funding bodies

Innovate UK

EPSRC Investing in research for discovery and innovation

arm

Towards a Data Centric Approach for the Design and Verification of Cryptographic Protocols

Luca **Arnaboldi**, Roberto **Metere**

The 26th ACM Conference on Computer and Communications Security, London - United Kingdom
Proceedings of ACM CCS 2019 - DOI: 10.1145/3319535.3363262 - Poster session

The Alan Turing Institute

Newcastle University
School of Computing
research group
Secure and Resilient Systems

Abstract

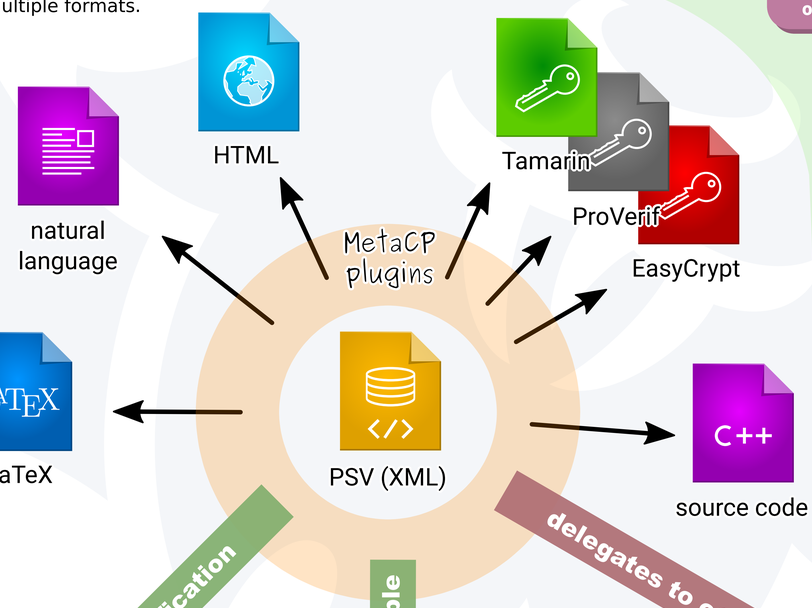
We propose MetaCP, a Meta Cryptographic Protocol verification tool, as an automated tool simplifying the design of security protocols through a graphical interface. The graphical interface can be seen as a modern editor of a non-relational database whose data are protocols.

The information of protocols is stored in XML, enjoying a fixed format and syntax aiming to contain all required information to specify any kind of protocol. This XML can be seen as an almost semanticless language, where different plugins confer strict semantics modelling the protocol into a variety of back-end verification languages.

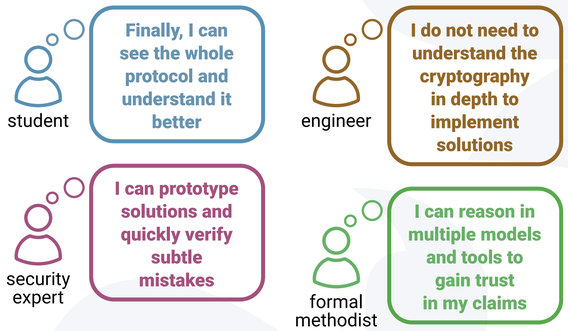
In the paper, we showcase the effectiveness of this novel approach by demonstrating how easy MetaCP makes it to design and verify a protocol going from the graphical design to formally verified protocol using a Tamarin prover plugin.

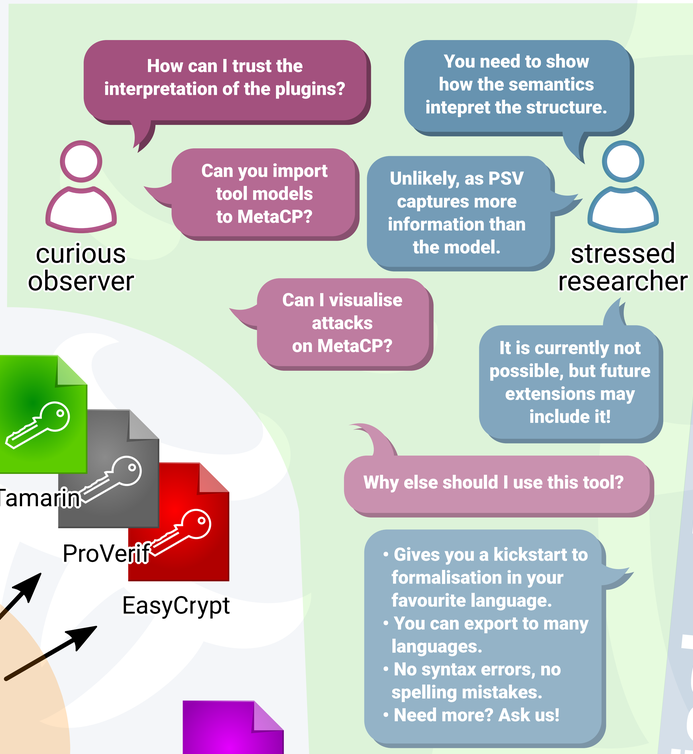
What is MetaCP?

