Secure information flow for concurrent processes

Jan Jürjens

LFCS, University of Edinburgh

(this research performed at Kestrel Institute, Palo Alto)

(currently at Bell Labs (Lucent), Palo Alto)

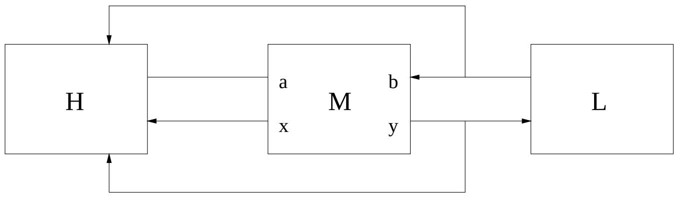
(moving to Computing Laboratory, University of Oxford)

Problem

Untrusted H (post-issuance download on multi-app smartcard, off-the shelf component, . . . possibly Trojan Horse) accesses confidential data.

Prevent H from sending data to L (e. g. Internet).

M (operating system (TCB), browser, . . .) should prevent information flow from H to L.



Subtlety

Covert channels (Butler Lampson 73):

E.g., send information from H through M to L by increased use of common resources at certain times

Dean e.a. 98: covert channels in web browsers

Background

Bell, LaPadula 75 does not treat covert channels.

Thus Noninterference (Goguen, Meseguer 82) for deterministic systems: L cannot distinguish different behaviours of H.

Nondeterministic systems: Nondeducibility-on-Strategies (Wittbold, Johnson 90). Attacks using statistical inference.

Probabilistic: Applied Flow Model (McLean 90, Gray 92), Probabilistic Noninterference (Gray 92).

Nonprobabilistic notions using process algebras (Ryan 90, Focardi/Gorrieri 94, Roscoe/Woodcock/Wulf 94, . . .).

Present work

Simplified verification of probabilistic secure information flow.

Note weakness of Applied Flow Model.

Prove results towards feasible verification of PNI:

- Determinism Theorem
- Compositionality (open in Gray 92),
  using rely/guarantee principle
- relation to Nondeducibility-on-Strategies

Why Probability ?

System M:

- receives high value a.
- with probability 1/2, M outputs a to Low,
- with probability 1/2, M outputs random value to Low.

Then

- M secure in nonprobabilistic models (that allow nondeterminism visible to L),
- covert channel from High to Low using statistical inference.

System Model: Probabilistic Dataflow

probabilistic vs. of I/O systems (Jonsson)

- concurrent probabilistic processes
- transmit data values over unidirectional FIFO channels
- communication asynchronous

Consider systems (security to be examined) and environments

Processes: Systems and Environments

$\mathcal{E}_C$ set of events $o : C \to \mathcal{D}$ (C channels, $\mathcal{D}$ data values)

For system M (I, O input, output channels), environment E:
- $\mathcal{E}^M := (\mathcal{E}_O \times \mathcal{E}_I)^*$ (system histories)
- $\mathcal{E}^E := \mathcal{E}_O \times (\mathcal{E}_I \times \mathcal{E}_O)^*$ (environment histories)

System: $M = (I, O, P_M)$, $P_M : \mathcal{E}_O \times \mathcal{E}^M \to [0, 1]$

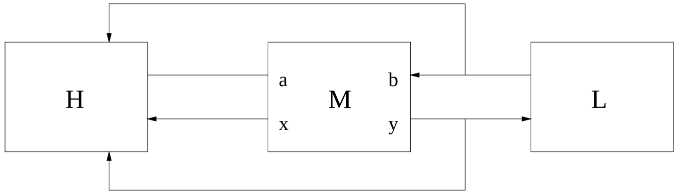
Environment: $E = (O, I, P_E)$, $P_E : \mathcal{E}_I \times \mathcal{E}^E \to [0, 1]$

For each w, $\sum_o P(o, w) = 1$.
$P(o \mid w) \stackrel{\text{def}}{=} P(o, w)$ (probability of value o after history w).

Processes: High and Low

Environment: independent components H (high) and L (low).
H can read low outputs.

$M = (I, O, P_M((x,y) \mid w))$ $(w \in \mathcal{E}^M)$,
$L = (O_l, I_l, P_L(b \mid w\lfloor_l))$
    ($w\lfloor_l$ restriction of $w \in \mathcal{E}^{H,L}$ to low channels)
$H = (O \cup I_l, I_h, P_H(a \mid w))$ $(w \in \mathcal{E}^{H,L})$.



1) Applied Flow Model

Definition: A system M satisfies Applied Flow Model (AFM) if for all traces w, w' identical wrt. the low input and output, and for all low outputs y,

$$\sum_x P_M((x,y) \mid w) = \sum_x P_M((x,y) \mid w').$$

Simple but too strict (Gray 92).

