Notes on Strand Spaces

— Verification of Security Protocols, Spring 2007 —

Christian Haack

April 24, 2007

1 Strand Spaces

Messages:

$T, A, B, N \in \mathsf{Text}$	(atomic text messages)
$K \in \mathsf{Key}$	(keys)
$m \in \mathsf{Msg} ::= T \mid (m, m) \mid \{m\}_K$	(messages)

For simplicity, we assume in these notes that we only have symmetric cryptography.

Strand Spaces:

A *Strand space* is a tuple (Σ, tr) where:

Σ is set	(the set of "strands")
tr is a function from Σ to $(\pm m)*$	(the "trace" mapping)

where $(\pm m)* \triangleq$ set of all sequences of signed messages.

Intuitive semantics of strands.

- Each strand corresponds to the view that an agent has of a complete protocol run.
- The trace of a strand is the sequence of send- and receive events that the agent sees.
- $+m$ represents a send-event ("$\mathsf{send}(m)$").
- $-m$ represents a receive-event ("$\mathsf{receive}(m)$").

Examples. Consider the following protocol:

$$\begin{array}{lcl} A \to B & : & A \\ B \to A & : & \{(A, T)\}_K \end{array}$$

(a) A single protocol run for fixed A, T, K in a trusted environment:

$$\begin{array}{rcl} \Sigma_0 & \triangleq & \{\mathsf{Init}, \mathsf{Resp}\} \\ tr_0(\mathsf{Init}) & \triangleq & \langle +A, -\{A,T\}_K \rangle \\ tr_0(\mathsf{Resp}) & \triangleq & \langle -A, +\{A,T\}_K \rangle \end{array}$$

(b) An arbitrary number of agents, each running both roles, arbitrary T and K, arbitrarily many parallel and consecutive runs for each agent, in a trusted environment:

$$\begin{array}{rcl} \Sigma_1 & \triangleq & \left\{ \begin{array}{l} \{\mathsf{Init}[A,B,T,K,i] \mid A,B,T \in \mathsf{Text}, K \in \mathsf{Key}, i \in I\!N\} \\ \cup\, \{\mathsf{Resp}[A,B,T,K,i] \mid A,B,T \in \mathsf{Text}, K \in \mathsf{Key}, i \in I\!N\} \end{array} \right. \\ tr_1(\mathsf{Init}[A,B,T,K,i]) & \triangleq & \langle +A, -\{A,T\}_K \rangle \\ tr_1(\mathsf{Resp}[A,B,T,K,i]) & \triangleq & \langle -A, +\{A,T\}_K \rangle \end{array}$$

(c) All this in the presence of eavesdroppers:

$$\begin{array}{rcl} \Sigma_2 & \triangleq & \Sigma_1 \ \cup\ \{\mathsf{Eaves}[m,i] \mid m \in \mathsf{Msg}, i \in I\!N\} \\ tr_2(s) & \triangleq & tr_1(s), \qquad \text{if } s \in \Sigma_1 \\ tr_2(\mathsf{Eaves}[m,i]) & \triangleq & \langle -m, +m \rangle \end{array}$$

