AFRL-AFOSR-UK-TR-2020-0003

Increasing the Scope of Automated Protocol Analysis

Cas Cremers
THE UNIVERSITY OF OXFORD
UNIVERSITY OFFICES
OXFORD, OX1 2JD
GB

06/06/2020
Final Report

DISTRIBUTION A: Distribution approved for public release.

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

1. REPORT DATE *(DD-MM-YYYY)*
06-06-2020

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
15 Feb 2017 to 14 Jun 2018

4. TITLE AND SUBTITLE
Increasing the Scope of Automated Protocol Analysis

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-17-1-0206

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Cas Cremers

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
THE UNIVERSITY OF OXFORD
UNIVERSITY OFFICES
OXFORD, OX1 2JD GB

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
EOARD
Unit 4515
APO AE 09421-4515

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-UK-TR-2020-0003

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This project with Prof Cas Cremers (formally of Oxford and now with the Helmholtz Center for Information Security (CISPA) a German national Big Science Institution) was one of the most successful grants let during my predecessors assignment (2016-2018).

Prof Cremers research group gained notoriety in performing detailed security analysis of the TLS draft specification the Transport Layer Security protocol is the de facto means for securing communications across the Internet. Prof Cremers research group studied the draft TLS 1.3 specification for three years while it was open for public review and comment. In their research, the team developed a fine-grain, modular, and well-annotated symbolic model of TLS 1.3 (draft 21) using the Tamarin prover, proved a majority of the protocols security requirements, and uncovered a security weakness. This model was built with the explicit goal of transparency which increases the models longevity and allows it to be used as the security protocol is updated over time which is certain to happen. Within the grant period, Prof Cremers' group produced two top tier research papers and regularly briefed DVs as they came through the EOARD office and/or made visits to Oxford University. Lastly, it is important to note that this project was a very good example of basic research approaches, tools, and science being applied to a real world problem of considerable interest as the group modeled and analyzed all of the TLS 1.3 (draft 21) protocols handshake modes (a likely place for security breaches to occur). The annotated model is available on the web for download and use.

Due to the confluence of multiple events: the EOARD IPOs rotated, the PI changed universities, and the new IPO deployed the final financial paperwork was never received.

15. SUBJECT TERMS
Protocol, Analysis, Automated, Invariant, Security

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
Unclassified	Unclassified	Unclassified	SAR	

19a. NAME OF RESPONSIBLE PERSON
MAILLOUX, LOGAN

19b. TELEPHONE NUMBER *(Include area code)*
314 235 6163

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

APA-SCOPE: Increasing the Scope of Automated Protocol Analysis

Final summary report AFOSR Grant FA9550-17-1-0206

June 2020

Prof. Dr. C. Cremers

Objectives

History has shown that the complexity of many deployed security mechanisms makes it extremely hard for humans to assess their security, missing many possible venues of attack. One approach that has revealed many subtle attacks is the area of symbolic protocol analysis, which has been used for example to find attacks on several ISO/IEC security protocol standards [Basin2013].

The objective of the APA-Scope project was to i*ncrease the scope of state-of-the-art security protocol analysis tools*. This will enable the analysis of many safety-critical systems that are currently out of scope of fully automated analysis.

Methodology and main takeaways

For the project, we pursued two distinct but but ultimately related approaches:

(a) To investigate the effectiveness of *simplifying transformations* of protocols for improving scope, and
(b) To investigate the use of *human specified proof hints* (invariants, lemmas) with the ultimate aim of automating these in future developments, thereby increasing scope.

We report on each of these in turn.

Simplifying transformations

In earlier works, there had been attempts to develop so-called simplifying attack-preserving abstractions for security protocol analysis. The underlying idea is that the analysis of a given protocol P with respect to a property phi can be infeasible for current algorithms; however, some of the details of the system might be irrelevant. The scientific question then becomes: can we provide an algorithm A: Protocol → Protocol such that

(a) Given a system S, we can efficiently compute a related system A(P),
(b) A(P) is easier to analyse for protocol analysis tools than A, and

(c) A is attack-preserving, i.e., if there exists an attack on S, then there exists an attack on A(S).

If we have such an algorithm A, we can analyse A(P) instead of P directly. If our analysis yields that the security property holds on A(P) (because there is no attack), then from the above properties, we can infer there is no attack on the original P, and hence we know the security property holds for P.

Our investigations within the APA-Scope context revealed that the set of transformations that were attack-preserving were heavily dependent on the target security properties. Given a specific property, one can derive an algorithm A, but it is much more complex to do this generically for all possible security properties expressed in a language. This means that this approach is much harder for tools that support expressive property languages. We therefore focused first on the Scyther tool [Cremers], which is very efficient at analysing a small fixed set of security properties (secrecy and forms of authentication).

