Applied Pi-calculus

Alessandro Bruni

Security II

The Applied Pi-calculus

$P, Q, R :=$ plain processes

- 0
- $P \parallel Q$
- $!P$
- $\nu n.P$
- if $t_1 = t_2$ then P else Q
- $\mathsf{in}(u, x).P$
- $\mathsf{out}(u, t).P$

$A, B, C :=$ extended processes

- P
- $A \parallel B$
- $\nu n.A$
- $\nu x.A$
- $\{^{t}/_{x}\}$

Frame of a process:

$$\phi(A) = \nu n_1 \ldots n_m \{^{t_1}/_{x_1}, \ldots, ^{t_k}/_{x_k}\}$$

$t \in \mathcal{T}(\mathcal{F}, \mathcal{X}, \mathcal{N})$ terms

$\mathcal{N}_{ch} \subseteq \mathcal{N}$ channel names

$\mathcal{X} = \mathcal{X}_b \uplus \mathcal{X}_{ch}$ base sort and channel sort for variables

Needham-Schröder

$$
\begin{aligned}
A \to B : &\quad \mathsf{aenc}(\langle a, n_a \rangle, \mathsf{pk}_b) \\
B \to A : &\quad \mathsf{aenc}(\langle n_a, n_b \rangle, \mathsf{pk}_a) \\
A \to B : &\quad \mathsf{aenc}(n_b, \mathsf{pk}_b)
\end{aligned}
$$

Needham-Schröder

$$
\begin{aligned}
A \to B: &\quad \mathsf{aenc}(\langle a, n_a \rangle, \mathsf{pk}_b) \\
B \to A: &\quad \mathsf{aenc}(\langle n_a, n_b \rangle, \mathsf{pk}_a) \\
A \to B: &\quad \mathsf{aenc}(n_b, \mathsf{pk}_b)
\end{aligned}
$$

Initiator:

$$
\begin{aligned}
P_A(sk_i, pk_r) \quad \hat{=} \quad & \nu n_a.\ \mathsf{out}(c, \mathsf{aenc}(\langle \mathsf{pk}(sk_i), n_a \rangle, \mathsf{pk}_r)). \\
& \mathsf{in}(c, x). \\
& \mathsf{if}\ \mathsf{fst}(\mathsf{adec}(x, sk_i)) = n_a\ \mathsf{then} \\
& \mathsf{let}\ x_{nb} = \mathsf{snd}(\mathsf{adec}(x, sk_i))\ \mathsf{in} \\
& \mathsf{out}(c, \mathsf{aenc}(x_{nb}, \mathsf{pk}_r))
\end{aligned}
$$

Responder:

$$
\begin{aligned}
P_B(sk_r) \quad \hat{=} \quad & \mathsf{in}(c, y). \\
& \mathsf{let}\ pk_i = \mathsf{fst}(\mathsf{adec}(y, sk_r))\ \mathsf{in} \\
& \mathsf{let}\ y_{na} = \mathsf{snd}(\mathsf{adec}(y, sk_r))\ \mathsf{in} \\
& \nu n_b.\mathsf{out}(c, \mathsf{aenc}(\langle y_{na}, n_b \rangle, pk_i)) \\
& \mathsf{in}(c, z). \\
& \mathsf{if}\ \mathsf{adec}(z, sk_r)) = n_b\ \mathsf{then}\ Q
\end{aligned}
$$

Putting it all together

$$P^1_{\mathsf{nspk}} \hat{=} \nu sk_a, sk_b.(P_A(sk_a, \mathsf{pk}(sk_b)) \parallel P_B(sk_b) \parallel \mathsf{out}(c, \mathsf{pk}(sk_a)) \parallel \mathsf{out}(c, \mathsf{pk}(sk_b)))$$

Problem? A is not willing to talk to the intruder.

$$P^2_{\mathsf{nspk}} \hat{=} \nu sk_a, sk_b.(P_A(sk_a, \mathsf{pk}(sk_b)) \parallel P_A(sk_a, \mathsf{pk}(sk_c)) \parallel P_B(sk_b) \parallel \mathsf{out}(c, \mathsf{pk}(sk_a)) \parallel \mathsf{out}(c, \mathsf{pk}(sk_b)))$$

