A Calculus for Cryptographic Protocols: The Spi Calculus

by M. Abadi and A. Gordon

Martin Paraskevov

University of Maryland

April 14, 2008

Security and the Pi Calculus

- The Spi Calculus is an extension of the Pi Calculus
- The Pi Calculus is used to describe protocols at an abstract level
- Protocols are processes
- Communication is the sole means of computation
- Channels can be created and passed
- Scoping is the basis of security

Why the Spi Calculus

- Pi Calculus does not express common crypto operations
- Other approaches are either informal or have tenuous relation to implementation
- The Spi Calculus has a formal semantics
- Provides a setting for analyzing protocols
- Security guarantees can be expressed as equivalences between processes
- The environment/adversary need not be modeled explicitely
- Writing such a model can be tedious
- Still, the Spi calculus is poorer than some models for informal mathematical reasoning
- It does not have any notion of probability or complexity

Basics of the Pi Calculus

- Small but expressive programming language
- Programs are systems of independent parallel processes
- They synchronize via message-passing handshakes on named channels
- Channels may be restricted
- Channels may be passed
- Extrusion of scope

Syntax of the Pi Calculus - Terms

$$
\begin{array}{lll}
L, M, N & ::= & \quad \text{terms} \\
 & ::= & n \\
 & ::= & (M, N) \\
 & ::= & 0 \\
 & ::= & suc(M) \\
 & ::= & x
\end{array}
$$

Syntax of the Pi Calculus - Processes

$$
\begin{array}{lll}
P, Q, R & ::= & \text{processes} \\
 & ::= & \bar{M}\langle N\rangle.P \\
 & ::= & M(x).P \\
 & ::= & P|Q \\
 & ::= & (\nu n)P \\
 & ::= & !P \\
 & ::= & [M\ is\ N]P \\
 & ::= & 0 \\
 & ::= & let(x, y) = M\ in\ P \\
 & ::= & case\ M\ of\ 0 : P\ suc(x) : Q
\end{array}
$$

Indistinguishability

$P \simeq Q$

A process R cannot distinguish running in parallel with P from running in parallel with Q

A First Example

Message 1 $\quad A \longrightarrow B : M$ on c_{AB}

$$
\begin{aligned}
A(M) &\triangleq \overline{c_{AB}}\langle M \rangle \\
B &\triangleq c_{AB}(x).0 \\
Inst(M) &\triangleq (\nu c_{AB})(A(M) | B)
\end{aligned}
$$

A First Example

Message 1 $\quad A \longrightarrow B : M$ on c_{AB}

$$\begin{aligned} A(M) &\triangleq \overline{c_{AB}}\langle M\rangle \\ B &\triangleq c_{AB}(x).F(x) \\ Inst(M) &\triangleq (\nu c_{AB})(A(M)|B) \end{aligned}$$

A First Example - Specification

Message 1 $\quad A \rightarrow B : M \text{ on } c_{AB}$

$$\begin{aligned} A(M) &\triangleq \overline{c_{AB}}\langle M\rangle \\ B_{spec}(M) &\triangleq c_{AB}(x).F(M) \\ Inst_{spec}(M) &\triangleq (\nu c_{AB})(A(M)|B_{spec}(M)) \end{aligned}$$

Authenticity and Secrecy

Authenticity: $Inst(M) \simeq Inst_{spec}(M)$, for any M
Secrecy: $Inst(M) \simeq Inst(M')$ if $F(M) \simeq F(M')$ for any M, M'

Wide Mouthed Frog

Message 1	$A \rightarrow S : c_{AB}$ on c_{AS}
Message 2	$S \rightarrow B : c_{AB}$ on c_{SB}
Message 3	$A \rightarrow B : M$ on c_{AB}

$$
\begin{aligned}
A(M) &\triangleq (\nu c_{AB})\overline{c_{AS}}\langle c_{AB}\rangle.\overline{c_{AB}}\langle M\rangle \\
S &\triangleq c_{AS}(x).\overline{c_{SB}}\langle x\rangle \\
B &\triangleq c_{SB}(x).x(y).F(y) \\
Inst(M) &\triangleq (\nu c_{AS})(\nu c_{SB})(A(M)|S|B)
\end{aligned}
$$