- **Meta C**ryptographic **P**rotocol verification tool, enables the prototyping of security protocol from the design to the formal verification in minutes, and more!
- **P**rotocol **S**pecification and **V**erification (PSV).
- All information required to describe the protocol.
- Basic language with syntax and very little semantics.
- The plugins interpret the PSV and confer target language semantics.
- Many interpretations through the plugins to export to multiple formats.



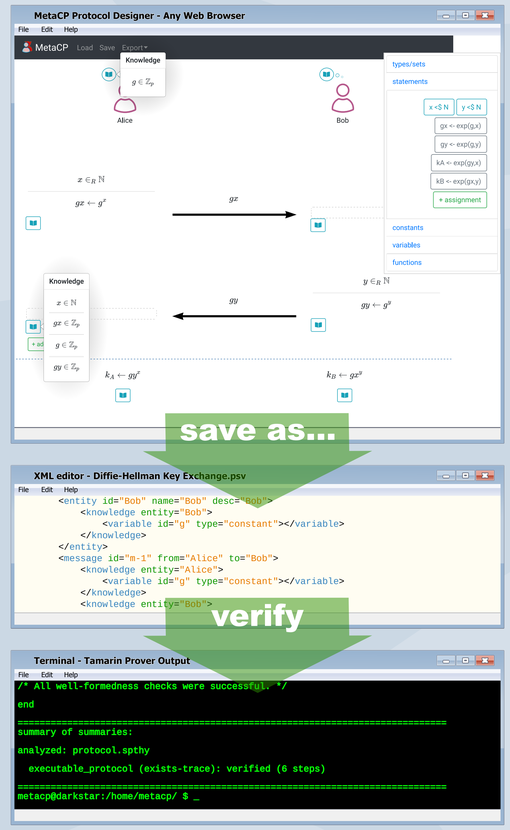
MetaCP Targets Diverse Audiences



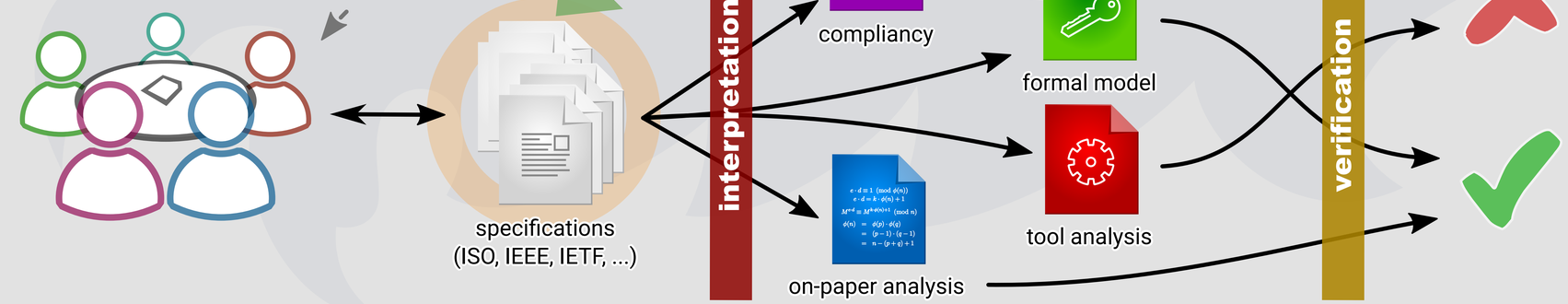


Diffie-Hellman Key Exchange in MetaCP

The following protocol allows two parties to exchange a secret key to enable secure communication.



1. The MetaCP **G**raphical **D**esign **E**ditor (GDE) aids the design of the protocol.
2. The protocol is then saved as a PSV file, which is a structured XML, validated against a DTD specification.
3. A plugin for Tamarin code interprets the PSV with Tamarin semantics: the result is coherent code.
4. The Tamarin prover is able to verify the code as expected.



https://doi.org/10.1145/3319535.3363262