Problem? We don't know a priori with whom agents should start a session.

$$P^3_{\mathsf{nspk}} \hat{=} \nu sk_a, sk_b.(\mathsf{in}(c, x_{pk}).P_A(sk_a, x_{pk}) \parallel P_B(sk_b) \parallel \mathsf{out}(c, \mathsf{pk}(sk_a)) \parallel \mathsf{out}(c, \mathsf{pk}(sk_b)))$$

Problem? Only one session for each role.

$$P^4_{\mathsf{nspk}} \hat{=} \nu sk_a, sk_b.(!\mathsf{in}(c, x_{pk}).P_A(sk_a, x_{pk}) \parallel !P_B(sk_b) \parallel \mathsf{out}(c, \mathsf{pk}(sk_a)) \parallel \mathsf{out}(c, \mathsf{pk}(sk_b)))$$

Problem? A never acts as B and viceversa. In principle this could be source of attacks

$$P^5_{\mathsf{nspk}} \hat{=} !\nu sk_a, sk_b.(!\mathsf{in}(c, x_{pk}).P_A(sk_a, x_{pk}) \parallel !P_B(sk_a) \parallel !\mathsf{in}(c, x_{pk}).P_A(sk_b, x_{pk}) \parallel !P_B(sk_b) \parallel \mathsf{out}(c, \mathsf{pk}(sk_a)) \parallel \mathsf{out}(c, \mathsf{pk}(sk_b)))$$

Problem? Nope ☺ but we can express this more succintly.

$$P^6_{\mathsf{nspk}} \hat{=} !\nu sk.(!\mathsf{in}(c, x_{pk}).P_A(sk, x_{pk}) \parallel !P_B(sk) \parallel \mathsf{out}(c, \mathsf{pk}(sk)))$$

Operational semantics

Structural equivalences:

$$
\begin{array}{lrcl}
\textsc{Par-0} & A \parallel 0 & \equiv & A \\
\textsc{Par-C} & A \parallel B & \equiv & B \parallel A \\
\textsc{Par-A} & (A \parallel B) \parallel C & \equiv & A \parallel (B \parallel C) \\
\textsc{Repl} & !P & \equiv & P \parallel !P \\
\\
\textsc{New-0} & \nu\, n.\, 0 & \equiv & 0 \\
\textsc{New-Par} & A \parallel \nu\, u.B & \equiv & \nu\, u.(A \parallel B) \quad \text{when } u \notin \mathsf{fv}(A) \cup \mathsf{n}(A) \\
\textsc{New-C} & \nu\, u.\nu\, v.A & \equiv & \nu\, v.\nu\, u.A \\
\\
\textsc{Alias} & \nu\, x.\{^t/_x\} & \equiv & 0 \\
\textsc{Subst} & \{^t/_x\} \parallel A & \equiv & \{^t/_x\} \parallel A\{^t/_x\} \\
\textsc{Rewrite} & \{^{t_1}/_x\} & \equiv & \{^{t_2}/_x\} \quad \text{when } t_1 =_E t_2
\end{array}
$$

Evaluation rules:

$$
\begin{array}{ll}
\textsc{Comm} & \mathsf{out}(c,t).P_1 \parallel \mathsf{in}(c,x).P_2 \rightarrow P_1 \parallel P_2\{^t/_x\} \\
\textsc{Then} & \mathsf{if}\ t = t\ \mathsf{then}\ P\ \mathsf{else}\ Q \rightarrow P \\
\textsc{Else} & \mathsf{if}\ t_1 = t_2\ \mathsf{then}\ P\ \mathsf{else}\ Q \rightarrow Q \\
 & \qquad \text{where } t_1, t_2 \text{ are ground and } t_1 \neq_E t_2
\end{array}
$$

