Symbolic Verification of Cryptographic Protocols

Protocol Analysis in the Applied Pi-Calculus

David Baelde

LSV, ENS Paris-Saclay

2018

Example: Needham-Schroeder

$\mathsf{I}(sk_a, pk_b)$	$\mathsf{R}(sk_b, n_b, honest)$
new n_a.	
out$(c, \mathrm{aenc}(\langle \mathrm{pub}(sk_a), n_a\rangle, pk_b))$.	in(c, y).
	let $pk_a = \mathrm{proj}_1(\mathrm{adec}(y, sk_b))$ in
	let $n_a = \mathrm{proj}_2(\mathrm{adec}(y, sk_b))$ in
in(c, x).	out$(c, \mathrm{aenc}(\langle n_a, n_b\rangle, pk_a))$.
if $n_a = \mathrm{proj}_1(\mathrm{adec}(x, sk_a)$ then	
out$(c, \mathrm{aenc}(\mathrm{proj}_2(\mathrm{adec}(x, sk_a)), pk_b))$	in(c, z).
	if $n_b = \mathrm{adec}(z, sk_b)$ then
	if $pk_a = honest$ then
	out$(c, \mathrm{senc}(secret, n_b))$

Example: Needham-Schroeder

$\mathsf{I}(sk_a, pk_b)$	$\mathsf{R}(sk_b, n_b, honest)$
new n_a.	
out$(c, \mathrm{aenc}(\langle \mathrm{pub}(sk_a), n_a \rangle, pk_b))$.	in(c, y).
	let $pk_a = \mathrm{proj}_1(\mathrm{adec}(y, sk_b))$ in
	let $n_a = \mathrm{proj}_2(\mathrm{adec}(y, sk_b))$ in
in(c, x).	out$(c, \mathrm{aenc}(\langle n_a, n_b \rangle, pk_a))$.
if $n_a = \mathrm{proj}_1(\mathrm{adec}(x, sk_a)$ then	
out$(c, \mathrm{aenc}(\mathrm{proj}_2(\mathrm{adec}(x, sk_a)), pk_b))$	in(c, z).
	if $n_b = \mathrm{adec}(z, sk_b)$ then
	if $pk_a = honest$ then
	out$(c, \mathrm{senc}(secret, n_b))$

Scenario ($sk_a, sk_b, n_b \in \mathcal{N}$)

out$(c, \langle \mathrm{pub}(sk_a), \mathrm{pub}(sk_b) \rangle).(\ \mathsf{I}(sk_a, \mathrm{pub}(sk_b)) \mid \mathsf{R}(sk_b, n_b, \mathrm{pub}(sk_a))\ )$

Example: Needham-Schroeder

$\mathsf{I}(sk_a, pk_b)$	$\mathsf{R}(sk_b, n_b, honest)$
new n_a.	
out$(c, \mathrm{aenc}(\langle \mathrm{pub}(sk_a), n_a\rangle, pk_b))$.	in(c, y).
	let $pk_a = \mathrm{proj}_1(\mathrm{adec}(y, sk_b))$ in
	let $n_a = \mathrm{proj}_2(\mathrm{adec}(y, sk_b))$ in
in(c, x).	out$(c, \mathrm{aenc}(\langle n_a, n_b\rangle, pk_a))$.
if $n_a = \mathrm{proj}_1(\mathrm{adec}(x, sk_a)$ then	
out$(c, \mathrm{aenc}(\mathrm{proj}_2(\mathrm{adec}(x, sk_a)), pk_b))$	in(c, z).
	if $n_b = \mathrm{adec}(z, sk_b)$ then
	if $pk_a = honest$ then
	out$(c, \mathrm{senc}(secret, n_b))$

Scenario ($sk_a, sk_b, n_b, sk_i \in \mathcal{N}$)

out$(c, \langle sk_i, \mathrm{pub}(sk_a), \mathrm{pub}(sk_b)\rangle)$. $(\mathsf{I}(sk_a, \mathrm{pub}(sk_i)) \mid \mathsf{R}(sk_b, n_b, \mathrm{pub}(sk_a)))$

Exercise: LAK

$$
\begin{array}{lllll}
R & \to & T & : & n_R \\
T & \to & R & : & n_T, h(n_R \oplus n_T \oplus k) \\
R & \to & T & : & h(h(n_R \oplus n_T \oplus k) \oplus k \oplus n_R)
\end{array}
$$

Questions

- Formalize with two processes $T(k)$ and $R(k)$.
- Exhibit a trace tr that can be executed with $T(k) \mid R(k) \mid T(k)$ but not $T(k) \mid R(k) \mid T(k')$.
- Explain how this leads to an authentication attack.
- Fix the protocol using pairs rather than xor, and check with Proverif.