Lecture notes:
Compositional Information-ow Security for Interactive Systems

Presenter: Jaesung Park

Feb 16, 2017

1 Overview

1. Interactive system model
   (a) Process, input/output interaction, state transition
   (b) Trace/stream of actions
   (c) Stream equivalence
   (d) Security level and observables: *who* can observe *what*
2. Non-interference
   (a) What is progress-insensitive noninterference (PINI)?
   (b) What is progress-sensitive noninterference (PSNI)?
   (c) How are they different?
3. Compositional System
   (a) Minimal compositional units
   (b) PINI and PSNI of composite units

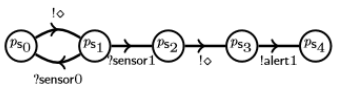
2 Interactive Systems

$p \in \mathbb{P}$: process

$a \in \mathbb{A}$: message input/output action through channel
$?cv$: input value v through channel c
$!cv$: output value v through channel c
$!\diamond$: internal actions

$\rightarrow \subseteq \mathbb{P} \times \mathbb{A} \times \mathbb{P}$: transition
$p \xrightarrow{a} p'$, $p \xrightarrow{a}$

repeat
  in sensor b
until $b = 1$
out alert 1



$$p_{s_0} \xrightarrow{!\diamond} p_{s_1} \xrightarrow{?\text{sensor0}} p_{s_0} \xrightarrow{!\diamond} p_{s_1} \xrightarrow{?\text{sensor1}} p_{s_2} \xrightarrow{!\diamond} p_{s_3} \xrightarrow{!\text{alert0}} p_{s_4}$$

$t \in \mathbb{T} = \mathbb{A}^*$: trace

$s \in \mathbb{S} = \mathbb{A}^\omega$: stream

$\bullet$: unobservable action due to security level
$p \xrightarrow{a}\!\!\!\!\rightarrow p' \quad$ iff $\quad a \neq \bullet \wedge (p \xrightarrow{a} p' \vee (p \xrightarrow{\bullet} \hat{p} \wedge \hat{p} \xrightarrow{a}\!\!\!\!\rightarrow p'))$

Definition 1. $\mathcal{R} \subseteq \mathbb{S} \times \mathbb{S}$ is a *strong stream relation* iff

$$\forall s_1, s_2. \quad s_1 \mathcal{R} s_2 \Rightarrow (s_1 \not\rightarrow \wedge s_2 \not\rightarrow) \vee$$
$$(\exists a, s_1', s_2'. \quad s_1 \xrightarrow{a} s_1' \wedge s_2 \xrightarrow{a} s_2' \wedge s_1' \mathcal{R} s_2').$$

s_1 and s_2 are *strongly stream related*, $s_1 = s_2$, iff there exists a strong stream relation $\mathcal{R}$ such that $s_1 \mathcal{R} s_2$.

Definition 2. $\mathcal{R} \subseteq \mathbb{S} \times \mathbb{S}$ is a *weak stream relation* iff

$$\forall s_1, s_2. \quad s_1 \mathcal{R} s_2 \Rightarrow (s_1 \not\twoheadrightarrow \wedge s_2 \not\twoheadrightarrow) \vee$$
$$(\exists a, s_1', s_2'. \quad s_1 \xrightarrow{a}\!\!\!\!\rightarrow s_1' \wedge s_2 \xrightarrow{a}\!\!\!\!\rightarrow s_2' \wedge s_1' \mathcal{R} s_2').$$

s_1 and s_2 are *weakly stream related*, $s_1 \simeq s_2$, iff there exists a strong stream relation $\mathcal{R}$ such that $s_1 \mathcal{R} s_2$.

Definition 3. $\mathcal{R} \subseteq \mathbb{S} \times \mathbb{S}$ is a *feeble stream relation* iff

$$\forall s_1, s_2. \quad s_1 \mathcal{R} s_2 \Rightarrow s_1 \twoheadrightarrow \vee s_2 \twoheadrightarrow \vee$$
$$(\exists a, s_1', s_2'. \quad s_1 \xrightarrow{a} \!\!\!\!\twoheadrightarrow s_1' \wedge s_2 \xrightarrow{a} \!\!\!\!\twoheadrightarrow s_2' \wedge s_1' \mathcal{R} s_2').$$

s_1 and s_2 are *feebly stream related*, $s_1 \approx s_2$, iff there exists a strong stream relation $\mathcal{R}$ such that $s_1 \mathcal{R} s_2$.

3 Non-Interference

Lattice $(\mathcal{L}, \sqsubseteq)$: partially-ordered set of security levels
Any input of higher-level channels is *unobervable*.

Definition 4. *$p\ \mathcal{R}_l$ -preserves the possibility of s_0 after t through s*, $\mathsf{preserve}^{l,\mathcal{R}}_{p,s_0}(t, s)$, is the largest predicate satisfying each of the following.

