

# SSH formal verification

François Michel  
francois.michel@uclouvain.be

# A new SSH BoF is coming!

- Focuses mostly on clean-up and adding new cryptography algorithms
- A part of the charter will address formal verification
  - Verifying the whole protocol seems out of scope but the extension negotiation mechanism has flaws
  - The potential WG will react when new flaws are brought-up by formal verification



# Formal verification

There already exist *a few* Tamarin proofs for parts of the protocol






- Initial key exchange
- user-auth

tamarin-prover / examples / sapic / export / SSH / 



charlie-j Sapic fixes diverse (#540) 

0dfcf68 · last year  History

Name	Last commit message	Last commit date
 ..		
 WIP	do not run ssh unbounded example	3 years ago
 ssh-with-forwarding-bounded.spthy	Sapic fixes diverse (#540)	last year
 ssh-with-one-forwarding.spthy	Feature destructor option (#521)	last year
 ssh-without-forwarding.spthy	Feature destructor option (#521)	last year

# Formal verification

There already exist *a few* Tamarin proofs for parts of the protocol

- Initial key exchange
- user-auth

Is there an interest from people in starting new work for SSH verification ?

- Formal verification of the parts of the protocol
- Machine-executable verification for parts of existing implementations.