2 Attacker Strands

M. Text message: $\langle +T \rangle$, if T in initial attacker knowledge

K. Public key: $\langle +K \rangle$, if K in initial attacker knowledge

F. Flushing: $\langle -m \rangle$

T. Tee: $\langle -m, +m, +m \rangle$

C. Concatenation: $\langle -m, -m', +(m,m') \rangle$

S. Separation: $\langle -(m,m'), +m, +m' \rangle$

E. Encryption: $\langle -K, -m, +\{m\}_K \rangle$

D. Decryption: $\langle -K, -\{m\}_K, +m \rangle$

3 Strand Spaces as Directed Graphs

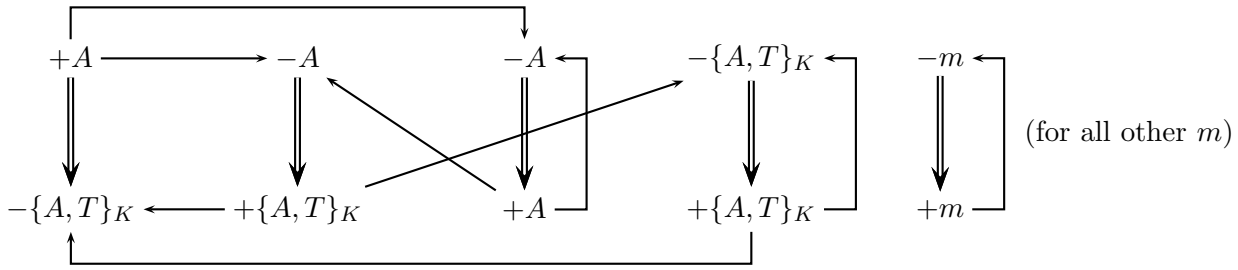
For any given strand space $\mathcal{S} = (\Sigma, tr)$, we define its associated directed graph $G_{\mathcal{S}} = (N_{\mathcal{S}}, \Rightarrow_{\mathcal{S}}, \rightarrow_{\mathcal{S}})$ with node set $N_{\mathcal{S}}$ and two kinds of edges $\Rightarrow_{\mathcal{S}}$ and $\rightarrow_{\mathcal{S}}$:

$$\begin{array}{rcl} N_{\mathcal{S}} & \triangleq & \{(s,i) \mid s \in \Sigma,\ 1 \le i \le \mathsf{length}(tr(s))\} \\ \Rightarrow_{\mathcal{S}} & \triangleq & \{((s,i),(s,i+1)) \mid s \in \Sigma,\ 1 \le i < \mathsf{length}(tr(s))\} \\ \rightarrow_{\mathcal{S}} & \triangleq & \{((s,i),(t,j)) \mid (\exists m)(tr(s)_i = +m \ \wedge\ tr(t)_j = -m)\} \end{array}$$

Example. Consider the following strand space $\mathcal{S} = (\Sigma, tr)$:

$$\begin{array}{rcl} \Sigma & \triangleq & \{\mathsf{Init}, \mathsf{Resp}\} \cup \{\mathsf{Eaves}[m] \mid m \in \mathsf{Msg}\} \\ tr(\mathsf{Init}) & \triangleq & \langle +A, -\{A,T\}_K \rangle \\ tr(\mathsf{Resp}) & \triangleq & \langle -A, +\{A,T\}_K \rangle \\ tr(\mathsf{Eaves}[m]) & \triangleq & \langle -m, +m \rangle \end{array}$$

Here is a picture of its associated directed graph $G_{\mathcal{S}}$:



4 Bundles

Bundles are finite subgraphs of strand spaces and represent finite, partial protocol executions. Not every finite subgraph of a strand space can sensibly be interpreted as a partial protocol execution. Conditions **(B1)**–**(B5)** axiomatize those subgraphs that can.

For $\mathcal{S} = (\Sigma, tr)$ and $(s, i) \in N_{\mathcal{S}}$, we define:

$$\begin{array}{rcll} \mathsf{sign}_{\mathcal{S}}(s,i) & \triangleq & +, & \text{if } tr(s)_i = +m \text{ for some } m \\ \mathsf{sign}_{\mathcal{S}}(s,i) & \triangleq & -, & \text{if } tr(s)_i = -m \text{ for some } m \end{array}$$

Definition 1 (Bundles) *Given a strand space $\mathcal{S}$ with $G_{\mathcal{S}} = (N_{\mathcal{S}}, \Rightarrow_{\mathcal{S}}, \rightarrow_{\mathcal{S}})$. A bundle of $\mathcal{S}$ is a graph $\mathcal{B} = (N_{\mathcal{B}}, \Rightarrow_{\mathcal{B}}, \rightarrow_{\mathcal{B}})$ such that the following conditions hold:*