1. $\forall o \leq s. \quad \exists s' \in \mathbb{A}^\omega_l. \quad s_0 \mathcal{R}_l t.o.s' \quad \wedge p \xrightarrow{t.o.s'} \quad \wedge \mathsf{preserve}^{l,\mathcal{R}}_{p,s_0}(t.o, s')$
2. $\forall i \preceq_l s. \quad \exists s' \in \mathbb{A}^\omega_l. \quad s_0 \mathcal{R}_l t.i.s' \quad \wedge p \xrightarrow{t.i.s'} \quad \wedge \mathsf{preserve}^{l,\mathcal{R}}_{p,s_0}(t.i, s')$
3. $\forall \tilde{i} \simeq_l s. \quad \exists s' \in \mathbb{A}^\omega_l, \bar{i} \leq \tilde{i}, o. \quad s_0 \mathcal{R}_l t.\bar{i}.o.s' \quad \wedge p \xrightarrow{t.\bar{i}.o.s'} \quad \wedge \mathsf{preserve}^{l,\mathcal{R}}_{p,s_0}(t.\bar{i}.o, s')$

Definition 5. p is *$\mathcal{R}$ -noninterfering* iff $\forall l.\, \forall s \in \mathbb{S}_{\mathsf{F}}(p)$.

$$\exists s' \in \mathbb{S}(p) \cap \mathbb{A}^\omega_l. \quad s \mathcal{R}_l s' \wedge \mathsf{preserve}^{l,\mathcal{R}}_{p,s}(\epsilon, s').$$

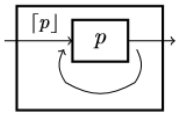
Definition 6. $p \in$ PSNI iff p is $\simeq$-noninterfering.
Definition 7. $p \in$ PINI iff p is $\approx$-noninterfering.

Lemma 1. $p \in \text{PSNI} \Rightarrow p \in \text{PINI}$.

4 Compositional System

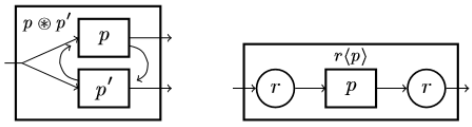
4.1 Loop Combinator and Its Limit

$\lceil p \rfloor$: Loop combinator
Receives input as p does
Output from p is sent to the environment, and then copy of output is fed to p.



$$\frac{p \xrightarrow{o} p' \quad p' \xrightarrow{o^{-1}} p''}{\lceil p \rfloor \xrightarrow{o} \lceil p'' \rfloor}\lceil\rfloor^{!} \qquad \frac{p \xrightarrow{i} p'}{\lceil p \rfloor \xrightarrow{i} \lceil p' \rfloor}\lceil\rfloor^{?}$$

4.2 Core combinators



1. *and* operator $p \circledast p'$

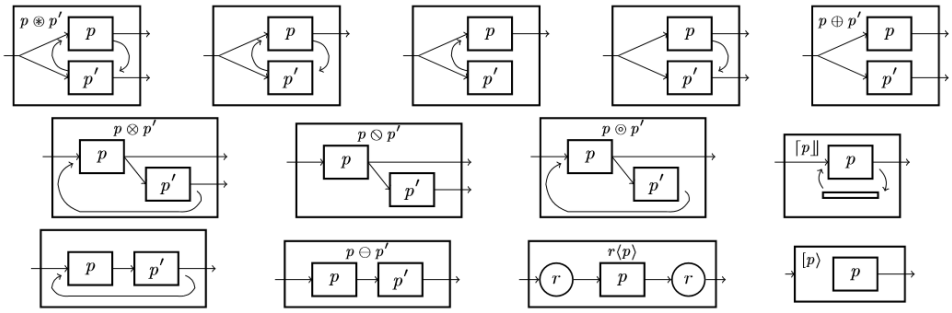
$$\frac{p_L \xrightarrow{o} p'_L \quad p_R \xrightarrow{o^{-1}} p'_R}{p_L \circledast p_R \xrightarrow{o} p'_L \circledast p'_R}\circledast^{!}_{L} \qquad \frac{p_R \xrightarrow{o} p'_R \quad p_L \xrightarrow{o^{-1}} p'_L}{p_L \circledast p_R \xrightarrow{o} p'_L \circledast p'_R}\circledast^{!}_{R}$$

$$\frac{p_L \xrightarrow{i} p'_L \quad p_R \xrightarrow{i} p'_R}{p_L \circledast p_R \xrightarrow{i} p'_L \circledast p'_R}\circledast^{?}$$

2. *router*

$$\frac{p \xrightarrow{r(i)} p'}{r\langle p \rangle \xrightarrow{i} r\langle p' \rangle}\langle\rangle^{?} \qquad \frac{p \xrightarrow{o} p'}{r\langle p \rangle \xrightarrow{r(o)} r\langle p' \rangle}\langle\rangle^{!}$$

Theorem 2. $p_L, p_R \in \text{PSNI} \Rightarrow p_L \circledast p_R \in \text{PSNI}$.
Corollary 1. $p_L, p_R \in \text{PINI} \Rightarrow p_L \circledast p_R \in \text{PINI}$.
Corollary 2. $p \in \text{PSNI} \Rightarrow r\langle p \rangle \in \text{PSNI}$ *for secure* r.
Corollary 3. $p \in \text{PINI} \Rightarrow r\langle p \rangle \in \text{PINI}$ *for secure* r.



4.3 Other combinators

$p \circledast p'$, $p \oslash p'$, $p \ominus p'$, $p \boxdot p'$, $p \circledcirc p'$, $\cdots$.
All can be represented by combining *and* and *router* combinators.

Corollary 4. For each binary combinator $\odot$, $p_L, p_R \in \text{PINI} \Rightarrow p_L \odot p_R \in \text{PINI}$, $p_L, p_R \in \text{PSNI} \Rightarrow p_L \odot p_R \in \text{PSNI}$.