Applied Flow Model: Subtlety

Worse: against common sense:

System S:

random number generator R outputs r to

- high output of S and to
- delay component D.

D outputs r after one time step at low output of S.

S secure: H has no way of influencing the low output of S.

S does not satisfy AFM.

However, if substitute D by wire (so L gets r earlier), get system that does satisfy AFM ! Unrealistic since L has state.

2) Weak AFM

Definition: A process M fulfils weak AFM
if for all possible traces w and w' that are
identical wrt. the low input and output and the high output,
and all low-level output events y,

$$\sum_x P_M((x,y) \mid w) = \sum_x P_M((x,y) \mid w').$$

Weak AFM: Subtlety

Also too strict:
Let M output $x_1 = 0$ resp. $x_1 = 1$ each with probability 1/2 to H, and $y_1 = 0$ to L.
On input of a_1 (resp. b_1) from H (resp. L) M outputs $x_2 = 0$ to H and y_2 to L:
$x_1 = 0$: $y_2 := a_1$ resp. $\neg a_1$ with probability 1/4 resp. 3/4
$x_1 = 1$: $y_2 := \neg a_1$ resp. a_1 with probability 1/4 resp. 3/4

M secure, because independently of H, L receives 0 and 1 each with probability 1/2.
But M does not satisfy weak AFM:
$P(a_1 \mid (a_1, x_1 = 0)) = 1/4 \neq 3/4 = P(a_1 \mid (\neg a_1, x_1 = 0))$.

Probabilistic Noninterference

Probability of history $w \in \mathcal{E}^M$ by $P^M_{H,L}(\varepsilon) \stackrel{\text{def}}{=} 1$,

$$P^M_{H,L}(w.(x,y).(a,b)) \stackrel{\text{def}}{=}$$
$$P^M_{H,L}(w) \cdot P_M((x,y) \mid w) \cdot P_H(a \mid w.(x,y)) \cdot P_L(b \mid w\downharpoonright_l .y)$$

Probability of low history w_l: $P^l_{H,L}(w_l) \stackrel{\text{def}}{=} \sum_{w : w\downharpoonright_l = w_l} P_{H,L}(w)$

Definition: System M satisfies Probabilistic Noninterference (PNI) if for all H, H', L and low histories w_l

$$P_{H,L}(w_l) = P_{H',L}(w_l).$$

M satisfies PNI $\Rightarrow$ communication channel from H to L has capacity zero (Gray 92).

Deterministic Adversaries suffice

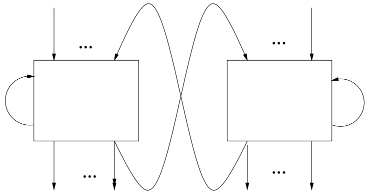
Process (I, O, P) is deterministic if for all w, o have $P(o \mid w) \in \{0, 1\}$.

Determinism Theorem: A system M satisfies Probabilistic Noninterference iff for all deterministic H, H', L and for all low system histories w_l we have

$$P_{H,L}(w_l) = P_{H',L}(w_l).$$

Composition

Define composition $M \otimes N$ of systems M, N with $O_M \cap O_N = \emptyset$:



- $O_{M\otimes N} = O_M \cup O_N$
- $I_{M\otimes N} = I_M \cup I_N \setminus O_{M\otimes N}$

- $P^{M\otimes N}(o \otimes p | v \otimes w) = P^M(o|v) \cdot P^N(p|w)$ for *compatible* v, w

For output events $e : O_M \to \mathcal{D}$, $f : O_N :\to \mathcal{D}$: $e \otimes f \stackrel{\text{def}}{=} (e \cup f)$,

for input events $e : I_M \to \mathcal{D}$, $f : I_N :\to \mathcal{D}$: $e \otimes f \stackrel{\text{def}}{=} (e \cup f) \restriction_{I_{M\otimes N}}$,

for histories v, w: $(v_1, \ldots, v_t) \otimes (w_1, \ldots, w_t) \stackrel{\text{def}}{=} (v_1 \otimes w_1, \ldots, v_t \otimes w_t)$.
Histories v, w are compatible if outputs match with inputs at corresponding channels at following time step.

Compositionality: Subtlety

Example: M, channels A_1, A_2 (high input), X (high output), Y (low output).
Time 1: M inputs bits a_1 on A_1, a_2 on A_2, outputs random bit x on X.
Time 2: M outputs $y := a_1 \oplus a_2 \oplus x$ on Y ($\oplus$: exclusive or).