(B1) *$\mathcal{B}$ is a subgraph of $\mathcal{S}$ (i.e., $\Rightarrow_{\mathcal{B}} \subseteq \Rightarrow_{\mathcal{S}}$ and $\rightarrow_{\mathcal{B}} \subseteq \rightarrow_{\mathcal{S}}$).*

(B2) *$\mathcal{B}$ is finite (i.e., $N_{\mathcal{B}}$, $\Rightarrow_{\mathcal{B}}$ and $\rightarrow_{\mathcal{B}}$ are finite sets).*

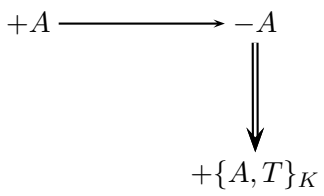
(B3) *$\mathcal{B}$ is acyclic.*

(B4) *If $n_2 \in N_{\mathcal{B}}$ and $n_1 \Rightarrow_{\mathcal{S}} n_2$, then $n_1 \Rightarrow_{\mathcal{B}} n_2$.*

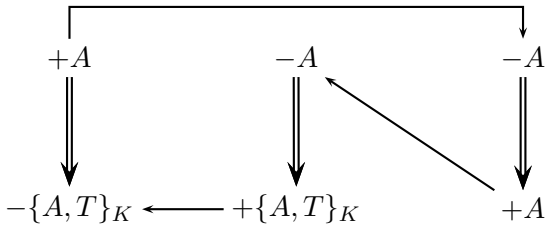
(B5) *If $n_2 \in N_{\mathcal{B}}$ and $\mathsf{sign}_{\mathcal{S}}(n_2) = -$, then there exists a unique n_1 such that $n_1 \rightarrow_{\mathcal{B}} n_2$.*

Examples.

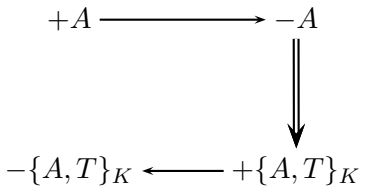
(a) The following graph is a bundle of the strand space $\mathcal{S}$ from Section 3:



(b) The following graph, too, is a bundle of the strand space $\mathcal{S}$ from Section 3:

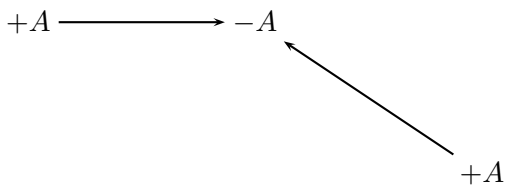


(c) The following graph is not a bundle of the strand space $\mathcal{S}$ from Section 3, because it violates the bundle axiom **(B4)**:

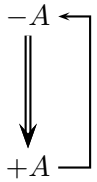


(d) The following graph is not a bundle of any strand space, because it violates the bundle axiom **(B5)**:

(e) The following graph is not a bundle of any strand space, because it violates the bundle axiom **(B5)**:



(f) The following graph is not a bundle of any strand space, because it violates the bundle axiom **(B3)**:



5 Non-injective Agreement

$$\begin{array}{rcl} \mathsf{bundle}(\mathcal{S}) & \triangleq & \text{set of all bundles of } \mathcal{S} \\ s \in_i \mathcal{B} & \triangleq & \{(s,i) \mid 1 \leq j \leq i\} \subseteq N_{\mathcal{B}} \\ s \in \mathcal{B} & \triangleq & s \in_{\mathsf{length}(tr(s))} \mathcal{B} \end{array}$$

Protocol roles are typically modeled as parameterized strands and non-injective agreement is specified by formulas of the following form:

$$(\forall \mathcal{B} \in \mathsf{bundle}(\mathcal{S}))(\forall \vec{T})(P[\vec{T}] \in_i \mathcal{B} \Longrightarrow Q[\vec{T}] \in_j \mathcal{B})$$

Intuitively, this is similar to inserting $\mathsf{end}(\vec{T})$ after the ith event of $P[\vec{T}]$ and $\mathsf{begin}(\vec{T})$ before the jth event of $Q[\vec{T}]$.

