary

This is the description of the final prototype.

2 Prototypes

2.1 The IoT Modeling Language and BIP Transpiler

The IoT modeling language [2] is a formal language for specifying and enforcing security in IoT systems. The BIP "transpiler" transforms an IoT system description in the modeling language into a BIP model. The principles of the transformation / compilation to BIP are presented in [2]. The implementation of the BIP transpiler is open source and freely available at `http://iot-modeling.gforge.inria.fr/`.

2.2 Stochastic BIP Engine and Plasma-Lab connection

Plasma-Lab [3] is a modular statistical model checking (SMC) platform that facilitates multiple SMC algorithms, multiple modelling and query languages and has multiple modes of use. The connection between the Stochastic-BIP Engine and Plasma-Lab allows for running all Plasma-Lab SMC algorithms on top of stochastic BIP models. Its usage is documented at `http://iot-modeling.gforge.inria.fr/`.

2.3 Importance Splitting for *S*BIP

*S*BIP [4, 6] is a statistical model checker that enriches the existing BIP tool-set [1] with statistical analyses. *S*BIP has been recently redesigned to support richer stochastic models as well as richer logics for expressing properties. In addition, it supports various statistical analysis, ranging from classical hypothesis testing and probability estimation to parametric exploration and importance splitting for rare events. Some of these extensions (i.e., importance splitting) were specifically developed to support research activities and experimentation in the SUCCESS project.

The prototype implementation of the *importance splitting* algorithm relies on the piece-wise simulator to analyze rare properties. These properties specify requirements where some rare event eventually happens but with very low probability, and are often of the shape $\Diamond_{[0,t]}\phi$.

Importance splitting overcomes the problem of estimating the probability $P(S \models \Phi)$ of a system S to satisfy these properties. This is done by considering a set of intermediate levels l_i that correspond to less rare properties ϕ_i , such that, $\phi_n \Rightarrow \phi_{n-1} \Rightarrow \cdots \Rightarrow \phi_1$, where $\phi_n = \phi$. $P(S \models \phi)$ is therefore computed as the product of the conditional probabilities to reach l_i from l_{i-1} , i.e., $\prod_{i=1}^{n} P(S \models \phi_i \mid S \models \phi_{i-1})$. In our implementation, the intermediate levels l_i and associated ϕ_i are defined via a score function given as input. More precisely, each level l_i is identified by a state formula ϕ_i and f returns the highest index of state formula that a system state s satisfies, i.e., $f(s) = \max\{l_i \mid s \models \phi_i\}$.

The *S*BIP algorithm is similar to the analysis procedure proposed in Plasma-Lab[3]. It iterates over levels, and for each one, it simulates m trace prefixes among which m_s reach the next level and m_f do not. The conditional probability to reach the next level is thus estimated as the ratio m_s/m . In the next iteration, the simulation of successful prefixes is resumed, while the rest (m_f) are replaced by successful ones sampled uniformly. Note that our implementation of importance splitting is currently limited to the analysis of DTMCs. It is fully available as part of the *S*BIP implementation from ...

2.4 Quantitative Risk Assessment

Security assessment of organization's information systems is becoming increasingly complex due to their growing size and the underlying architectures (e.g.,cloud). Analyzing potential attacks is a pragmatic approach that provides insightful information to achieve this purpose. As part of our work in the SUCCESS project, we proposed to synthesize effective defense configurations for sophisticated attack strategies, which are obtained by minimizing resource usage while ensuring a high probability of success. Obtained results on real-life case studies show substantial improvement compared to existing techniques. The method is fully described in [5]. A prototype implementation is available open-source in the SUCCESS repository software `https://github.com/success-iot`.