For this fixed set of properties, we managed to obtain highly effective simplifying and attack-preserving transformations. This made the tool much more efficient, and the analysis of more complex protocols has become feasible. We published this work at one of the top computer security journals:

- **Abstractions for security protocol verification**
  With Thanh Binh Nguyen and Christoph Sprenger.
  Journal of Computer Security, 2018.

Human invariants and moving towards automation

A second approach we considered is to study complex models and their human-generated invariants. In earlier analysis of early versions of TLS 1.3, we had used state-of-the-art tools such as the Tamarin prover. These tools allow human operators to specify hints to the tool in the form of invariants. To analyse the complete TLS 1.3, we needed many such hints and invariants.

Within this project, and contrary to our earlier attempts, we manually devised these invariants in a structured approach, analysing dependencies along the way. Ultimately, this enabled us to achieve two things:

(a) To provide a comprehensive analysis of the full TLS 1.3 protocol, and
(b) To obtain deeper insights into the classes of invariants for such models and their interdependencies.

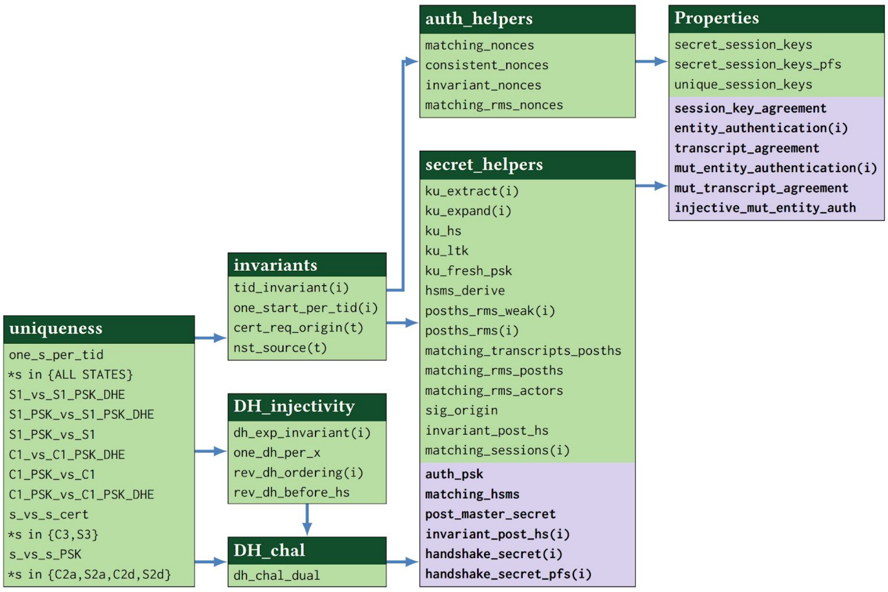

Figure 7: Lemma Map. Bold lemma names with a purple background indicate where manual interaction via the Tamarin visual interface was required. The remaining lemmas were automatically proven by Tamarin, without manual interaction. An arrow from one category to another implies that the proof of the latter depends on the former. The Properties box contains the main TLS 1.3 properties.

We show an image from the resulting paper above. In the box "properties" on the right, we list the properties of the system we set out to establish. The other boxes indicate manually constructed invariants, categorized by type. A green background indicates that the Tamarin prover could automatically prove the property, and a purple background indicates that some human guidance was needed for Tamarin to find the proof. This type of structural analysis has provided deep new insights into the type of invariants that are needed for the analysis of such complex protocols, and how they relate to each other. For example, while we can see that in the third column, authentication and secrecy invariants are distinct, all of them ultimately rely on uniqueness lemmas (related to the use of nonces), whereas for the TLS 1.3 model, the properties of the Diffie-Hellman (DH) exponentiations used in the derivation of the session keys, are only needed for the secrecy properties.

This work was documented in the following paper, which appeared at one of the top security conferences.

- **A Comprehensive Symbolic Analysis of TLS 1.3**
  With M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe.
  ACM CCS 2017: Proceedings of the 24th ACM Conference on Computer and Communications Security, Dallas, USA, 2017.

Overall, this work led to extremely promising results for further follow-up work, in which we aim to automate the generation of the invariants for such complex models. Now that we have analysed their structure and relations, we are in a position to identify those that we can likely need and generate.

Conclusions

We would like to thank AFOSR for their support in performing this research.

The directly visible outcome of the APA-Scope project is two top-tier security papers. However, the more important impact has been to yield new simplifying abstractions, and systematic construction of protocol invariants. These have already shown to increase the scope of our existing methods.

Perhaps more importantly, based on these results, we expect that further investigation into the automated generation of invariants will open up entirely new classes of protocols and systems for automated security analysis in the near future.