Confinement Properties for Multi-Threaded Programs

Geoffrey Smith
School of Computer Science
Florida International University
Miami, FL 33199, USA
smithg@cs.fiu.edu

Dennis Volpano
Computer Science Department
Naval Postgraduate School
Monterey, CA 93943, USA
volpano@cs.nps.navy.mil

Abstract
Given a program that has access to some private information, how can we ensure that it does not improperly leak the information? We formalize the desired security property as a property called noninterference. We discuss versions of noninterference appropriate for multi-threaded programs with probabilistic scheduling and describe rules for ensuring noninterference.

1 Introduction
Ensuring the privacy of information is a major problem today, made both more pressing and more difficult by the enormous growth of the Internet. In this paper, we address one aspect of this problem: given a program $P$ that has access to some private information, how can we prevent $P$ from leaking the information? (This problem was called the confinement problem by Lamport [6], who first raised the issue in the early 1970s.) We will focus in particular on the case when $P$ is multi-threaded.

The difficulty of preventing a program $P$ from leaking private information depends greatly on what kinds of observations of $P$ are possible. If we can

---

1 This material is based upon activities supported by the National Science Foundation under Agreements Number CCR-9612176 and CCR-9612345.

©1999 Published by Elsevier Science B.V.
**Confinement Properties for Multi-Threaded Programs**

School of Computer Science Florida International University Miami, FL 33199

Approved for public release, distribution unlimited

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
<td>UU</td>
<td>11</td>
<td></td>
</tr>
</tbody>
</table>
make external observations of \( P \)'s running time, memory usage, and so forth, then preventing leaks becomes very difficult. For example, \( P \) could modulate its running time in order to encode the private information. Furthermore, these modulations might depend on low-level implementation details, such as paging and caching behavior. But this means that it is insufficient to prove confinement with respect to an abstract semantics—every implementation detail that affects running time must be addressed in the proof of confinement. For this reason, we will not consider such external observations further.

If, instead, we can only make internal observations of \( P \)'s behavior, the confinement problem becomes more tractable. Internal observations include the values of program variables, together with any system-provided functions that can be called by \( P \). Of course, if the system provides a real-time clock, then running time is observable internally, and we are no better off than before. But in this case we can design the system with confinement in mind, excluding features (like real-time clocks) that are problematic. This situation is relevant to the case of mobile code, which runs under the control of a host machine that can limit what the code can observe.

When only internal observations are possible, we can formulate the confinement problem as follows [1,2]: if each program variable is classified as \( L \) (low, public) or \( H \) (high, private), then we wish to ensure that information cannot flow from \( H \) variables to \( L \) variables.

For example, Figure 1 suggests the behavior of a tax return applet which could be downloaded from a site called TrustMe. The applet runs on my machine, allowing me to complete my tax return. When I finish, the applet sends the completed tax return to the IRS and sends billing information back to TrustMe, using encryption to protect the privacy of these communications.
But how do I know that my private financial information is not somehow encoded in the billing information sent back to TrustMe? If I classify the tax return as $H$ and the billing information as $L$, then I would like to know that no information can flow from $H$ variables to $L$ variables.

2 Possibilistic Noninterference

Formally, we want programs to satisfy a property called noninterference [10], which says that the final values of $L$ variables don’t depend on the initial values of $H$ variables. In the case when programs are multi-threaded, and hence nondeterministic, we need a possibilistic noninterference property [8], which says that changing the initial values of $H$ variables cannot change the set of possible final values of $L$ variables.

Here’s a non-example, similar to one in [8]. Suppose $x$ is $H$, with value 0 or 1, and $y$ is $L$. Also, assume that $t$ is initially 0. Consider the following program, which consists of two threads:

Thread $\alpha$: \(\text{if } x = 1 \text{ then}
\begin{align*}
\text{while } t = 0 \text{ do } & \text{skip;} \\
y & := 1; \\
t & := 1
\end{align*}
\)

Thread $\beta$: \(\text{if } x = 0 \text{ then}
\begin{align*}
\text{while } t = 0 \text{ do } & \text{skip;} \\
y & := 0; \\
t & := 1
\end{align*}
\)

Note that thread $\alpha$ always assigns 1 to $y$, and thread $\beta$ always assigns 0 to $y$, but the order in which these assignments are done depends on the value of $x$. As a result, with any fair scheduler the value of $x$ is copied to $y$.

Suppose that we adopt a formal semantics for our multi-threaded language that specifies a purely nondeterministic scheduler. Such a scheduler is characterized by the simple rule:

At each step, any thread can be selected to run for a step.

Suppose that we prove that a program $P$ satisfies possibilistic noninterference with respect to this scheduler. Can we conclude that $P$ remains secure if we implement something more deterministic, such as round-robin time slicing?

