Imperial College London

3RD Year Computing

Interim Report

Implementation of a New Web Language

Author:
William de Renzy-Martin

Supervisor:
Sergio Maffeis

February 20, 2014

1 Introduction

The applied pi-calculus is an expressive formal language describing computations as communicating processes. Its primary use in both industry and academia is to model security protocols. These models being built, they can then be statically analysed either by hand, or automatically by using a tool such as ProVerif.

For the purposes of static analysis, models built using applied pi-calculus have proven very useful. However, they are limited by the fact that they cannot currently be executed, as there is no existing language implementation.

Without an implementation, any models built using the applied pi-calculus cannot be used to actually demonstrate protocols they are modelling, and those models can be very difficult to debug.

1.1 Objective

The aim of this project is to provide an implementation of the applied pi-calculus such that one might be able to build a model of a web protocol and then execute it interoperably with existing implementations written in PHP, Javascript or any other web language. The resulting implementation will hopefully not only be a very powerful and concise language for reasoning about and implementing protocols, but a useful scripting tool for the web.

At the very least, we would like to be able to write something similar to:

```
in(a,M);
out(b,M);
```

And have it execute successfully, receiving a message in on channel a, and sending the same message out again on channel b. However, ideally we would like to write something like the following:

```
let HttpServer () =
in ( net ,( b : Browser , o : Origin , m : bitstring ));
get serverIdentities (= originhost ( o ), pr , pk P , sk P , xdrp ) in
let ( k : symkey , httpReq ( u , hs , req )) = reqdec ( o , m , sk P ) in
if origin ( u ) = o then
    let corr = mkCorrelator ( k ) in
    out ( httpServerRequest ,( u , hs , req , corr ));
    in ( httpServerResponse ,(= u , resp : HttpResponse , cookieOut : CookieSet ,= corr
    out ( net ,( o , b , respenc ( o , httpResp ( resp , cookieOut , xdrp ), k ))).
```

1.2 Approach

[1]

References

[1] Martín Abadi and Cédric Fournet. Mobile values, new names, and secure communication. In *POPL'01: Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 104–115. ACM Press, 2001.