Wide Mouthed Frog - Specification

Message 1	$A \rightarrow S : c_{AB}$ on c_{AS}
Message 2	$S \rightarrow B : c_{AB}$ on c_{SB}
Message 3	$A \rightarrow B : M$ on c_{AB}

$$A(M) \triangleq (\nu c_{AB})\overline{c_{AS}}\langle c_{AB}\rangle.\overline{c_{AB}}\langle M\rangle$$

$$S \triangleq c_{AS}(x).\overline{c_{SB}}\langle x\rangle$$

$$B_{spec}(M) \triangleq c_{SB}(x).x(y).F(M)$$

$$Inst_{spec}(M) \triangleq (\nu c_{AS})(\nu c_{SB})(A(M)|S|B_{spec}(M))$$

Authenticity and Secrecy

Authenticity: $Inst(M) \simeq Inst_{spec}(M)$, for any M
Secrecy: $Inst(M) \simeq Inst(M')$ if $F(M) \simeq F(M')$ for any M, M'

Syntax of the Spi Calculus with Shared Key Cryptography - Terms

$$
\begin{aligned}
L, M, N \quad &::= \quad \text{terms} \\
&::= \quad n \\
&::= \quad (M, N) \\
&::= \quad 0 \\
&::= \quad suc(M) \\
&::= \quad x \\
&::= \quad \{M\}_N
\end{aligned}
$$

Syntax of the Spi Calculus with Shared Key Cryptography - Processes

$$
\begin{array}{lll}
P, Q, R & ::= & \text{processes} \\
 & ::= & \bar{M}\langle N\rangle.P \\
 & ::= & M(x).P \\
 & ::= & P|Q \\
 & ::= & (\nu n)P \\
 & ::= & !P \\
 & ::= & [M\ is\ N]P \\
 & ::= & 0 \\
 & ::= & let(x, y) = M\ in\ P \\
 & ::= & case\ M\ of\ 0 : P\ suc(x) : Q \\
 & ::= & case\ L\ of\ \{x\}_N\ in\ P
\end{array}
$$

Semantics Preliminaries

- $fn(M), fn(P)$ - sets of free names in term M and process P
- $fv(M), fv(P)$ - sets of free variables in term M and process P
- A term M or a process P is closed if it has no free variables
- $Proc = \{P | fv(P) = \emptyset\}$

The Reduction Relation

$$
\begin{array}{rcl}
!P & > & P|!P \\
[M \ is \ M]\, P & > & P \\
let(x, y) = (M, N) \ in \ P & > & P[M/x][N/y] \\
case \ 0 \ of \ 0 : P \ suc(x) : Q & > & P \\
case \ suc(M) \ of \ 0 : P \ suc(x) : Q & > & Q[M/x] \\
case\{M\}_N \ of \ \{x\}_N \ in \ P & > & P[M/x]
\end{array}
$$

Structural Equivalence

$$
\begin{aligned}
P|0 &\equiv P \\
P|Q &\equiv Q|P \\
P|(Q|R) &\equiv (P|Q)|R \\
(\nu m)(\nu n)P &\equiv (\nu n)(\nu m)P \\
(\nu n)(P|Q) &\equiv P|(\nu n)Q
\end{aligned}
$$

$$\frac{P > Q}{P \equiv Q} \qquad \frac{}{P \equiv P}$$

$$\frac{P \equiv Q}{Q \equiv P} \qquad \frac{P \equiv Q \quad Q \equiv R}{P \equiv R}$$

$$\frac{P \equiv P'}{P|Q \equiv P'|Q} \qquad \frac{P \equiv P'}{(\nu m)P \equiv (\nu m)P'}$$

The Reaction Relation

$$\overline{m}\langle N\rangle.P|m(x).Q \rightarrow P|Q[N/x]$$

$$\frac{P \equiv P' \qquad P' \rightarrow Q' \qquad Q' \equiv Q}{P \rightarrow Q}$$

$$\frac{P \rightarrow P'}{P|Q \rightarrow P'|Q} \qquad \frac{P \rightarrow P'}{(\nu n)P \rightarrow (\nu n)P'}$$

P exibits barb β

$$m(x).P \downarrow m \qquad \overline{m}\langle M\rangle.P \downarrow \overline{m}$$

$$\frac{P \downarrow \beta}{P|Q \downarrow \beta} \qquad \frac{P \downarrow \beta \quad \beta \notin \{m, \overline{m}\}}{(\nu m)P \downarrow \beta}$$

$$\frac{P \equiv Q \quad Q \downarrow \beta}{P \downarrow \beta}$$

$$\frac{P \downarrow \beta}{P \Downarrow \beta} \qquad \frac{P \rightarrow Q \quad Q \Downarrow \beta}{P \Downarrow \beta}$$

