Special topics in Security and Applied Logic Project List

Ioana Leuştean Bogdan Macovei

Rules

- Each student writes a report and delivers a 20-30 minutes presentation.
- The project is chosen by filling the form `https://tinyurl.com/stlsprojects2526`

A. Tools

You need to write a paper for this topic containing an introduction to the tool, how it handles the toy examples from the course plus some other suggestive examples.

Examples:

- CryptoVerif
  - `https://bblanche.gitlabpages.inria.fr/CryptoVerif/`
  - `https://bblanche.gitlabpages.inria.fr/publications/BlanchetOakland06.pdf`
- Verifpal
  - `https://verifpal.com/`
  - `https://eprint.iacr.org/2019/971.pdf`
- AVISPA
  - `http://www.avispa-project.org/`
  - `http://www.avispa-project.org/package/tutorial.pdf`
- FDR
  - `https://cocotec.io/fdr/index.html`
  - `https://www.cs.ox.ac.uk/people/gavin.lowe/Security/index.html`
- MaudeNPA
  - `http://maude.cs.illinois.edu/w/index.php/Maude_Tools:_Maude-NPA`
  - `https://www.researchgate.net/publication/221056944_Maude-NPA_Cryptographic_Protocol_Analysis_Modulo_Equational_Properties`
- Tools from:

  `https://bblanche.gitlabpages.inria.fr/proverif/proverif-users.html` (sectiunea Tools)

B. Formal Systems

For this project type, you have to read, understand and review a scientific paper or a book chapter. Your report should include necessary background knowledge. For important theoretical results you can present a sketch demonstration, without including all the technical details. For materials with associated tools or experiments, a practical example should pe presented.

Examples:

- Multi-protocol attacks, chapter in C.Cremers, S. Mauw, Operational Semantics and Verification of Security Protocols,Springer 2012 (Chapter 5 from `https://pure.tue.nl/ws/files/2425555/200612074.pdf`)
- Generalizing NSL for Multi-party Authentication, chapter in C.Cremers, S. Mauw, Operational Semantics and Verification of Security Protocols,Springer 2012 (Chapter 6 from https://pure.tue.nl/ws/files/2425555/200612074.pdf)
- J. Heather, G. Lowe, S. Schneider, How to Prevent Type Flow Attacks on Security Protocols, Proceedings 13th IEEE Computer Security Foundations Workshop. CSFW-13, 2000. `https://www.researchgate.net/publication/3857343_How_to_prevent_type_flaw_attacks_on_security_protocols`
- J. Herzog, A computational interpretation of Dolev-Yao adversaries, Theoretical Computer Science 340(1), 57-81, 2005. `https://www.sciencedirect.com/science/article/pii/S0304397505001179`
- H. Comon-Lundh, V. Cortier, E. Zalinescu, Deciding security properties for cryptographic protocols. Application to key cycles, ACM Transactions on Computational Logic, 1-89, 2018. `https://arxiv.org/pdf/0708.3564.pdf`
- K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, A Formal Security Analysis of the Signal Messaging Protocol, Journal of Cryptology, 2020 `https://eprint.iacr.org/2016/1013.pdf`
- D. Basin, C. Cremers, Know Your Enemy: Compromising Adversaries in Protocol Analysis, ACM Transactions on Information and System Security, 2014. https://people.cispa.io/cas.cremers/downloads/papers/compromise-tissec.pdf
- Research papers: `https://bblanche.gitlabpages.inria.fr/proverif/proverif-users.html`

  `https://tamarin-prover.com/publications.html`

  `https://people.cispa.io/cas.cremers/publications/index.html`

C. Real-World Security Protocols

For this topic, choose a formally analyzed *real-world* security protocol. The paper must include a presentation of the protocol, formalization and results obtained. It is desirable that the paper be accompanied by a practical experiment whose results are also included in the paper.

Examples of real-world formally analyzed security protocols:

- `https://people.cispa.io/cas.cremers/tools/protocols.html`
- `https://bblanche.gitlabpages.inria.fr/proverif/proverif-users.html`
- `https://tamarin-prover.com/`

D. Student Proposed Project

The student proposes a project, related to the topics presented in the course - students can choose the topic only after receiving the teacher's consent. The proposal, accompanied by bibliographic references, must be sent to ioana@fmi.unibuc.ro and bogdan.macovei@fmi.unibuc.ro.