Structural equivalence (Example 5.1)

$$
\begin{array}{rcll}
\mathsf{out}(c, t_1) & \equiv & \mathsf{out}(c, t_1) \parallel 0 & \text{by } \textsc{Par-0} \\
& \equiv & \mathsf{out}(c, t_1) \parallel \nu\, x.\{^{t_1}/_{x}\} & \text{by } \textsc{Alias} \\
& \equiv & \nu\, x.(\mathsf{out}(c, t_1) \parallel \{^{t_1}/_{x}\}) & \text{by } \textsc{New-Par} \\
& \equiv & \nu\, x.(\{^{t_1}/_{x}\} \parallel \mathsf{out}(c, t_1)) & \text{by } \textsc{Par-C} \\
& \equiv & \nu\, x.(\{^{t_1}/_{x}\} \parallel \mathsf{out}(c, x)) & \text{by } \textsc{Subst} \\
& \equiv & \nu\, x.(\{^{t_2}/_{x}\} \parallel \mathsf{out}(c, x)) & \text{by } \textsc{Rewrite} \\
& \equiv & \nu\, x.(\{^{t_2}/_{x}\} \parallel \mathsf{out}(c, t_2)) & \text{by } \textsc{Subst} \\
& \equiv & \nu\, x.(\mathsf{out}(c, t_2) \parallel \{^{t_2}/_{x}\}) & \text{by } \textsc{Par-C} \\
& \equiv & \mathsf{out}(c, t_2) \parallel \nu\, x.\{^{t_2}/_{x}\} & \text{by } \textsc{New-Par} \\
& \equiv & \mathsf{out}(c, t_2) \parallel 0 & \text{by } \textsc{Alias} \\
& \equiv & \mathsf{out}(c, t_2) & \text{by } \textsc{Par-0}
\end{array}
$$

Executing Needham-Schröder

$$
\begin{array}{lrl}
 & \nu sk_a, sk_b.\ P_A(sk_a, \mathsf{pk}(sk_b)) \parallel P_B(sk_b) & \\
\rightarrow & \nu sk_a, sk_b, n_a, n_b. & \mathsf{in}(c, x). \\
 & & \mathsf{if}\ \mathsf{fst}(\mathsf{adec}(x, sk_i)) = n_a\ \mathsf{then} \\
 & & \mathsf{let}\ x_{nb} = \mathsf{snd}(\mathsf{adec}(x, sk_i))\ \mathsf{in} \\
 & & \mathsf{out}(c, \mathsf{aenc}(x_{nb}, \mathsf{pk}_r)) \\
 & \parallel & \mathsf{out}(c, \mathsf{aenc}(\langle n_a, n_b \rangle, \mathsf{pk}(sk_a))) \\
 & & \mathsf{in}(c, z). \\
 & & \mathsf{if}\ \mathsf{adec}(z, sk_b)) = n_b\ \mathsf{then}\ Q \\
\rightarrow & \nu sk_a, sk_b, n_a, n_b. & \mathsf{if}\ n_a = n_a\ \mathsf{then} \\
 & & \mathsf{out}(c, \mathsf{aenc}(n_b, \mathsf{pk}_r)) \\
 & \parallel & \mathsf{in}(c, z). \\
 & & \mathsf{if}\ \mathsf{adec}(z, sk_b)) = n_b\ \mathsf{then}\ Q \\
\rightarrow & \nu sk_a, sk_b, n_a, n_b. & \mathsf{out}(c, \mathsf{aenc}(n_b, \mathsf{pk}_r)) \\
 & \parallel & \mathsf{in}(c, z). \\
 & & \mathsf{if}\ \mathsf{adec}(z, sk_b)) = n_b\ \mathsf{then}\ Q \\
\rightarrow & \nu sk_a, sk_b, n_a, n_b. & \mathsf{if}\ n_b = n_b\ \mathsf{then}\ Q \\
\rightarrow & \nu sk_a, sk_b, n_a, n_b. & Q
\end{array}
$$

Observational equivalence

Barb: we write A $\Downarrow a$ iff A is able to send on channel a, that is, $A \rightarrow^* C[out(a,t).P]$ for some evaluation context $C[\_]$ that does not bind a.

Definition 5.1. Observational equivalence, denoted $\approx$, is the largest symmetric relation $\mathcal{R}$ on closed extended processes with same domain such that if $A \mathcal{R} B$ then

1. if $A \Downarrow a$ then $B \Downarrow a$;
2. if $A \rightarrow^* A'$ then there exists B' such that $B \rightarrow^* B'$ and $A' \mathcal{R} B'$;
3. for all closing evaluation context $C[\_]$ we have that $C[A] \mathcal{R} C[B]$.

Observational-equivalent?

