AFRL-AFOSR-UK-TR-2022-0057

Advanced symbolic methods for the cryptographic protocol analyzer Maude-NPA

Escobar-Romain, Santiago
UNIVERSIDAD POLITECNICA DE VALENCIA
CAMINO VERA 14
VALENCIA, , 46020
ES

06/03/2022
Final Technical Report

Air Force Research Laboratory
Air Force Office of Scientific Research
European Office of Aerospace Research and Development
Unit 4515 Box 14, APO AE 09421

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
17-09-2020	final	Jul 2017 - Jun 2020;

4. TITLE AND SUBTITLE
Advanced symbolic methods for the cryptographic protocol analyzer Maude-NPA

5a. CONTRACT NUMBER
FA9550-17-1-0286

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Santiago Escobar

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
UNIVERSIDAD POLITECNICA DE VALENCIA.
CAMINO VERA, S/N VALENCIA 46020 SPAIN

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
USAF, AFRL DUNS 143574726
AF OFFICE OF SCIENTIFIC RESEARCH 875 NORTH RANDOLPH STREET, RM 3112
ARLINGTON VA 22203-1954

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Maude-NPA is a protocol analyzer developed by Catherine Meadows (Naval Research Laboratory, Washington DC, US), Jose Meseguer (University of Illinois at Urbana-Champaign, IL, US) and Santiago Escobar (Universitat Politècnica de València, Spain). It is a specialized model checker that relies on equational unification for the generation of the search state space. In this project, we have focused on (i) the equational unification capabilities of the Maude programming language, which are currently being used by Maude-NPA but also by the protocol analyzers Tamarin, developed at ETH Zurich, and AKISS, developed at INRIA France, (ii) integrating satisfiability technology (SMT solvers) into protocol analysis, and (iii) on analyzing new protocols using Maude-NPA, where we have analyzed protocols with time, protocols using bilinear pairing, and protocols using exclusive-or.

15. SUBJECT TERMS
protocol analysis, symbolic execution, model checking, cryptographic properties

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*

Advanced symbolic methods for the cryptographic protocol analyzer Maude-NPA
Grant No. FA9550-17-1-0286
Final Report July 2019 - June 2020

Santiago Escobar
Universitat Politècnica de València
Valencia, Spain

Contents

1 Summary

Maude-NPA is a protocol analyzer developed by Catherine Meadows (Naval Research Laboratory, Washington DC, US), Jose Meseguer (University of Illinois at Urbana-Champaign, IL, US) and Santiago Escobar (Universitat Politècnica de València, Spain). It is a specialized model checker that relies on equational unification for the generation of the search state space.

During this third year, we have obtained some publications on the unification capabilities of the Maude programming language and on new features for Maude-NPA. The Maude-NPA tool has been updated to version 3.1.4, although the manual is still in version 3.1.1, see `http://maude.cs.illinois.edu/tools/Maude-NPA`.

2 Introduction

Formal analysis of cryptographic protocols has become one of the most successful applications of formal methods to security. The idea is to verify protocols that use cryptography to guarantee security against an attacker —commonly called the Dolev-Yao attacker— who has complete control of the network, and can intercept, alter, and redirect traffic, create new traffic on his/her own, perform all operations available to legitimate participants, and may have access to some subset of the longterm keys of legitimate principals.

A number of protocol analysis tools are available nowadays: AKISS [7], ProVerif [8], Maude-NPA [12], Scyther [11], and Tamarin [5]. There has been a growing body of research in extending these tools to reason about different types of equational theories such as Abelian groups, exclusive-or, and Diffie-Hellmann.

Maude-NPA incorporates a hybrid equational unification framework by combining three approaches: (i) unification algorithms for common algebraic properties such as combinations of associativity, commutativity and identity, (ii) specialized unification algorithms for theories such as homomorphism or exclusive-or, and (iii) a generic variant-based unification algorithm for equational theories that satisfy the finite variant property such as exclusive-or, Abelian groups, or Diffie-Hellman. Maude-NPA is built on top of the Maude programming language [10] using its meta-programming capabilities. Maude is the one actually providing the unification approaches (i) and (iii) of Maude-NPA. Indeed, other protocol analysis tools such as Tamarin [9] from ETH Zurich, Switzerland, and AKISS [7] from INRIA, France, use Maude for similar purposes.

3 Methods, Assumptions and Procedures

The expected deliverables of this project include publications, new versions of the Maude programming language, and new versions of the Maude-NPA protocol analysis tool. The PI is part of the development teams of both Maude and Maude-NPA systems.

4 Results and Discussion

This project considers two main research lines for the Maude-NPA tool:

1. Extending the unification and satisfiability capabilities to express more cryptographic properties.

2. Integrating satisfiability modulo theories (SMT) capabilities to tackle new protocols and standards.

During this third year we focused on both research lines. First, we obtained the following publications on the unification and satisfiability capabilities of the Maude programming language.

1. We published a survey article on JLAMP [4] about the Maude programming language summarizing all the symbolic features added to Maude during the last ten years. A new version, 3.0, of the Maude programming language has been released during this third year, see `http://maude.cs.illinois.edu`. We envisage new tools and applications based on these novel features. There is no other programming language with such unification and narrowing infrastructure.

