



PIG - Protocol Implementation Generator



Jose Quaresma, Danmarks Tekniske Universitet

What is PIG?

PIG, or Protocol Implementation Generator, is a framework for sharing, verifying, translating and using secure protocols.

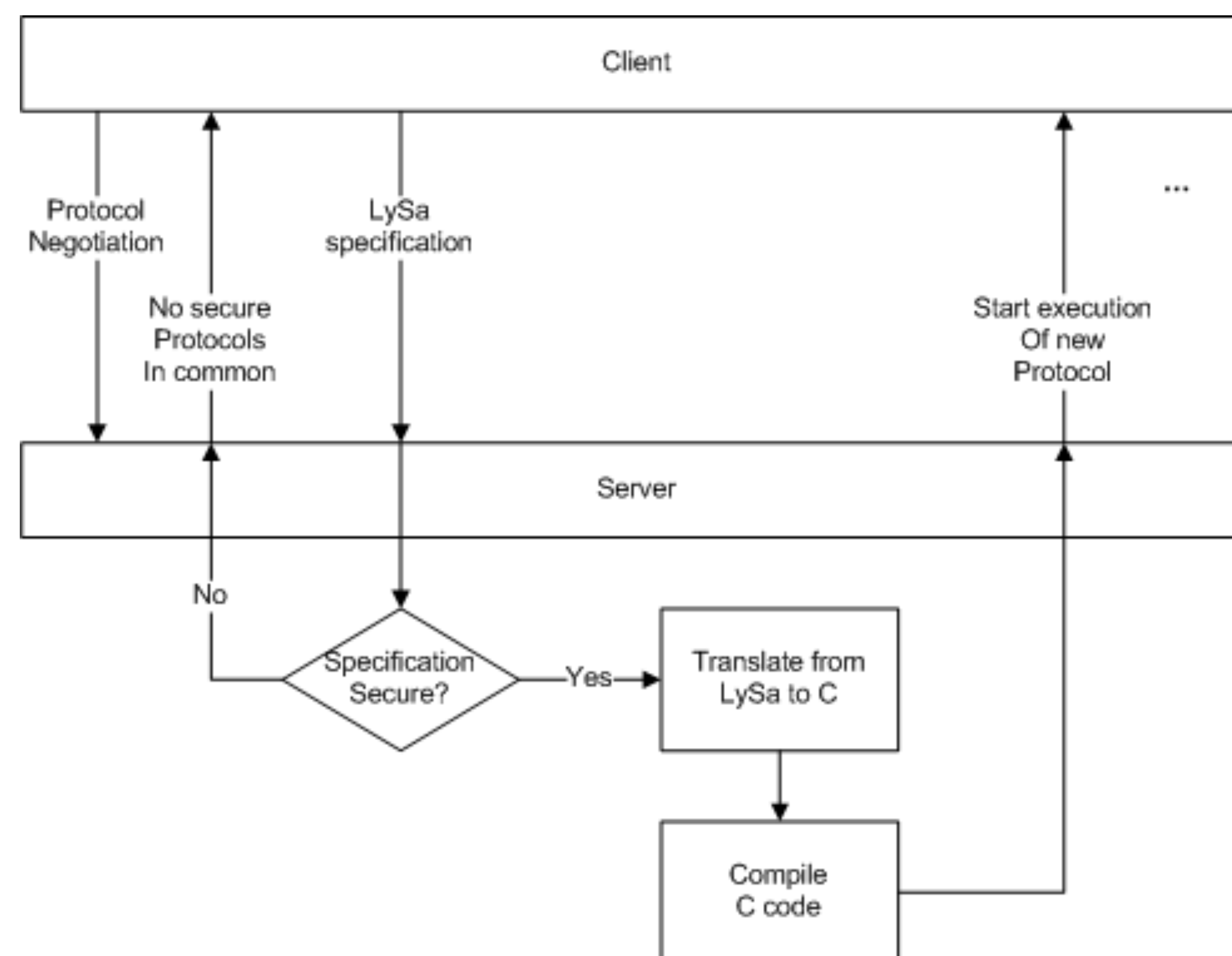
Status Quo

Presently, whenever two hosts try to establish a secure communication and the intersection of their known secure protocols is empty, it is not possible to establish a secure communication channel between them

How does PIG help?

This framework can be used in the above situation. When no shared protocols exist, one of the hosts (the Client) will send the other host (the Server) a high-level specification (LySa) of a chosen secure protocol to the second host. The latter will be able to verify the security properties of that protocol (using LySatool) and, if proven secure, it will compile it (to C) and execute it. Thus, a secure communication channel between the two hosts can be established.

PIG execution



LySa and LySatool

LySa is a process algebra for security protocols developed in collaboration between University of Pisa and Technical University of Denmark. It is based on the π -calculus, although it assumes one global communication medium to which all processes have access.

The LySatool is a Static Analysis automated tool for verifying security properties of protocols that use cryptography to protect network communication from tampering by malicious parties. Protocols modeled in the process calculus LySa are input to the tool. The LySatool makes a fully automated over-approximating program analysis that can guarantee confidentiality and authentication properties for the referred LySa processes.

PIG step by step:

- Encode the protocol in LySa
- Share the LySa Protocol Spec.
- Verify the Protocol Specification
- Translate that specification into C
- Compile the C code
- Run it

Turning the PIG around

In case there is the need to assure that the protocol implementation lives up to the protocol specification, it is possible to derive the specification from the implementation.

Proof-Carrying Protocols

Another alternative way to implement this framework would be to use it in a similar way to Proof-Carrying Code. The Client would send the security proof together with the specification. Then, the Server would only need to check the specification against the proof and if that is successful, the C code can be generated from the specification.