The answer is no. For suppose that $x$ is $H$, with value 0 or 1, $y$ is $L$, and $c$ is a command that doesn’t alter $x$ or $y$, but that takes longer than a time slice. Consider the following program:

Thread $\alpha$: \(\text{if } x = 1 \text{ then } (c; c); \\
y := 1
\)

Thread $\beta$: \(c; \\
y := 0\)
With respect to the purely nondeterministic scheduler, this program satisfies
possibilistic noninterference: regardless of the initial value of \( x \), the final value
of \( y \) can be either 0 or 1. But under round-robin time slicing, the value of
\( x \) is always copied to \( y \). Thus we see that noninterference is not a safety
property—it is not closed under trace subsetting.

3 Probabilistic Noninterference

A purely nondeterministic scheduler is convenient in a formal semantics, but
it is unclear how such a scheduler might be implemented; it seems to require
an “erratic daemon”.\(^2\)

We might consider a probabilistic implementation that flips coins to select
the thread to run in the next step. But note that this moves us from a nonde-
terministic semantics, in which events are either possible or impossible, to a
probabilistic semantics, in which events have a probability of occurring. Still,
we can say that this gives an implementation of the purely nondeterministic
scheduler, if we are willing to equate “possible” with “occurs with nonzero
probability”.

But now suppose that \( x \) is \( H \), with value between 1 and 100, and \( y \) is
\( L \). Suppose that \( \text{random}(100) \) returns a random number between 1 and 100.
Consider the following program:

Thread \( \alpha \):
\[
y := x
\]

Thread \( \beta \):
\[
y := \text{random}(100)
\]

This program satisfies possibilistic noninterference: regardless of the initial
value of \( x \), the final value of \( y \) can be any number between 1 and 100. But
with a probabilistic semantics, this is not good enough, because the final values
of \( y \) are not equally likely. In particular, if we can run the program repeatedly,
we expect the final values of \( y \) to look something like

\[
75, 22, 12, 22, 22, 93, 4, 22, \ldots
\]

allowing us to conclude (in this case) that \( x \) is probably 22. Thus we see that
possibilistic noninterference is not sufficient to prevent probabilistic informa-
tion flows.\(^3\) Instead, we now need a probabilistic noninterference property,
which says that changing the initial values of \( H \) variables cannot change the
joint distribution of possible final values of \( L \) variables [9]. In the next section,
we develop this idea more formally.

---

\(^2\) The term is due to Dijkstra [3].

\(^3\) This observation can be credited to McLean [7] and Wittbold and Johnson [11].
4 Multi-Threaded Programs as Markov Chains

We assume that threads are written in a simple imperative language:

\[ c ::= \text{skip} \]
\[ \mid x ::= e \]
\[ \mid c_1 ; c_2 \]
\[ \mid \text{if } e \text{ then } c_1 \text{ else } c_2 \]
\[ \mid \text{while } e \text{ do } c \]

Integers are the only values; we use 0 for false and nonzero for true. We assume that all expressions are pure and total, and that expressions are executed atomically.

Programs are executed with respect to a single shared memory \( \mu \), which is a map from identifiers to integers. We extend this to a map from expressions to integers, writing \( \mu(e) \) to denote the value of expression \( e \) in memory \( \mu \).

The semantics of commands is given by a standard transition semantics \( \rightarrow \) on configurations \( (c, \mu) \) or \( \mu \). The rules are given in Figure 2.

A multi-threaded program is modeled by an object map \( O \) that maps thread identifiers \( (\alpha, \beta, \ldots) \) to commands. The semantics of multi-threaded programs is given via global transitions \( \xrightarrow{p} \) on global configurations \( (O, \mu) \). The three rules are

\[
\text{(global)} \quad O(\alpha) = c \\
(c, \mu) \xrightarrow{} \mu' \\
p = \frac{1}{|O|} \\
(O, \mu) \xrightarrow{p} (O - \alpha, \mu')
\]

\[
O(\alpha) = c \\
(c, \mu) \xrightarrow{} (c', \mu') \\
p = \frac{1}{|O|} \\
(O, \mu) \xrightarrow{p} (O[\alpha := c'], \mu')
\]

\[
(\{ \}, \mu) \xrightarrow{} (\{ \}, \mu)
\]

The first and second rules deal with a nonempty set of threads; the third deals with an empty set of threads. Note that we are assuming a uniform scheduler, that selects each thread in \( O \) with equal probability.