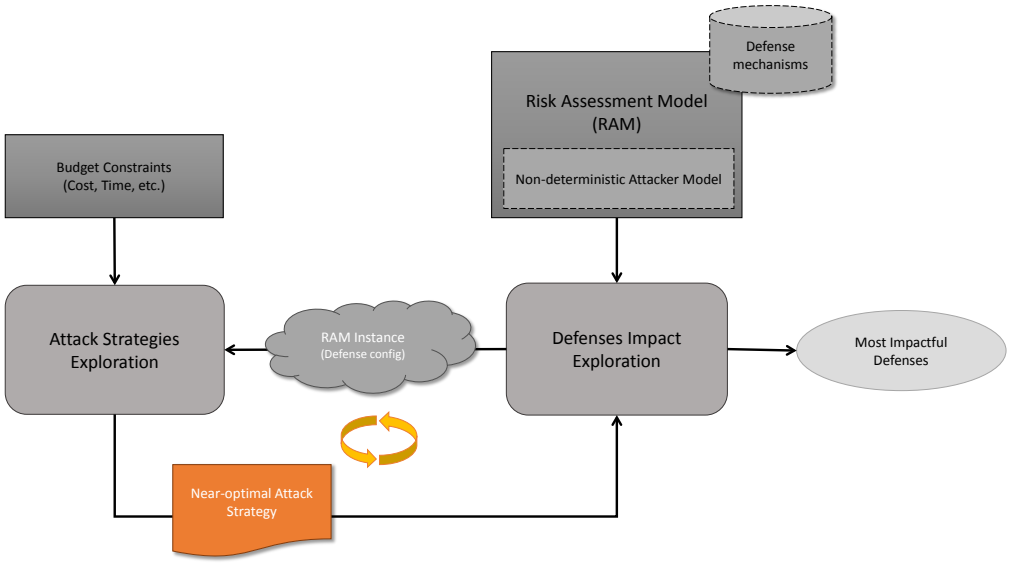

Figure 2.1: Quantitative Risk Assessment Methodology

The proposed risk assessment method is illustrated in Figure 2.1. We follow an offensive approach, that is, evaluating defenses by performing attacks on the system under study. In our heuristic, we focus on finding the adequate defenses against an optimized attack strategy characterized in terms of attack cost and success probability. These characteristics are computed using Statistical Model Checking techniques with respect to a near-optimal cost-effective attack strategy. This strategy is explored by a hybrid variant of a genetic algorithm and local search (IEGA), as opposed to alternative methods that rely on reinforcement learning. Genetic algorithms are evolutionary algorithms that have shown effectiveness in exploring large solution spaces to select high-quality answers for optimization and search problems. Moreover, several extensions allow to perform multi-objective explorations. For our method, the role of IEGA is to learn a strategy of attack that minimizes the attacker cost while maximizing its probability to succeed, given a deployed defense configuration.

3 Conclusion

Bibliography

[1] A. Basu, S. Bensalem, M. Bozga, J. Combaz, M. Jaber, T.-H. Nguyen, and J. Sifakis. Rigorous component-based system design using the bip framework. *IEEE Software*, 28(3), 2011.

[2] D. Beaulaton, N. B. Said, I. Cristescu, and S. Sadou. Security analysis of iot systems using attack trees. In M. Albanese, R. Horne, and C. W. Probst, editors, *Graphical Models for Security - 6th International Workshop, GraMSec@CSF 2019, Hoboken, NJ, USA, June 24, 2019, Revised Papers*, volume 11720 of *Lecture Notes in Computer Science*, pages 68–94. Springer, 2019.

[3] B. Boyer, K. Corre, A. Legay, and S. Sedwards. Plasma-lab: A flexible, distributable statistical model checking library. In K. Joshi, M. Siegle, M. Stoelinga, and P. R. D'Argenio, editors, *Quantitative Evaluation of Systems*, pages 160–164, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[4] B. L. Mediouni, A. Nouri, M. Bozga, M. Dellabani, A. Legay, and S. Bensalem. *S* BIP 2.0: Statistical model checking stochastic real-time systems. In S. K. Lahiri and C. Wang, editors, *Automated Technology for Verification and Analysis - 16th International Symposium, ATVA 2018, Los Angeles, CA, USA, October 7-10, 2018, Proceedings*, volume 11138 of *Lecture Notes in Computer Science*, pages 536–542. Springer, 2018.

[5] B. L. Mediouni, A. Nouri, M. Bozga, A. Legay, and S. Bensalem. Mitigating security risks through attack strategies exploration. In T. Margaria and B. Steffen, editors, *Leveraging Applications of Formal Methods, Verification and Validation. Verification*, pages 392–413, Cham, 2018. Springer International Publishing.

[6] A. Nouri, B. L. Mediouni, M. Bozga, J. Combaz, S. Bensalem, and A. Legay. Performance evaluation of stochastic real-time systems with the SBIP framework. *IJCCBS*, 8(3/4):340–370, 2018.