ArmoredSoftware Demo4

Spi Calculus Representation: Attempt 1

$$A(R) \triangleq (\nu N_{\mathrm{A}})\ \overline{C_{\mathrm{AB}}}\langle R\rangle.C_{\mathrm{AB}}(P).F(R,P)$$

$$\begin{aligned}
B \triangleq\ & (C_{\mathrm{BA}}(d, N_{\mathrm{A}}, PCR_{\mathrm{m}})\ \mid\ \overline{C_{\mathrm{BT}}}\langle m\_id\rangle.C_{\mathrm{BT}}(AIK^{+}, AIK_{\mathrm{h}})).\\
& \overline{C_{\mathrm{BC}}}\langle (B, AIK^{+})\rangle.C_{\mathrm{BC}}(K_{\mathrm{cipher}}, cert_{\mathrm{cipher}}).\\
& \overline{C_{\mathrm{BT}}}\langle act\_id(AIK_{\mathrm{h}}, K_{\mathrm{cipher}})\rangle.C_{\mathrm{BT}}(K).\\
& \mathsf{case}\ \{cert_{\mathrm{cipher}}\}_{K}\ \mathsf{of}\ cert\ \mathsf{in}\\
& \overline{C_{\mathrm{BM}}}\langle d\rangle.C_{\mathrm{BM}}(e).\\
& \overline{C_{\mathrm{BT}}}\langle tpm\_quote(AIK_{\mathrm{h}}, PCR_{\mathrm{m}}, |(e, N_{\mathrm{A}}, cert)|)\rangle.C_{\mathrm{BT}}(PCR_{\mathrm{c}}, qSig).\\
& \overline{C_{\mathrm{AB}}}\langle e, N_{\mathrm{A}}, cert, PCR_{\mathrm{c}}, qSig\rangle.B
\end{aligned}$$

$$\begin{aligned}
T \triangleq\ & (\nu AIK, AIK_{\mathrm{h}})\ C_{\mathrm{BT}}(x).\mathsf{case}\ x\ \mathsf{of}\ m\_id\ \mathsf{in}\\
& \overline{C_{\mathrm{BT}}}\langle AIK^{+}, AIK_{\mathrm{h}}\rangle.\\
& C_{\mathrm{BT}}(y).\mathsf{case}\ y\ \mathsf{of}\ act\_id(AIK_{\mathrm{h}}, K_{\mathrm{cipher}})\ \mathsf{in}\\
& \mathsf{case}\ \{K_{\mathrm{cipher}}\}_{EK^{-}}\ \mathsf{of}\ (K, aik_{\mathrm{hash}})\ \mathsf{in}\\
& [loaded(AIK_{\mathrm{h}})].[|pub(AIK_{\mathrm{h}})|\ is\ aik_{\mathrm{hash}}].\\
& \overline{C_{\mathrm{BT}}}\langle K\rangle.C_{\mathrm{BT}}(z).\\
& \mathsf{case}\ z\ \mathsf{of}\ tpm\_quote(AIK_{\mathrm{h}}, PCR_{\mathrm{m}}, exdata_{\mathrm{hash}})\ \mathsf{in}\\
& \overline{C_{\mathrm{BT}}}\langle (PCR_{\mathrm{c}}, sig((|PCR_{\mathrm{c}}|, exdata_{\mathrm{hash}}), AIK^{-})\rangle.T
\end{aligned}$$

$$\begin{aligned}
C \triangleq\ & (\nu K, CA)\ C_{\mathrm{BC}}(x, AIK^{+}).[lookup(x)].\mathsf{let}\ EK^{+} = end(x)\ \mathsf{in}\\
& \overline{C_{\mathrm{BC}}}\langle (\{K, |AIK|\}_{EK^{+}}, \{\{|AIK|\}_{CA^{-}}\}_{K})\rangle.C
\end{aligned}$$

$$M \triangleq C_{\mathrm{BM}}(d).\overline{C_{\mathrm{BM}}}\langle measure(d)\rangle.M$$

Key:

A:	Appraiser
B:	Attestation Agent
T:	TPM
C:	Certificate Authority
M:	Measurer
d :	desired evidence
e :	gathered evidence
R:	Request
P:	Response
F:	appraisal function that evaluates P based on R and A's internal standards
$\mathrm{N_A}$:	nonce generated by A
$\mathrm{PCR_m}$:	pcr mask indicating desired pcr registers
$\mathrm{PCR_c}$:	pcr composite structure containing select pcr register values
$\mathrm{AIK_h}$:	AIK key handle(used by TPM to reference loaded keys)
K:	Session key created by C
cipher :	as a subscript, this indicates encrypted text(as opposed to plaintext)
hash :	as a subscript, this indicates hashed text(like encrypted text, the plaintext contents cannot be discovered directly)
loaded(H) :	takes a key handle H as input, and is successful if H is loaded in the TPM
pub(H) :	takes a key handle H(of a loaded key) as input, and returns the associated Public Key
sig(data, key) :	signs (the hash of) data with key and returns the signature
lookup(ID) :	takes an identity(ID) as input, and is successful if the local id → EK table has an EK associated with ID
end(ID) :	takes an identity(ID) as input and returns the associated public EK

Note: In our current implementation, channels $\mathrm{C_{XY}}$ and $\mathrm{C_{YX}}$ are equivalent for any two parties X, Y.