ArmoredSoftware Semantics 0.0

ArmoredSoftware Crew
Information and Telecommunication Technology Center
The University of Kansas
palexand@ku.edu

November 23, 2014

Contents

List of Figures

Abstract

This document describes evolving ArmoredSoftware semantic definitions.

1 Introduction

2 SPI Calculus

?

A Glossary

- $\mathbf{0}$ - null process
- $|M|$ - hash of M
- K^+ - public half of asymmetric key K
- K^- - private half of asymmetric key K
- $\{M\}_K$ - encrypt M with symmetric key K
- $\{M\}_{K^+}$ - encrypt M with the public key from K
- $\{M\}_{K^-}$ - decrypt M with the public key from K
- $\{|M|\}_{K^-}$ - sign M with the private key from K
- $\{|M|\}_{K^+}$ - check signature on M with the public key from K
- $(\nu x)P$ - new variable x defined in scope of P
- $\overline{c}\langle M\rangle$ - send M on channel c
- $c(M)$ - receive M on channel c
- $!P$ - infinite replication of P
- $P\ +\ Q$ - P or Q
- $P\ \mid\ Q$ - P in parallel with Q
- $\mathsf{case}\ \{M\}_k\ \mathsf{of}\ x\ \mathsf{in}\ P$ - attempt to decrypt $\{M\}_k$ and bind to x in P if successful. Stuck if unsuccessful
- $\mathsf{case}\ \{M\}_{k^-}\ \mathsf{of}\ x\ \mathsf{in}\ P$ - attempt to decrypt $\{M\}_{k^+}$ and bind to x in P if successful. Stuck if unsuccessful
- $\mathsf{case}\ \{|M|\}_{k^+}\ \mathsf{of}\ x\ \mathsf{in}\ P$ - attempt to check signature $\{|M|\}_{k^-}$ and bind to x in P if successful. Stuck if unsuccessful
- $\mathsf{case}\ x\ \mathsf{of}\ y\ 0 : P\ suc(x) : Q$ - case splitting over integers. x is bound in Q.
- $\mathsf{let}\ (x, y) = M\ \mathsf{in}\ y$ - match M to (x, y) binding x and y to pair elements in M
- $A \triangleq B$ - define an equivalence
- $A \rightarrow B : M\ \mathsf{on}\ c$ - A sends B message M on channel c

$$\begin{aligned} A &\triangleq (\nu c)\ \overline{c}\langle M\rangle.\mathbf{0}\ \mid \\ &\ c(M).A \end{aligned}$$