chist-era

SUCCESS

Design Principles

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):	S. Bensalem, A. Legay (UGA)
Contributors:	Stefano Schivo, Ioana-Domnina Cristescu
Workpackage(s):	WP2
Reviewer(s):	Florian Kammüller
Due Date:	Month 18
Submission Date:	??
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.

Copyright © 2018. All rights reserved.

Design Principles

Ioana-Domnina Cristescu[1]

[1]INRIA

REVISION HISTORY

Date	Version	Author	Modification
2.10.2018	1.0	F. Kammüller	Set up the delivery documentation
3.10.2018	1.1	I. Cristescu	Added summary of Security Enforcement Process [2]
23.10.2018	1.2	F. Kammüller	Minor editions
24.10.2018	1.3	F. Kammüller	Added section on ATTop, Edited Intro, Conclusion
02.11.2018	1.4	S. Schivo	Some changes to ATTop section
06.11.2018	1.4	I.-D. Cristescu	Minor corrections
7.11.2018	1.5	F. Kammüller	Final spell-check and approval

APPROVALS

Role	Name	Partner	Date
Project coordinator	F. Kammueller	MU	Approved

Contents

1 Executive Summary

The Design Principles lay out the SUCCESS process integrating high level specification of security properties, architecture, attack tree analysis, and BIP design.

The current document specifies these constituents of the SUCCESS process refering to the earlier technical deliverable Milestone M2.1 that provided a draft of the conceptual framework. A more detailed account on the SUCCESS process elaborating on the Design Principles is given in the deliverable Milestone 2.2.

2 Design Principles of the SUCCESS Process

2.1 Security Requirements Elicitation and High Level Architecture and Analysis

In the early requirements phases we use eFRIEND for requirements elicitation of ethical requirements [5]. We then map the non-functional requirements to functional (technical) requirements:

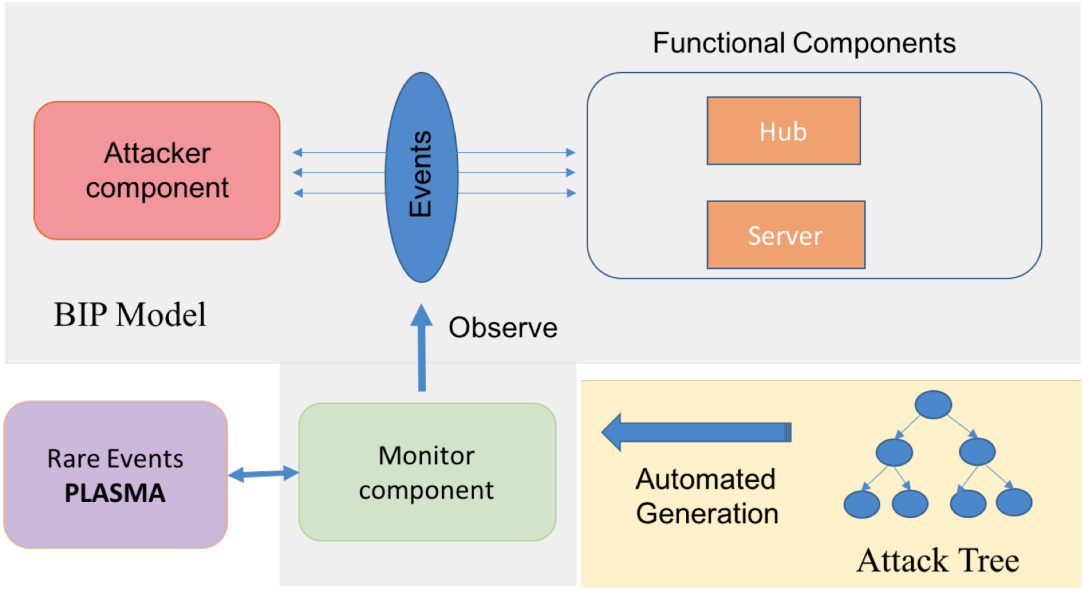
- Use Isabelle Infrastructure framework as detailed in M2.1 and [4, 3] to
  - Derive a formal specification of high level system infrastructure with actors and Security and Privacy policy from requirements specification;
  - Perform analysis of this formal specification by formal proof of security properties with special regard to GDPR mandatory privacy requirements using attack tree calculus.

The end result of this early process is a high level formal system architecture description and security and privacy policies with properties that can be formally proved in the interactive theorem prover Isabelle. The abstract system architecture needs to be mapped however systematically onto concrete IoT systems while still guaranteeing the preservation of corresponding security and privacy properties. This is provided in the next step of security enforcement with attack trees on BIP models and probabilistic rare event model checking.