Example 5.3

$$\begin{aligned} A &= \mathsf{in}(c, x).\ \text{if } x = 0 \text{ then } \mathsf{out}(c, 1) \\ B &= \mathsf{in}(c, x).\ \text{if } x = 0 \text{ then } \mathsf{out}(c, 0) \end{aligned}$$

Example 5.4

$$\begin{aligned} A &= \mathsf{in}(c, x).\ \nu n.\ \mathsf{out}(c, h(n)) \\ B &= \mathsf{in}(c, x).\ \nu n.\ \mathsf{out}(c, h(\langle x, n \rangle)) \end{aligned}$$

Labelled semantics

IN $$\mathsf{in}(a, x).P \xrightarrow{in(a,t)} P\{^t/_x\}$$

OUT-CH $$\mathsf{out}(a, c).P \xrightarrow{out(a,c)} P$$

OPEN-CH $$\frac{A \xrightarrow{out(a,c)} A' \qquad c \neq a}{\nu c.A \xrightarrow{\nu c.\mathsf{out}(a,c)} A'}$$

OUT-T $$\mathsf{out}(a, t).P \xrightarrow{\nu x.out(a,x)} P \mid \{^t/_x\} \qquad x \notin \mathsf{fv}(P) \cup \mathsf{fv}(t)$$

SCOPE $$\frac{A \xrightarrow{\alpha} A' \qquad u \text{ does not occur in } \alpha}{\nu u.A \xrightarrow{\alpha} \nu u.A'}$$

PAR $$\frac{A \xrightarrow{\alpha} A' \quad bv(\alpha) \cap fv(B) = bn(\alpha) \cap fn(B) = \emptyset}{A \mid B \xrightarrow{\alpha} A' \mid B}$$

STRUCT $$\frac{A \equiv B \quad B \xrightarrow{\alpha} B' \quad A' \equiv B'}{A \xrightarrow{\alpha} A'}$$

Labelled bisimilarity & Observational equivalence

Definition 5.2. *Labelled bisimilarity*, denoted $\approx_\ell$, is the largest symmetric relation $\mathcal{R}$ on closed extended processes, such that if $A\mathcal{R}B$ then we have

- $A \sim B$;
- if $A \to A'$ then there exists B' such that $B \to^* B'$ and $A'\mathcal{R}B'$;
- if $A \xrightarrow{\alpha} A'$ and $\mathsf{fv}(\alpha) \subseteq \mathsf{Dom}(A)$ and $\mathsf{bn}(\alpha) \cap \mathsf{n}(B) = \emptyset$ then there exists B' such that $B \to^* \xrightarrow{\alpha} \to^* B'$ and $A'\mathcal{R}B'$;

Theorem 5.1 ([Abadi and Fournet, 2001])**.** Let A and B be two closed extended processes. $A \approx B$ if and only if $A \approx_\ell B$.

Note: labelled bisimilarity implies static equivalence of frames .

$$A \approx_l B \Rightarrow \phi(A) \sim \phi(B)$$

Events

$$\textsc{Event} \quad \text{event } e(t).\ P \to P$$

Secrecy

Can be defined in term of events:

Definition 6.2. Let A be a closed extended process such that the event ded does not occur in A and $s \in \mathsf{n}(A)$. Let $A^s = \nu s.(A \parallel (in(c, x) \text{ if } x = s \text{ then event } ded(s))$. We say that s is (weakly) secret in A if and only if for all reduction sequence $R = A^s \xrightarrow{(\alpha_1)} A_1 \ldots \xrightarrow{(\alpha_n)} A_n$ we have that R does not satisfy $ded(s)$.

Authentication

The ISO/IEC-9798-1 standard defines the goal of (entity) authentication as follows:

> *Entity authentication mechanisms allow the verification, of an entity's claimed identity, by another entity. The authenticity of the entity can be ascertained only for the instance of the authentication exchange.*

[G. Lowe, 1997]
A hierarchy of authentication specifications.

Definition 2.1 (Aliveness). We say that a protocol guarantees to an initiator A *aliveness* of another agent B if, whenever A (acting as initiator) completes a run of the protocol, apparently with responder B, then B has previously been running the protocol.

