

Workshop on Network Protocols

Olivier Levillain

September 17th 2024

Tour de table

Tour de table

ANSSI

- ▶ Clément Parssegny

Tour de table

ANSSI

- ▶ Clément Parssegny

KU Leuven

- ▶ H  lo  se Gollier

Tour de table

ANSSI

- ▶ Clément Parssegny

KU Leuven

- ▶ Héloïse Gollier

LORIA

- ▶ Tom Gouville
- ▶ Lucca Hirschi
- ▶ Steve Kremer
- ▶ Michael Mera

Tour de table

ANSSI

- ▶ Clément Parssegny

KU Leuven

- ▶ Héloïse Gollier

LORIA

- ▶ Tom Gouville
- ▶ Lucca Hirschi
- ▶ Steve Kremer
- ▶ Michael Mera

Radboud University

- ▶ Seyed Behnam Andarzian
- ▶ Cristian Daniele
- ▶ Patrick Lodeweegs
- ▶ Erik Poll

Tour de table

ANSSI

- ▶ Clément Parssegny

KU Leuven

- ▶ Héloïse Gollier

LORIA

- ▶ Tom Gouville
- ▶ Lucca Hirschi
- ▶ Steve Kremer
- ▶ Michael Mera

Radboud University

- ▶ Seyed Behnam Andarzian
- ▶ Cristian Daniele
- ▶ Patrick Lodeweegs
- ▶ Erik Poll

Télécom SudParis

- ▶ Adam Chader
- ▶ Olivier Levillain
- ▶ Mathieu Michel
- ▶ Yohan Pipereau
- ▶ Arthur Tran Van

Tour de table

ANSSI

- ▶ Clément Parssegny

KU Leuven

- ▶ Héloïse Gollier

LORIA

- ▶ Tom Gouville
- ▶ Lucca Hirschi
- ▶ Steve Kremer
- ▶ Michael Mera

Radboud University

- ▶ Seyed Behnam Andarzian
- ▶ Cristian Daniele
- ▶ Patrick Lodeweegs
- ▶ Erik Poll

Télécom SudParis

- ▶ Adam Chader
- ▶ Olivier Levillain
- ▶ Mathieu Michel
- ▶ Yohan Pipereau
- ▶ Arthur Tran Van

Uppsala University

- ▶ Paul Fiterau Brostean
- ▶ Fredrik Tåquist

Tour de table

ANSSI

- ▶ Clément Parssegny

KU Leuven

- ▶ Héloïse Gollier

LORIA

- ▶ Tom Gouville
- ▶ Lucca Hirschi
- ▶ Steve Kremer
- ▶ Michael Mera

Radboud University

- ▶ Seyed Behnam Andarzian
- ▶ Cristian Daniele
- ▶ Patrick Lodeweegs
- ▶ Erik Poll

Télécom SudParis

- ▶ Adam Chader
- ▶ Olivier Levillain
- ▶ Mathieu Michel
- ▶ Yohan Pipereau
- ▶ Arthur Tran Van

Uppsala University

- ▶ Paul Fiterau Brostean
- ▶ Fredrik Tåquist

Valeo

- ▶ Aina Toky Rasoamanana (Valeo)

Research Interests

GASP (a Generic Approach to Secure network Protocols)



Research directions

- ▶ automatically derive parsers and unparsers from a DSL
- ▶ automatically derive reference implementations from a DSL
- ▶ analyze existing protocol implementations using active learning

Studied Protocols

- ▶ TLS
- ▶ SSH
- ▶ OPC-UA

Selected Published Work

Parser Generators

[LangSec14] *Parsifal: A Pragmatic Solution to the Binary Parsing Problem*. OL. LangSec Workshop @ IEEE SSP 2014

[LangSec21] *Work-in-Progress: Towards a Platform to Compare Binary Parser Generators*. OL, S. Naud et A. T. Rasoamanana. LangSec Workshop @ IEEE SSP 2021

State Machine Inference and Analysis

[ESORICS23] *Towards a Systematic and Automatic Use of State Machine Inference to Uncover Security Flaws and Fingerprint TLS Stacks*. A. T. Rasoamanana, OL, H. Debar. ESORICS 2023

[ARES24] *Mealy Verifier: An Automated, Exhaustive, and Explainable Methodology for Analyzing State Machines in Protocol Implementations*. A. Tran Van, OL, H. Debar. ARES 2024

Subjects For Today... and Beyond?

- ▶ Active and Passive Learning
- ▶ Improving Inference using Grey Box Techniques
- ▶ Convergence Between Inference and (Stateful) Fuzzing
- ▶ Reasoning on State Machines to Find Bugs
- ▶ Automatic Derivation of Mapper / Stub Implementations

Agenda

9:45-10:15	Cristian Daniele (Radboud University) <i>LibAFL*: Fast and State-aware Protocol Fuzzing</i>
10:15-10:30	Erik Poll (Radboud University) <i>Work in Progress on Passive Learning</i>
10:30-11:15	Steve Kremer and Lucca Hirschi (LORIA) <i>DY Fuzzing</i>
11:15-11:45	Yohan Pipereau, Mathieu Michel and Olivier Levillain (TSP) <i>Speeding up equivalence methods with greybox inference (Ongoing work)</i>
14:00-14:45	Paul Fiterau Brostean and Fredrik Tåquist (Uppsala University) <i>Automata-Based Automated Detection of State Machine Bugs in Protocols</i>
14:45-15:30	Arthur Tran Van (Télécom SudParis) <i>Mealy Verifier</i>
16:00-17:30	Discussion and closing remarks

“Rules” and Logistics

The goal is primarily to discuss today!

- ▶ do not hesitate to ask questions and throw ideas!
- ▶ the time slots the agenda are just indications

“Rules” and Logistics

The goal is primarily to discuss today!

- ▶ do not hesitate to ask questions and throw ideas!
- ▶ the time slots the agenda are just indications

But we **must** be at lunch at 11:45!

Possible Next Steps

If all goes as planned today, we will want to meet again!

Possible Next Steps

If all goes as planned today, we will want to meet again!

A discussion for the end of the workshop about possible next steps

- ▶ a european edition of the LangSec workshop?
- ▶ maybe a more open workshop, as part of a european conference (ARES, ...ESORICS)?
- ▶ a Dagstuhl seminar?
- ▶ student exchanges

Possible Next Steps

If all goes as planned today, we will want to meet again!

A discussion for the end of the workshop about possible next steps

- ▶ a european edition of the LangSec workshop?
- ▶ maybe a more open workshop, as part of a european conference (ARES, ...ESORICS)?
- ▶ a Dagstuhl seminar?
- ▶ student exchanges

Let us keep that in mind, and dive into the science!

Questions ?

Merci de votre attention