Example 1 *Let $\mathcal{S}$ be the strand space from Section 3. Then the following formula holds:*

$$(\forall \mathcal{B} \in \mathsf{bundle}(\mathcal{S}))(\mathsf{Init} \in \mathcal{B} \Longrightarrow \mathsf{Resp} \in \mathcal{B})$$

Proof. Let $\mathcal{B} \in \mathsf{bundle}(\mathcal{S})$. Suppose $\mathsf{Init} \in \mathcal{B}$. Because $\mathsf{sign}_{\mathcal{S}}(\mathsf{Init}, 2) = -$, we know by axiom **(B5)** that either $(\mathsf{Resp}, 2) \rightarrow_{\mathcal{B}} (\mathsf{Init}, 2)$ or $(\mathsf{Eaves}[\{A, T\}_K], 2) \rightarrow_{\mathcal{B}} (\mathsf{Init}, 2)$.

Case, $(\mathsf{Resp}, 2) \rightarrow_{\mathcal{B}} (\mathsf{Init}, 2)$: In this case, $(\mathsf{Resp}, 1) \Rightarrow_{\mathcal{B}} (\mathsf{Resp}, 2)$, by axiom **(B4)**. Then $\{(\mathsf{Resp}, 1), (\mathsf{Resp}, 2)\} \subseteq N_{\mathcal{B}}$. That means that $\mathsf{Resp} \in \mathcal{B}$.

Case, $(\mathsf{Eaves}[\{A, T\}_K], 2) \rightarrow_{\mathcal{B}} (\mathsf{Init}, 2)$: In this case, $(\mathsf{Eaves}[\{A, T\}_K], 1) \Rightarrow_B (\mathsf{Eaves}[\{A, T\}_K], 2)$, by axiom **(B4)**. Then $(\mathsf{Eaves}[\{A, T\}_K], 2) \rightarrow_{\mathcal{B}} (\mathsf{Eaves}[\{A, T\}_K], 1)$ or $(\mathsf{Resp}, 2) \rightarrow_{\mathcal{B}} (\mathsf{Eaves}[\{A, T\}_K], 1)$. The former is impossible, by axiom **(B3)**. In the latter case, we have $(\mathsf{Resp}, 1) \Rightarrow_{\mathcal{B}} (\mathsf{Resp}, 2)$, by axiom **(B4)**. Then $\{(\mathsf{Resp}, 1), (\mathsf{Resp}, 2)\} \subseteq N_{\mathcal{B}}$. That means that $\mathsf{Resp} \in \mathcal{B}$. □

The strand space from Section 3 is not a realistic protocol model, because each trace has only one incarnation as a strand. In particular, this means that the eavesdropper can only see each message once! This is clearly unrealistic. If we model eavesdroppers more realistically, then the proof from Example 1 gets a little more complicated. This has to do with the fact that there is no more bound on the size of bundles that contain Init.

The following simple gadget helps to cleanly deal with such complications.

Definition 2 (The Causal Precedence Order) *For any bundle $\mathcal{B}$, we define $\preceq_{\mathcal{B}}$ as the reflexive, transitive closure of $\Rightarrow_{\mathcal{B}} \cup \rightarrow_{\mathcal{B}}$. (That is, $n \preceq_{\mathcal{B}} n'$ iff it is possible to get from n to n' by following zero or more $\Rightarrow_{\mathcal{B}}$- or $\rightarrow_{\mathcal{B}}$-edges.)*

The following simple observation is an immediate consequence of the fact that bundles are finite and acyclic.