Definition 2.2 (Weak agreement). We say that a protocol guarantees to an initiator A *weak agreement* with another agent B if, whenever A (acting as initiator) completes a run of the protocol, apparently with responder B, then B has previously been running the protocol, apparently with A.

Definition 2.3 (Non-injective agreement). We say that a protocol guarantees to an initiator A *non-injective agreement* with a responder B on a set of data items ds (where ds is a set of free variables appearing in the protocol description) if, whenever A (acting as initiator) completes a run of the protocol, apparently with responder B, then B has previously been running the protocol, apparently with A, and B was acting as responder in his run, and the two agents agreed on the data values corresponding to all the variables in ds.

Definition 2.4 (Agreement). We say that a protocol guarantees to an initiator A *agreement* with a responder B on a set of data items ds if, whenever A (acting as initiator) completes a run of the protocol, apparently with responder B, then B has previously been running the protocol, apparently with A, and B was acting as responder in his run, and the two agents agreed on the data values corresponding to all the variables in ds, and each such run of A corresponds to a *unique* run of B.

Authentication in the Applied Pi-calculus

Weak agreement ~ event correspondence

Definition 6.3. A closed extended process A satisfies the correspondence property $e(t) \rightsquigarrow e'(t')$ if and only if for all reduction $R = A \xrightarrow{(\alpha_1)} A_1 \ldots \xrightarrow{(\alpha_n)} A_n$ we have that if R satisfies $e(t\sigma)$ for some σ with $\mathsf{Dom}(\sigma) = \mathsf{fv}(t, t')$ then R satisfies $e'(t'\sigma)$.

Strong agreement ~ injective event correspondence

Definition 6.4. A closed extended process A satisfies the injective correspondence property $e(t) \rightsquigarrow_{\mathsf{inj}} e'(t')$ if and only if for all reduction $R = A \xrightarrow{(\alpha_1)} A_1 \ldots \xrightarrow{(\alpha_n)} A_n$, there exists a partial, injective function $\phi : \{1, \ldots, n\} \nrightarrow \{1, \ldots, n\}$ such that if R satisfies $e(t\sigma)$ for some σ with $\mathsf{Dom}(\sigma) = \mathsf{fv}(t, t')$ at step i then R satisfies $e'(t'\sigma)$ at step $\phi(i)$.

Diff-equivalences

In ProVerif we can write Applied Pi-calculus programs containing diff-terms. That is:

$$(P_1, P_2) = C[\{^{choice[t_1, t_2]}/_{x}\}]$$

Where P_1, P_2 are the two processes where x gets the value t_1 and t_2, respectively.

ProVerif can often check automatically that $P_1 \approx P_2$

Strong Secrecy

$$\mathsf{in}(c, x_1).\ \mathsf{in}(c, x_2).P\{^{x_1}/_{x}\} \approx \mathsf{in}(c, x_1).\ \mathsf{in}(c, x_2).P\{^{x_2}/_{x}\}$$

Example 6.3. Consider the protocol A that simply outputs the public key encryption of a secret.

$$A = \nu sk.\ \mathsf{out}(c, \mathsf{aenc}(x, \mathsf{pk}(sk))) \parallel \{^{\mathsf{pk}(sk)}/_{y}\}$$

The active substitution models that the public key is known to the adversary. It is easy to see that x is not strongly secret in A, i.e.,

$$\mathsf{in}(c, x_1).\ \mathsf{in}(c, x_2).A\{^{x_1}/_{x}\} \not\approx \mathsf{in}(c, x_1).\ \mathsf{in}(c, x_2).A\{^{x_2}/_{x}\}$$

Real-or-random Secrecy

$$\nu s.(\phi(A_n) \parallel \{^{s}/_{x}\}) \sim \nu s.(\phi(A_n) \parallel \nu s'.\ \{^{s'}/_{x}\})$$

Privacy in e-voting

$$S[V\{^{a}/_{id}, ^{v_1}/_{v}\} \parallel V\{^{b}/_{id}, ^{v_2}/_{v}\}] \approx S[V\{^{a}/_{id}, ^{v_2}/_{v}\} \parallel V\{^{b}/_{id}, ^{v_1}/_{v}\}]$$

Unlinkability in RFID Protocols

$$!\nu k.\ !P \approx \nu k.\ !P$$