With these definitions, a program \( O \) executing in memory \( \mu \) is a Markov chain [4]. The states of the Markov chain are all the global configurations reachable from the initial state \( (O, \mu) \) under \( \xrightarrow{p} \), and the transition matrix \( T \)
is given by

\[ T([(O_1, \mu_1), (O_2, \mu_2)]) = \begin{cases} 
  p, & \text{if } (O_1, \mu_1) \xrightarrow{\mu} (O_2, \mu_2) \\
  0, & \text{otherwise}
\end{cases} \]

It is now useful to define a \textit{probabilistic state} \( u \) to be a (discrete) probability distribution on the set of global configurations [5]. Concretely, \( u \) is a row vector with unit sum. With this viewpoint, we can model the execution of \( O \) under memory \( \mu \) as a \textit{deterministic} sequence of probabilistic states:

\[ u_0, u_1, u_2, u_3, \ldots \]

where \( u_0 \) is the distribution that assigns probability 1 to \((O, \mu)\) and 0 to all other configurations, and \( u_{k+1} = u_k T \). We can now write a very simple expression for the \( k \)th probabilistic state: \( u_k = u_0 T^k \).
For example, consider the program

\[
O = \left\{ \begin{array}{l}
\alpha : \text{while } l = 0 \text{ do skip} \\
\beta : l := 1
\end{array} \right\}
\]

executed in a memory that sets \( l \) to 0 initially. There are a total of five reachable states in the Markov chain:

\[
q_1 : \left( \left\{ \begin{array}{l}
\alpha : \text{while } l = 0 \text{ do skip} \\
\beta : (l := 1)
\end{array} \right\}, [l := 0] \right)
\]

\[
q_2 : (\{ \alpha : \text{while } l = 0 \text{ do skip} \}, [l := 1])
\]

\[
q_3 : \left( \left\{ \begin{array}{l}
\alpha : \text{skip; while } l = 0 \text{ do skip} \\
\beta : (l := 1)
\end{array} \right\}, [l := 0] \right)
\]

\[
q_4 : (\{ \alpha : \text{skip; while } l = 0 \text{ do skip} \}, [l := 1])
\]

\[
q_5 : (\{ \}, [l := 1])
\]

The transition matrix \( T \) for this program is as follows:

<table>
<thead>
<tr>
<th></th>
<th>( q_1 )</th>
<th>( q_2 )</th>
<th>( q_3 )</th>
<th>( q_4 )</th>
<th>( q_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q_1 )</td>
<td>0</td>
<td>1/2</td>
<td>1/2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( q_2 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( q_3 )</td>
<td>1/2</td>
<td>0</td>
<td>0</td>
<td>1/2</td>
<td>0</td>
</tr>
<tr>
<td>( q_4 )</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( q_5 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

For instance, we get the first row of \( T \) by noting that running thread \( \alpha \) from state \( q_1 \) takes us to state \( q_3 \), and running thread \( \beta \) takes us to state \( q_2 \). Thus, under our uniform scheduling assumption, we go from \( q_1 \) either to \( q_2 \) or to \( q_3 \), each with probability \( 1/2 \).
In terms of probabilistic states, the initial distribution \( u_0 \) is \( (1 \ 0 \ 0 \ 0 \ 0) \). And we can trace the probabilistic states that \( O \) passes through:

<table>
<thead>
<tr>
<th></th>
<th>( q_1 )</th>
<th>( q_2 )</th>
<th>( q_3 )</th>
<th>( q_4 )</th>
<th>( q_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_0 )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_0T )</td>
<td>0</td>
<td>1/2</td>
<td>1/2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( u_0T^2 )</td>
<td>1/4</td>
<td>0</td>
<td>0</td>
<td>1/4</td>
<td>1/2</td>
</tr>
<tr>
<td>( u_0T^3 )</td>
<td>0</td>
<td>3/8</td>
<td>1/8</td>
<td>0</td>
<td>1/2</td>
</tr>
<tr>
<td>( u_0T^4 )</td>
<td>1/16</td>
<td>0</td>
<td>0</td>
<td>1/16</td>
<td>7/8</td>
</tr>
<tr>
<td>( u_0T^5 )</td>
<td>0</td>
<td>3/32</td>
<td>1/32</td>
<td>0</td>
<td>7/8</td>
</tr>
<tr>
<td>( u_0T^6 )</td>
<td>1/64</td>
<td>0</td>
<td>0</td>
<td>1/64</td>
<td>31/32</td>
</tr>
</tbody>
</table>

Of course, \( O \) will converge to the probabilistic state \((0 \ 0 \ 0 \ 0 \ 1)\).

