CLOUDFLARE

Introducing the Usable Formal Methods Research Group

CLOUDFLARE

Background

CLOUDFLARE

What are Formal Methods?

The use of mathematical techniques and formalisms to assist in the specification, design, analysis, and implementation of, in this case, protocols.

CLOUDFLARE

What are Formal Methods?

Can we bring mathematical rigour to our work with protocols?

CLOUDFLARE

An Abridged History of Formal Methods

- Developed out of work in the 50s, 60s, 70s on safety
- Applied to protocol analysis specifically in the late 70s
- Proof techniques were initially very limited
  - Couldn’t specify complex properties
  - Couldn’t specify complex protocols
  - Required heavy / unrealistic assumptions
  - Required huge amounts of manual work
- Tools and techniques improved over the years
- Eventually mature enough to become involved in the development and specification of TLS 1.3

Formal Analysis vs Formal Verification

Formal Analysis:

- Prove a protocol specification has a specific property
- “Design Correctness”

Formal Verification:

- Prove a protocol implementation i.e. a specific piece of code correctly implements a protocol specification
- “Implementation correctness”

The TLS 1.3 Design Process

- Involved academics in the design process from the beginning
- Yielded significant contributions (finding and fixing significant attacks in the protocol drafts) *before* the RFC was published
- This is where I first became involved in the IETF

CLOUDFLARE

Problem Solved?

Issues

- Proofs are very long
  - Automated TLS 1.3 proof ran to 750k lines and took several years to create
  - “By-hand” proofs can easily run to 40-50 pages of algebra
- Hard to produce
- Hard to understand
- Hard to verify
- Hard to adjust
- For academics: High risk - Low reward

CLOUDFLARE

Enter UFMRG(proposed)

CLOUDFLARE

How can we make Formal Methods *Usable*?

- Provide a place for experts to gather
- Accumulate a pool of knowledge
- Build a tower of training materials
- Provide feedback to tool designers
- Provide a venue to publish “negative” results
- Provide a place to store proofs and checkers

Non-goals

- Change IETF processes
  - We're an IRTF group
  - If we're successful people will *want* to use Formal Methods
  - We don't want to be an obstacle, we want to provide useful tools

CLOUDFLARE

Come join us!

Questions?