2.2 Security enforcement in IoT systems using Attack Trees

Our approach for modeling security threats for IoT systems consists in explicitly representing the vulnerabilities of the system. A malicious entity, called the Attacker, tries to break a security property of the system by using different attack scenarios.

The Attacker interacts with the IoT system. In particular, the IoT entities can inadvertently help the Attacker by leaking sensitive data. We propose a formal language to model an IoT system and an Attacker. We also implemented a translator from our formal language to BIP. A user can write a formal description of the IoT system and the Attacker and obtain a BIP model containing the two. The BIP simulation engine can then execute the system. A first type of security analysis consists of detecting the executions for which the attack is successful [1].



Attack scenarios are modelled by *attack trees*. The user provides an attack tree in a json format for which we have implemented a tool that transforms it into a BIP monitor. The monitor observes the interactions between the Attacker and the rest of the system and can determine when an attack was successful but also how far the Attacker is from a successful attack. The monitor communicates his observations to Plasma, which is the SMC tool we use. The interaction between the BIP engine and Plasma requires a Plasma plugin, that we developed for this purpose.

Plasma implements SMC using either the Monte Carlo method or using rare events techniques. The latter are particularly interesting for our analysis, as successful attacks occur with a very small probability, and are thus *rare* events. Moreover, the importance splitting method is a rare event SMC technique that uses formalisms similar to attack trees to guide the analysis and it is therefore adapted for our approach [2].

2.3 Attack Trees (AT)

Attack Trees (AT) weave through the process of high level requirements elicitation, abstract system specification, and enforcement including probabilistic rare event attack analysis. Therefore the SUCCESS process needs to be accompanied by a highly flexible adaptable Attack Tree framework. This is provided by the ATTop tool [6] providing flexible support encompassing the uses of ATs in the other steps of the SUCCESS process and adding timed analysis via timed automata and UPPAAL.

ATTop is a *software bridging tool* that enables automated analysis of ATs using a model-driven engineering approach. Thanks to a common metamodel, ATTop facilitates interoperation between several AT analysis methodologies and resulting tools (e.g., ATE, ATCalc, ADTool 2.0). Moreover, it allows us to perform a comprehensive analysis of ATs by translating them into timed automata and analyzing them using the popular model checker UPPAAL. The analysis results are automatically translated back to the original ATs domain: this grants security practitioners access to advanced analysis techniques without the need to learn any new formalism.

3 Conclusion

In summary, this document defined the Principles of the SUCCESS approach using a range of formal methods but centred around Attack Trees (AT): (a) high-level analysis using the ethical eFRIENDS framework mapping onto a formal system specification in the Isabelle insider framework providing architecture level formal Security and Privacy proofs using a formal representation of AT. (b) AT represented in json are designed for BIP models (derived from a special formal IoT language) and are employed as a monitor in BIP. The system can be verified with statistical rare event model checking in Plasma. (c) The diverse uses of AT are supported by the flexible support tool ATTop adding timed analysis via timed automata and UPPAAL.

Bibliography

[1] D. Beaulaton, I. Cristescu, A. Legay, and J. Quilbeuf. A modeling language for security threats of iot systems. In F. Howar and J. Barnat, editors, *Formal Methods for Industrial Critical Systems*, pages 258–268, Cham, 2018. Springer International Publishing.

[2] D. Beaulaton, N. B. Said, I. Cristescu, A. Legay, and J. Quilbeuf. Security enforcement in iot systems using attack trees. work in progress.

[3] F. Kammüller. Attack trees in isabelle. In *20th International Conference on Information and Communications Security*, volume 11149 of *LNCS*. Springer, 2018.

[4] F. Kammüller. Formal modeling and analysis of data protection for gdpr compliance of iot healthcare systems. In *IEEE Systems, Man, and Cybernetics, IEEE SMC'18*. IEEE, 2018.

[5] F. Kammüller, J. C. Augusto, and S. Jones. Security and privacy requirements engineering for human centric iot systems using efriend and isabelle. In *IEEE/ACIS 15th International Conference on Software Engineering Research, Management and Application, SERA2017*, CPS. IEEE, 2017.

[6] R. Kumar, S. Schivo, E. Ruijters, B. M. Yildiz, D. Huistra, J. Brandt, A. Rensink, and M. Stoelinga. Effective analysis of attack trees: A model-driven approach. In A. Russo and A. Schürr, editors, *Fundamental Approaches to Software Engineering, 21st International Conference, FASE 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings.*, volume 10802 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2018.