Now, to formalize the probabilistic noninterference property, we need to define a notion of equivalence on probabilistic states. To this end, we say that probabilistic states \( u \) and \( u' \) are equivalent, written \( u \sim u' \), if they are equal after \( H \) variables are projected out. Intuitively, \( u \) and \( u' \) agree about everything except the values of \( H \) variables. For example, if \( x \) is \( H \) and \( y \) is \( L \), then

\[
\begin{align*}
\{ (O, [x := 0, y := 0]) : 1/2, \\
(O, [x := 1, y := 0]) : 1/2
\end{align*}
\]

is equivalent to

\[\{ (O, [x := 2, y := 0]) : 1 \},\]

since in both cases the result of projecting out \( x \) is

\[\{ (O, [y := 0]) : 1 \} .\]

Finally, we can give the formal definition of probabilistic noninterference:

**Definition 4.1** Program \( O \) satisfies probabilistic noninterference if for all probabilistic states \( u \) and \( u' \), \( u \sim u' \) implies \( uT \sim u'T \).

This definition gives us what we want, for suppose that we execute a program \( O \) under two memories \( \mu \) and \( \mu' \) that agree on the values of \( L \) variables. Then

\[\{ (O, \mu) : 1 \} \sim \{ (O, \mu') : 1 \}\]

and hence

\[\{ (O, \mu) : 1 \} T^k \sim \{ (O, \mu') : 1 \} T^k \]

for all \( k \). That is, the two executions proceed in probabilistic lockstep.
5 Ensuring Probabilistic Noninterference

We can perform a static analysis that ensures that a program $O$ satisfies probabilistic noninterference. The analysis is described formally (as a type system) in [9]; here we give an intuitive presentation as a set of rules. The rules impose constraints on assignments, while loops, and if statements:

- For an assignment, $y := e$, the rule is that if $y$ is $L$, then $e$ must contain no $H$ variables.
- For a while loop, while $e$ do $c$, the rule is that $e$ must contain no $H$ variables.
- For an if statement, if $e$ then $c$ else $c'$, the rule is that if $e$ contains any $H$ variables, then
  
  (i) $c$ and $c'$ must contain no assignments to $L$ variables,
  
  (ii) $c$ and $c'$ must contain no while loops, and
  
  (iii) the entire if statement must be protected, so that it executes atomically.

For the last rule, we introduce a new command, protect $c$, whose semantics is given by

$$
\frac{
(c, \mu) \rightarrow^* \mu'
}{
(\text{protect } c, \mu) \rightarrow \mu'
}
$$

That is, if $(c, \mu)$ can reach $\mu'$ in one or more steps, then $(\text{protect } c, \mu)$ can reach $\mu'$ in exactly one step.

Applying these rules to the first program of Section 2, we see that the program is illegal, because both threads have while loops within the bodies of if statements whose guards are $H$. And for the second program of Section 2 to be legal, the if statement of thread $\alpha$ needs to be protected; this will mask the amount of time needed to execute it, thereby eliminating the timing channel. Of course, our rules are necessarily conservative. More experience is needed to determine how burdensome they are in practice.

It can be shown that any program $O$ that satisfies the above rules satisfies probabilistic noninterference. Details can be found in [9]; here we sketch part of the argument.

First, we can show probabilistic noninterference for point masses; that is, for distributions in which some configuration has probability 1 and all others have probability 0:

**Theorem 5.1** If $O$ satisfies the above rules and $\iota \sim \iota'$, where $\iota$ and $\iota'$ are point masses, then $\iota T \sim \iota' T$.

Then we can extend the result to arbitrary distributions by exploiting the linearity of $T$:

**Lemma 5.2** If $u_i \sim u_i'$, for all $i$, then

$$a_1 u_1 + a_2 u_2 + \cdots \sim a_1 u_1' + a_2 u_2' + \cdots$$
Lemma 5.3 If \( u \sim u' \), then there exist coefficients \( c_1, c_2, c_3, \ldots \) and point masses \( t_1, t_2, t_3, \ldots \) and \( t_1', t_2', t_3', \ldots \) with \( t_i \sim t_i' \) for all \( i \), such that

\[
u = c_1 t_1 + c_2 t_2 + c_3 t_3 + \cdots\]

and

\[
u' = c_1 t_1' + c_2 t_2' + c_3 t_3' + \cdots\]

Corollary 5.4 If \( O \) satisfies the above rules and \( u \sim u' \), then \( uT \sim u'T \).

Proof. Since \( T \) is a continuous linear transformation,

\[
u T = (c_1 t_1 + c_2 t_2 + c_3 t_3 + \cdots)T = c_1 (t_1 T) + c_2 (t_2 T) + c_3 (t_3 T) + \cdots \sim (c_1 t_1' T) + c_2 (t_2' T) + c_3 (t_3' T) + \cdots = (c_1 t_1' + c_2 t_2' + c_3 t_3') T = u' T \]

\[\Box\]

6 Conclusion

To develop secure computer systems, it is first necessary to identify the precise security properties of interest. We have presented one such property, probabilistic noninterference, aimed at protecting information privacy and we have described rules sufficient to guarantee it; our hope is that such rules provide a basis for constructing provably-secure systems in practice.

References