2. We published a paper at ICLP'20 [1] improving the variant-based unification algorithm implemented in Maude 3.0, which is not always able to provide a minimal set of most general unifiers. This paper improves upon the publication [6] of this project published the previous year.

Second, we have worked on improving the Maude-NPA crypto tool during this third year.

1. We published a paper at ESORICS'20 [2] providing a protocol transformation that allows complex protocols to be manageable by Maude-NPA and by many other crypto tools such as Tamarin. Our protocol transformation is able to safely get rid of many cryptographic properties under some conditions. The time and space difference between verifying the protocol with all the crypto properties and verifying the protocol with a minimal set of the crypto properties is remarkable. We also provide, for the first time, an encoding of the theory of bilinear pairing into Maude-NPA that goes beyond the encoding of bilinear pairing available in the Tamarin tool.

2. We published a paper at INDOCRYPT'20 [3] where we extend Maude-NPA with real-time and are able to analyze many time-specific properties of distance-bounding protocols, e.g., Mafia-fraud attacks (i.e., an attacker tries to convince the verifier that an honest prover is close to him whereas he is far away), and distance-hijacking-fraud attacks (i.e., a dishonest prover located far away succeeds in convincing a verifier that he is actually closer, and he may only exploit the presence of honest participants in the neighborhood to achieve his goal).

During this third year, only Damián Aparicio (PhD student) has been working on the project at full-time, apart of myself.

5 Conclusions

We have advanced in the two topics of this project: (i) improving the unification infrastructure in Maude and (ii) specifying and analyzing new protocols and standards in Maude-NPA.

6 Project Publications

[1] Damián Aparicio-Sánchez, Santiago Escobar and Julia Sapiña. Variant-based Equational Unification under Constructor Symbols. In *Technical Communications of the 36th International Conference on Logic Programming, ICLP 2020*, 2020. https://arxiv.org/abs/2009.11070

[2] Damián Aparicio-Sánchez, Santiago Escobar, Raúl Gutiérrez and Julia Sapiña. An Optimizing Protocol Transformation for Constructor Finite Variant Theories in Maude-NPA. In Proceedings, Part II, of the *25th European Symposium on Research in Computer Security*, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part II, volume 12309 of *Lecture Notes in Computer Science*, pages 230–250. Springer, 2020. https://doi.org/10.1007/978-3-030-59013-0_12

[3] Damián Aparicio-Sánchez, Santiago Escobar, Catherine Meadows, José Meseguer, and Julia Sapiña. Protocol Analysis with Time. In Proceedings of the *21st International Conference on Cryptology in India*, INDOCRYPT 2020. *Lecture Notes in Computer Science*, in press. Springer, 2020.

[4] Francisco Durán, Steven Eker, Santiago Escobar, Narciso Martí-Oliet, José Meseguer, Rubén Rubio and Carolyn L. Talcott. Programming and symbolic computation in Maude. *Journal of Logical and Algebraic Methods in Programming (JLAMP)*, volume 110, Elsevier 2020. https://doi.org/10.1016/j.jlamp.2019.100497.

7 References

[5] The Tamarin-Prover Manual (June 4, 2019). Available on: https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf

[6] Santiago Escobar and Julia Sapiña. Most general variant unifiers. In *Technical Communications of the 35th International Conference on Logic Programming, ICLP 2019*, 2019. https://doi.org/10.4204/EPTCS.306.21

[7] Baelde, D., Delaune, S., Gazeau, I., Kremer, S.: Symbolic verification of privacy-type properties for security protocols with XOR. In: 30th IEEE Computer Security Foundations Symposium, CSF 2017, pp. 234–248. IEEE Computer Society (2017).

[8] Bruno Blanchet. Automatic verification of security protocols in the symbolic model: The verifier proverif. In Alessandro Aldini, Javier Lopez, and Fabio Martinelli, editors, *Foundations of Security Analysis and Design VII - FOSAD 2012/2013 Tutorial Lectures*, volume 8604 of *Lecture Notes in Computer Science*, pages 54–87. Springer, 2013.

[9] Dreier, J., Duménil, C., Kremer, S., Sasse, R.: Beyond subterm-convergent equational theories in automated verification of stateful protocols. In Principles of Security and Trust, 2017. LNCS, vol. 10204, pp. 117–140. Springer (2017).

[10] Manuel Clavel, Francisco Durán, Steven Eker, Santiago Escobar, Patrick Lincoln, Narciso Martí-Oliet, José Meseguer, Rubén Rubio, and Carolyn Talcott. Maude 3.1 Manual. January 2020, `http://maude.cs.uiuc.edu`.

[11] Cas J. F. Cremers. The Scyther tool: Verification, falsification, and analysis of security protocols. In *CAV*, pages 414–418, 2008.

[12] S. Escobar, C. Meadows, and J. Meseguer. Maude-NPA (Version 3.1.1), 2019. Available at: `http://maude.cs.uiuc.edu/tools/Maude-NPA`.