Testing Equivalence

$$P \simeq Q \quad \stackrel{\triangle}{=} \quad \text{for any test } (R, \beta),$$
$$(P|R) \Downarrow \beta \Leftrightarrow (Q|R) \Downarrow \beta$$

A First Cryptographic Example

Message 1 $\quad A \longrightarrow B : M$ on c_{AB}

$$\begin{aligned} A(M) &\triangleq \overline{c_{AB}}\langle \{M\}_{K_{AB}} \rangle \\ B &\triangleq c_{AB}(x).case\ x\ of\ \{y\}_{K_{AB}}\ in\ F(y) \\ Inst(M) &\triangleq (\nu K_{AB})(A(M)|B) \end{aligned}$$

A First Cryptographic Example - Specification

Message 1 $\quad A \rightarrow B : M$ on c_{AB}

$$
\begin{aligned}
A(M) &\triangleq \overline{c_{AB}}\langle\{M\}_{K_{AB}}\rangle \\
B_{spec}(M) &\triangleq c_{AB}(x).case\ x\ of\ \{y\}_{K_{AB}}\ in\ F(M) \\
Inst_{spec}(M) &\triangleq (\nu K_{AB})(A(M)|B_{spec}(M))
\end{aligned}
$$

Authenticity and Secrecy

Authenticity: $Inst(M) \simeq Inst_{spec}(M)$, for any M

Secrecy: $Inst(M) \simeq Inst(M')$ if $F(M) \simeq F(M')$ for any M, M'

Key Establishment

Message 1	$A \to S : \{K_{AB}\}_{K_{AS}}$ on c_{AS}
Message 2	$S \to B : \{K_{AB}\}_{K_{SB}}$ on c_{SB}
Message 3	$A \to B : \{M\}_{K_{AB}}$ on c_{AB}

$$
\begin{aligned}
A(M) &\triangleq (\nu K_{AB})\overline{c_{AS}}\langle\{K_{AB}\}_{K_{AS}}\rangle.\overline{c_{AB}}\langle\{M\}_{K_{AB}}\rangle \\
S &\triangleq c_{AS}(x).case\ x\ of\ \{y\}_{K_{AS}}\ in\ \overline{c_{SB}}\langle\{y\}_{K_{SB}}\rangle \\
B &\triangleq c_{SB}(x).case\ x\ of\ \{y\}_{K_{SB}}\ in \\
&\quad\ c_{AB}(z).case\ z\ of\ \{w\}_{y}\ in\ F(w) \\
Inst(M) &\triangleq (\nu K_{AS})(\nu K_{SB})(A(M)|S|B)
\end{aligned}
$$

Key Establishment - Specification

Message 1	$A \rightarrow S : \{K_{AB}\}_{K_{AS}}$ on c_{AS}
Message 2	$S \rightarrow B : \{K_{AB}\}_{K_{SB}}$ on c_{SB}
Message 3	$A \rightarrow B : \{M\}_{K_{AB}}$ on c_{AB}

$$
\begin{aligned}
A(M) &\triangleq (\nu K_{AB})\overline{c_{AS}}\langle\{K_{AB}\}_{K_{AS}}\rangle.\overline{c_{AB}}\langle\{M\}_{K_{AB}}\rangle \\
S &\triangleq c_{AS}(x).case\ x\ of\ \{y\}_{K_{AS}}\ in\ \overline{c_{SB}}\langle\{y\}_{K_{SB}}\rangle \\
B_{spec}(M) &\triangleq c_{SB}(x).case\ x\ of\ \{y\}_{K_{SB}}\ in \\
&\quad\ c_{AB}(z).case\ z\ of\ \{w\}_{y}\ in\ F(M) \\
Inst_{spec}(M) &\triangleq (\nu K_{AS})(\nu K_{SB})(A(M)|S|B_{spec}(M))
\end{aligned}
$$

Authenticity and Secrecy

Authenticity: $Inst(M) \simeq Inst_{spec}(M)$, for any M
Secrecy: $Inst(M) \simeq Inst(M')$ if $F(M) \simeq F(M')$ for any M, M'