> *If $\mathcal{B}$ is a bundle and N' is a non-empty subset of $N_{\mathcal{B}}$, then N' has a minimal element with respect to $\preceq_{\mathcal{B}}$. (That is, $(\exists n' \in N')(\forall n'' \in N')(n'' \preceq_{\mathcal{B}} n' \Longrightarrow n'' = n').$)*[1]

This simple observation is used in most manual authenticity proofs that are based on the strand space model.

Example 2 *Suppose that* $\mathsf{Name} \subseteq \mathsf{Text}$, $\mathsf{SharedKey} \subseteq \mathsf{Key}$ *and that there is a map* k *from* $\mathsf{Name} \times \mathsf{Name}$ *to* $\mathsf{SharedKey}$ *such that* $\mathsf{k}(A,B) = \mathsf{k}(A',B')$ *only if* $\{A,B\} = \{A',B'\}$. *Suppose, furthermore, that $\mathcal{A}$ is some set of strands. We define:*

$$\begin{array}{rcl}
\Sigma & \triangleq & \{\mathsf{Init}[A,B,T,i] \mid A,B \in \mathsf{Name}, T \in \mathsf{Text}, i \in I\!N\} \\
 & & \cup\ \{\mathsf{Resp}[A,B,T,i] \mid A,B \in \mathsf{Name}, T \in \mathsf{Text}, i \in I\!N\} \\
tr(\mathsf{Init}[A,B,T,i]) & \triangleq & \langle +(B,A), -(A,\{B,T\}_{\mathsf{k}(A,B)})\rangle \\
tr(\mathsf{Resp}[A,B,T,i]) & \triangleq & \langle -(B,A), +(A,\{B,T\}_{\mathsf{k}(A,B)})\rangle \\
tr(s) & \in & \{\langle -m, +m\rangle \mid m \in \mathsf{Msg}\}, \quad \textit{for all } s \in \mathcal{A}
\end{array}$$

Let $\mathcal{S} = (\Sigma \cup \mathcal{A}, tr)$. Then the following formula holds:

$$\begin{array}{l}
(\forall \mathcal{B} \in \mathsf{bundle}(\mathcal{S}), A, B \in \mathsf{Name}, T \in \mathsf{Text}, i \in I\!N) \\
\quad (\mathsf{Init}[A,B,T,i] \in \mathcal{B} \Longrightarrow (\exists i')(\mathsf{Resp}[A,B,T,i'] \in \mathcal{B}))
\end{array}$$

Proof. Let $\mathcal{B} \in \mathsf{bundle}(\mathcal{S})$, $A, B \in \mathsf{Name}$, $T \in \mathsf{Text}$ and $i \in I\!N$. Suppose $\mathsf{Init}[A,B,T,i] \in \mathcal{B}$. We define the following set of nodes:

$$N' \triangleq \{(s,j) \in N_{\mathcal{B}} \mid (s,j) \preceq_B (\mathsf{Init}[A,B,T,i],2) \ \wedge\ tr(s)_j \in \pm(A,\{B,T\}_{\mathsf{k}(A,B)})\ \}$$

Clearly, $(\mathsf{Init}[A,B,T,i],2) \in N'$. Thus, N' is non-empty. Therefore, N' has a $\preceq_{\mathcal{B}}$-minimal element. Let's call this element $n_0 = (s_0, i_0)$. There are three possible cases: either $s_0 \in \mathcal{A}$, or s_0 is an initiator strand, or s_0 is a responder strand.

[1] Note that a minimal element does not need to be unique.

Case, $s_0 \in \mathcal{A}$: Then $tr(s_0) = \langle -(A, \{B, T\}_{\mathsf{k}(A,B)}), +(A, \{B, T\}_{\mathsf{k}(A,B)})\rangle$. Because $(s_0, 1) \in N'$ and $(s_0, 1) \prec_{\mathcal{B}} (s_0, 2)$, i_0 cannot be 2, by minimality of (s_0, i_0). But i_0 cannot by 1 either, because there exists a node n' in N' such that $n' \prec_B (s_0, 1)$, by bundle axiom **(B5)**. So this case is impossible.