In Gray's model, M secure since $a_1 \oplus a_2$ independent from x, so y is 0 or 1 each with probability 1/2 independent of H.
But feedback of X into A_2 not secure: takes a value a_1 on A_1 at time 1 and outputs a_1 at time 2.

Our model allows environment's output to depend on input at same time (rushing adversary, B. Pfitzmann).

Thus M is correctly insecure.

Compositionality Theorem

Theorem: If M and N satisfy PNI, so does $M \otimes N$.

Proof uses rely-guarantee principle (inspired by Abadi, Lamport's which does not apply here (McLean 94)).

Inductive Compositionality: Setting

$\mathcal{S}$ set of "systems", $\mathcal{E}$ of "environments"; $\mathcal{S} \subseteq \mathcal{E}$.

$\otimes$ binary composition on $\mathcal{E}$ restricting to $\mathcal{S}$.

For each $t \in \mathbb{N}_{\geq 0}$ have properties $\phi_t \subseteq \mathcal{E}$ and $\sigma_t \subseteq \mathcal{S} \times \mathcal{E}$ with $\phi_0 = \mathcal{E}$, $\sigma_0 = \mathcal{S} \times \mathcal{E}$.

If $(M, E) \in \sigma_t$ say M guarantees σ_t in E.

If M guarantees σ_t in any E satisfying ϕ_s say M guarantees σ_t assuming ϕ_s.

Write ϕ for $\bigwedge_t \phi_t$ and σ for $\bigwedge_t \sigma_t$.

Suppose if M guarantees σ_{t+1} assuming ϕ_{t+1}, then M guarantees σ_t assuming ϕ_t (each t, M).

Also M guarantees σ assuming ϕ iff for all t, M guarantees σ_t assuming ϕ_t.

Inductive Compositionality: Result

Suppose that for each t:

a) For any E, if E satisfies ϕ_{t+1} and M guarantees σ_t assuming ϕ_t and "guarantee σ_t assuming ϕ_t" is compositional, then $E \otimes M$ satisfies ϕ_{t+1}.

b) For all E, M_1, M_2: $M_1 \otimes M_2$ guarantees σ_t in E if

- M_1 guarantees σ_t in $E \otimes M_2$ and
- M_2 guarantees σ_t in $E \otimes M_1$.

If M_1 and M_2 guarantee σ assuming ϕ then $M_1 \otimes M_2$ guarantees σ assuming ϕ.

Nondeducibility-on-Strategies

Nonprobabilistic process $(I, O, \mathcal{H})$: $\mathcal{H}$ set of histories.

Strategy π for H assigns high input $a = \pi(w)$ to history $w \in \mathcal{E}_E$.

History $(x_1, y_1), (a_1, b_1,), \ldots, (a_t, b_t)$ compatible with strategy π if for each $s \leq t$, $\pi((x_1, y_1), (a_1, b_1,), \ldots, (x_s, y_s)) = a_s$.

Low history w_l compatible with π if exists history w with $w\lfloor_l = w_l$ such that w compatible with π.

w_l possible if exists strategy with which compatible.

Definition: M satisfies Nondeducibility-on-Strategies if for any π and any possible low history w_l there is a w compatible with π such that $w\lfloor_l = w_l$.

Probabilistic vs. Possibilistic: Embedding

For possibilistic M construct probabilistic $\widehat{M}$:
uniform distribution on possible outputs.

From probabilistic system M construct possibilistic system $|M|$:
history possible if has nonzero probability.

Theorem

a) Possibilistic M satisfies NOS iff $\widehat{M}$ satisfies PNI.

b) If probabilistic M satisfies PNI then $|M|$ satisfies NOS.

(Proof: uses Determinism Theorem.)

Related Work

Nonprobabilistic noninterference using process algebras:

CSP: translation of noninterference not suitable for FDR, also “refinement paradox”. Thus “noninterference through determinism” (Roscoe, Woodcock, Wulf 95).
But too restrictive (Lowe 99, Mislove 00).

CCS: reformulation of NOS called BNDC (Focardi, Gorrieri 94).
Under suitable conditions equivalent to “determinism” approach.

Bi-directional “handshake” communication subtle: low behaviour may interfere with high behaviour, but not other way (Roscoe, Goldsmith 99)

Conclusion

Towards practical verification of Probabilistic Noninterference:

- Determinism Theorem
- Compositionality (using Inductive Compositionality Principle)
- relation to Nondeducibility-on-Strategies.

Further Work

expressed PNI using discrete Markov chains (probabilistic modelchecking, Kwiatkowska) using coinductive definition.

wrapper (Sewell, Vitek), derive overall "leakage"

nondeterminism, refinement