Developing redistributable practical materials for Formal Methods in Security

Martin Lester, University of Reading

Lecturer in Computer Science, Admissions Tutor,
Open Research Champion

CyBOK showcase event, 2nd March 2022

Formal Methods in Security

CyBOK 1.1 includes a new Knowledge Area: **Formal Methods in Security**

- Some degrees have plenty of **Formal Methods**, but little **Security**.
  - They would benefit from some practical work with examples from **Security**.
- Some degrees have plenty of **Security**, but little **Formal Methods**.
  - They would benefit from some practical work with examples from Formal Methods.
- Some practitioners may want to study the area independently.

So I developed some practical exercises in this area...

Content

Each practical exercise comprises a series of tasks to be completed on computer, perhaps independently, or perhaps in a computer lab with supervision.

- **Practical 1**: A Known Plaintext Attack using CBMC and CryptoMiniSat
- **Practical 2**: An Information Flow Control Type System

Content produced for each:

- Long lab — software and manual
- Short lab — software and manual
- Slide deck

Known Plaintext Attack using CBMC...

Model checker **CBMC** uses a **SAT solver** to find assertion violations in C programs.

Idea: Assert that it is impossible for a known **plaintext** to encrypt to a known **ciphertext**.

Counterexample trace produced gives the encryption **key**.

Long lab: Recover key for weak Crypto1 cipher.

Short lab: Demonstrate how tiny error in implementation of a cipher can make it trivial to decrypt.

Both labs include an introduction to CBMC and basic usage.

Information Flow Control Type System

Noninterference: high inputs can't affect low outputs.

Noninterference can be enforced statically using an **information flow control type system**.

Slides: Type system for a simple imperative language.

Long lab: Prove correctness of the type system in Coq.

Short lab: Add the type system to an existing toy compiler.

Long lab presented as an extra chapter to Software Foundations.

Practicalities

- Released under Creative Commons licence.
- Solutions provided for all labs.
- Archived on Zenodo for long-term availability.
- Software versions and environment documented for easy setup.
- Manuals and slides written in Markdown — easy to edit and adapt.

Status

Drafts of all materials has been reviewed.

Final versions to be submitted next week for approval.

Thank you for listening