SSH formal verification

François Michel
francois.michel@uclouvain.be

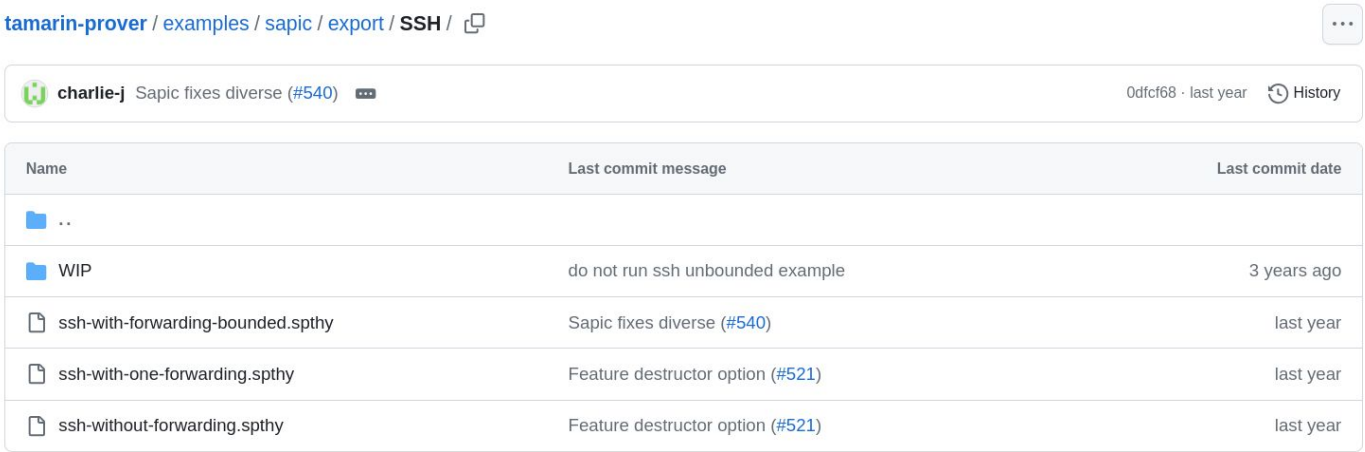
A new SSH BoF is coming!

- 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 negitiation 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



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.