Example of Reaction

$$
\begin{aligned}
Inst(M) &\equiv (\nu K_{AS})(\nu K_{SB})(A(M)|S|B) \\
&\rightarrow (\nu K_{AS})(\nu K_{SB})(\nu K_{AB}) \\
&\qquad (\overline{c}_{AB}\langle\{M\}_{K_{AB}}\rangle|\overline{c}_{SB}\langle\{K_{AB}\}_{K_{SB}}\rangle|B) \\
&\rightarrow (\nu K_{AS})(\nu K_{SB})(\nu K_{AB}) \\
&\qquad (\overline{c}_{AB}\langle\{M\}_{K_{AB}}\rangle|c_{AB}(z).case\ z\ of\ \{w\}_{K_{AB}}\ in\ F(w)) \\
&\rightarrow (\nu K_{AS})(\nu K_{SB})(\nu K_{AB})F(M) \\
&\equiv F(M)
\end{aligned}
$$

A complete authetication example (with a flaw)

- So far channel establishment and data communication happen only once
- Consider a system with a server S and n other principals
- $suc(0), suc(suc(0)), \ldots$ will denote the other principals. Abreviate them as $\underline{1}, \underline{2}, \ldots$
- Principal $\underline{i}$ has input channel c_i
- S and $\underline{i}$ share a key for each direction of communication - K_{iS} and K_{Si}

A complete authentication example (with a flaw) (continued)

Message 1	$A \rightarrow S : A, \{B, K_{AB}\}_{K_{AS}}$ on c_S
Message 2	$S \rightarrow B : \{A, K_{AB}\}_{K_{SB}}$ on c_B
Message 3	$A \rightarrow B : A, \{M\}_{K_{AB}}$ on c_B

A complete authentication example (with a flaw) (continued)

- An instance is determined by a choice of parties A and B
- An instance is $I = (i, j, M)$
- There is an abstraction F representing the behavior of any principal after receipt of Message 3: $F(\underline{i}, \underline{j}, M)$

A complete authentication example (with a flaw) (continued)

$$Send(i,j,M) \triangleq (\nu K)(\overline{c}_S\langle(\underline{i}, \{\underline{j}, K\}_{K_{iS}})\rangle | \overline{c}_j\langle(\underline{i}, \{M\}_K)\rangle)$$

$$\begin{aligned} Recv(j) \triangleq\ & c_j(y_{cipher}).case\ y_{cipher}\ of\ \{x_A, x_{key}\}_{K_{Sj}}\ in \\ & c_j(z_A, z_{cipher}).\ [x_A\ is\ z_A] \\ & case\ z_{cipher}\ of\ \{z_{plain}\}_{x_{key}}\ in\ F(x_A, \underline{j}, z_{plain}) \end{aligned}$$

$$\begin{aligned} S \triangleq\ & c_S(x_A, x_{cipher}). \\ & \prod_{i \in 1..n} [x_A\ is\ \underline{i}]\ case\ x_{cipher}\ of\ \{x_B, x_{key}\}_{K_{iS}}\ in \\ & \prod_{j \in 1..n} [x_B\ is\ \underline{j}]\ \overline{c}_j\langle\{x_A, x_{key}\}_{K_{Sj}}\rangle \end{aligned}$$

A complete authentication example (with a flaw) (continued)

$$
\begin{aligned}
Sys(I_1, ..., I_m) \;\triangleq\; & (\nu \vec{K_{iS}})(\nu \vec{K_{Sj}}) \\
& (Send(I_1)|...|Send(I_m)| \\
& !S| \\
& !Recv(1)|...|!Recv(n))
\end{aligned}
$$

A complete authentication example (with a flaw) (continued)

$$
\begin{aligned}
Send_{spec}(i,j,M) &\triangleq (\nu p)(Send(i,j,p)|p(x).F(\underline{i},\underline{j},M)) \\
Recv_{spec}(j) &\triangleq c_j(y_{cipher}).case\ y_{cipher}\ of\ \{x_A, x_{key}\}_{K_{Sj}}\ in \\
&\quad c_j(z_A, z_{cipher}).\,[x_A\ is\ z_A] \\
&\quad case\ z_{cipher}\ of\ \{z_{plain}\}_{x_{key}}\ in\ \overline{z}_{plain}\langle * \rangle \\
S &\triangleq \text{ stays the same} \\
Sys_{spec}(I_1, \ldots, I_m) &\triangleq (\nu \vec{K_{iS}})(\nu \vec{K_{Sj}}) \\
&\quad (Send_{spec}(I_1)|\ldots|Send_{spec}(I_m)| \\
&\quad !S| \\
&\quad !Recv_{spec}(1)|\ldots|!Recv_{spec}(n))
\end{aligned}
$$