Case, $s_0 = \mathsf{Init}[A', B', T', i']$ *for some* A', B', T', i': This is only possible if $i_0 = 2$, because nodes that are labeled with messages of the form $+(B', A')$ are not in N', by definition of N'. But $(\mathsf{Init}[A', B', T', i'], 2)$ is a negative node and, thus, cannot be minimal in N', by **(B5)**. So this case is impossible.

Case, $s_0 \in \mathsf{Resp}[A', B', T', i']$ *for some* A', B', T', i': This is only possible if $i_0 = 2$, because nodes that are labeled with messages of the form $-(B', A')$ are not in N', by definition of N'. Moreover, $(\mathsf{Resp}[A', B', T', i'], 2)$ can only be in N', if $+(A', \{B', T'\}_{k(A',B')}) = tr(\mathsf{Resp}[A', B', T', i'])_2 \in \pm(A, \{B, T\}_{k(A,B)})$, by definition of N'. But $+(A', \{B', T'\}_{k(A',B')}) \in \pm(A, \{B, T\}_{k(A,B)})$ is only possible, if $A' = A$, $B' = B$ and $T' = T$. We, thus, have established that $n_0 = (s_0, i_0) = (\mathsf{Resp}[A, B, T, i'], 2)$. Because $n_0 \in N' \subseteq N_{\mathcal{B}}$, it the case that $(\mathsf{Resp}[A, B, T, i'], 1) \Rightarrow_{\mathcal{B}} n_0$, by **(B4)**. Then $\{(\mathsf{Resp}[A, B, T, i'], 1), (\mathsf{Resp}[A, B, T, i'], 2)\} \subseteq N_{\mathcal{B}}$. That means that $\mathsf{Resp}[A, B, T, i'] \in \mathcal{B}$. □

Exercise 1 *Let* Σ *be as in Example 2 and, for all* s *in* Σ, $tr(s)$ *be defined as in Example 2. Assume that, for all* s *in* $\mathcal{A}$, $tr(s)$ *is an attacker trace of the kind* ***M****,* ***K****,* ***F****,* ***T****,* ***C*** *or* ***S*** *(see Section 2), where* SharedKey *is disjoint from the initial attacker knowledge. Let* $\mathcal{S} = (\Sigma \cup \mathcal{A}, tr)$.

(a) *Prove that the following formula holds:*

$$(\forall \mathcal{B} \in \mathsf{bundle}(\mathcal{S}), A, B \in \mathsf{Name}, T \in \mathsf{Text}, i \in I\!N)$$
$$(\mathsf{Init}[A, B, T, i] \in \mathcal{B} \Longrightarrow (\exists i')(\mathsf{Resp}[A, B, T, i'] \in \mathcal{B}))$$

(b) *Does this formula still hold if we omit the agent name* B *from the ciphertext? Like this:*

$$tr(\mathsf{Init}[A, B, T, i]) \triangleq \langle +(B, A), -(A, \{T\}_{\mathsf{k}(A,B)})\rangle$$
$$tr(\mathsf{Resp}[A, B, T, i]) \triangleq \langle -(B, A), +(A, \{T\}_{\mathsf{k}(A,B)})\rangle$$

Why or why not?

Exercise 2 *Consider the same strand space as in Exercise 1 but, in addition, allow attacker traces of the kinds* ***E*** *and* ***D****. Prove that the formula from Exercise 1 still holds.*

Although reasoning in the strand space model is quite intuitive, manual proofs become quite tedious for larger protocols. It is nice that tools like Athena, Scyther and ProVerif automate this kind of reasoning for us!

References

[FHG99] F. J. Thayer Fabrega, J. C. Herzog, and J. D. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7(1), 1999.