Authenticity

$Sys(I_1, ..., I_m) \triangleq Sys_{spec}(I_1, ..., I_m)$
for any instances $I_1, ..., I_m$
does not hold

- Consider the system $Sys(I, I')$ where $I = (i, j, M)$ and $I' = (i, j, M')$
- An attacker can replay messages of one instance and get them mistaken for messages of the other instance
- M will be passed twice to F
- Sys_{spec} will run each of $F(\underline{i}, \underline{j}, M)$ and $F(\underline{i}, \underline{j}, M')$ at most once
- Formally, a process may distinguish between $Sys(I, I')$ and Sys_{spec} within the Spi Calculus

A complete authentication example (repaired)

Message 1	$A \rightarrow S : A$ on c_S
Message 2	$S \rightarrow A : N_S$ on c_A
Message 3	$A \rightarrow S : A, \{A, A, B, K_{AB}, N_S\}_{K_{AS}}$ on c_S
Message 4	$B \rightarrow B : *$ on c_B
Message 5	$B \rightarrow S : N_B$ on c_S
Message 6	$S \rightarrow B : \{S, A, B, K_{AB}, N_B\}_{K_{SB}}$ on c_B
Message 7	$A \rightarrow B : A, \{M\}_{K_{AB}}$ on c_B

$$
\begin{aligned}
Send(i,j,M) &\triangleq \overline{c}_S\langle i\rangle | c_i(x_{nonce}).(\nu K)(\overline{c}_S\langle(\underline{i}, \{\underline{i}, \underline{i}, \underline{j}, K, x_{nonce}\}_{K_{iS}})\rangle | \\
&\qquad\qquad \overline{c}_j\langle(\underline{i}\{M\}_k)\rangle) \\
S &\triangleq c_S(x_A). \prod_{i \in 1..n} [x_A \text{ is } \underline{i}]\,(\nu N_S)(\overline{c}_i\langle N_S\rangle | \\
&\quad c_S(x'_A, x_{cipher}). \left[x'_A \text{ is } \underline{i}\right] \\
&\quad case\ x_{cipher}\ of\ \{y_A, z_A, x_B, x_{key}, x_{nonce}\}_{K_{iS}}\ in \\
&\quad \prod_{j \in 1..n} [y_A \text{ is } \underline{i}]\,[z_A \text{ is } \underline{i}]\,\left[x_B \text{ is } \underline{j}\right]\,[x_{nonce} \text{ is } N_S] \\
&\quad (\overline{c}_j\langle * \rangle | c_S(y_{nonce}).\overline{c}_j\langle\{S, \underline{i}, \underline{j}, x_{key}, y_{nonce}\}_{K_{Sj}}\rangle))
\end{aligned}
$$

Seven-Message Protocol continued

$$
\begin{aligned}
Recv(j) \;\triangleq\;& c_j(w).(\nu N_B)(\overline{c}_S\langle N_B\rangle| \\
& c_j(y_{cipher}). \\
& case\ y_{cipher}\ of\ \{x_S, x_A, x_B, x_{key}, y_{nonce}\}_{K_{S_j}}\ in \\
& \prod_{i\in 1..n} [x_S\ is\ S]\,[x_A\ is\ \underline{i}]\,[x_B\ is\ \underline{j}]\,[y_{nonce}\ is\ N_B] \\
& c_j(z_A, z_{cipher}).\,[z_A\ is\ x_A] \\
& case\ z_{cipher}\ of\ \{z_{plain}\}_{x_{key}}\ in\ F(\underline{i}, \underline{j}, z_{plain})) \\
Sys(I_1, \ldots, I_m) \;\triangleq\;& (\nu \vec{K_{iS}})(\nu \vec{K_{Sj}}) \\
& (Send(I_1)|\ldots|Send(I_m)| \\
& !S| \\
& !Recv(1)|\ldots|!Recv(n))
\end{aligned}
$$

Authenticity and Secrecy

Authenticity: $Sys(I_1, ..., I_m) \simeq Sys_{spec}(I_1, ..., I_m)$, for any $I_1, ..., I_m$

Secrecy: $Sys(I_1, ..., I_m) \simeq Sys(J_1, ..., J_m)$ if $I_k \simeq J_k$ for $k \in 1..m$

Conclusions

- Applied the Pi and Spi calculi to the description and analysis of protocols
- Takes into account attacks but does not need to model an attacker
- The Spi calculus can be extended to handle other crypto primitives
- Restriction and scope extrusion play central role