Analysis of security properties

MPRI — Cours 2.6 “Interprétation abstraite : application à la vérification et à l’analyse statique”

Xavier Rival

INRIA

Feb, 13th, 2023
Security

What does “security” mean?

There are many examples of “potential security issues”:

- **Leakage of sensitive information:**
  an unauthorized user is able to retrieve or even just guess critical information

- **Code injection:**
  a user succeeds in getting malicious code executed with a high privilege (and can corrupt data or take control of the system)

- **Authentication breach:**
  a malicious user pretends to be another user

“Security” is a rather general and vague term. We need to be more specific on what it means.

**Rough intuition** (that we will formalize):

- **safety issue**, e.g., runtime error: failure in presence of just the environment

- **security issue**: failure resulting from (malicious) deliberate user action
Objectives of this course

1. **Understand the difficulty inherent in security properties:**
   In general, security properties are significantly harder to reason about than safety properties.

2. **Introduce hyperproperties:**
   A *more general framework* than the trace properties we are used to, which can express many relevant program properties.

3. **Describe a few abstractions for security:**
   - extension of abstractions for safety
   - specific abstractions

In one class, we can only provide an introduction to the field. Our goal is to understand the main problems.
Outline

1. Introduction
2. Non-interference
3. Specificities of security properties
4. Hyperproperties
5. Dependence analysis for non-interference
6. Relational reasoning over non-interference
7. Conclusion
Notations

We focus on imperative programs viewed as transition systems:

- set of control states: $\mathbb{L}$ (program points)
- set of variables: $\mathbb{X}$ (all assumed globals)
- set of values: $\mathbb{V}$
- set of memory states: $\mathbb{M}$
- set of states: $\mathbb{S} = \mathbb{L} \times \mathbb{M}$ and initial states $\mathbb{S}_i \subseteq \mathbb{S}$
- transition relation: $(\rightarrow) \subseteq \mathbb{S} \times \mathbb{S}$, assumed deterministic

Semantics:

- reachable states: $\llbracket P \rrbracket_{\mathcal{R}} \subseteq \mathbb{S}$
- finite execution traces: $\llbracket P \rrbracket_{\mathcal{T}^*} \subseteq \mathbb{S}^*$
- denotational semantics: $\llbracket P \rrbracket_{\mathcal{F}} : \mathbb{S} \longrightarrow \mathcal{P}(\mathbb{S})$
  where $\llbracket P \rrbracket_{\mathcal{F}}(\sigma) = \{ \sigma' \in \mathbb{S} \mid \sigma \rightarrow^* \sigma' \}$

Given $\ell, \ell' \in \mathbb{L}$, we also let $\llbracket P \rrbracket_{\mathcal{F}[\ell,\ell']} : \mathbb{M} \longrightarrow \mathcal{P}(\mathbb{M})$ be defined by
$\llbracket P \rrbracket_{\mathcal{F}[\ell,\ell']}(m) = \{ m' \in \mathbb{M} \mid (\ell, m) \rightarrow^* (\ell', m') \}$.

For us today, most of the time we use the denotational semantics.
Non-interference

Among the many possible security properties, we choose one, that is very representative.

It describes the fact that some secret information should not be guessed (directly or indirectly) by any unauthorized user.

Non-interference (informal definition)

Notations: $X = X_{\text{pub}} \cup X_{\text{sec}}$ where,

- $X_{\text{pub}}$: public variables, observed by anybody
  (also called “low”, i.e., it requires only a low authorization)

- $X_{\text{sec}}$: secrete variables, should not be observed by anybody, save authorized users (also called “high”, i.e., high authorization)

We say that a program $P$ satisfies the non-interference property defined by $X_{\text{pub}}, X_{\text{sec}}$ if and only if any execution of the program where one can only observe the values of the variables in $X_{\text{pub}}$ does not allow to derive any information about the values of the variables in $X_{\text{sec}}$.

This definition is quite informal, and we will make it precise and formal soon.
Example of program violating non-interference

Let us consider the program below:

```c
int s; // private variable, should be secure
int i; // public variable, can be seen by anybody

s = private_computation(); // should remain secret

i = s + 8;
// anyone can observe i here!
```

We should let:

- $X_{pub} = \{i\}$
- $X_{sec} = \{s\}$ (for readability we will write $s$ for the private variable that should remain secure)

This program clearly violates non-interference.

If we know the final value of $i$ we can subtract 8 and derive the value of $s$. 
Example of program satisfying non-interference

We now consider the program below, with the same $X_{\text{pub}}, X_{\text{sec}}$:

```c
int s; // private variable, should be secure
int i; // public variable, can be seen by anybody

s = private_computation( ); // should remain secret

i = user_input( ) + 8;
// anyone can observe i here!
```

This program satisfies non-interference.

The final value of $i$ is computed in a way that is never influenced by that of $s$ (the user input ignores the value of $s$ at this point).
A few more subtle cases

We use the **same conventions** (with variables \( i, s \)).

**Program 1**: non-interference **violated**

```c
// ... as before, \( s \) stores the secret
if ( s == 7 )
   i = 1;
else
   i = -1;
```

There is an **implicit information flow**. If we observe that \( i \) is 1, we know exactly what \( s \) is.

**Program 2**: non-interference **violated**

```c
s = 8 / s;
i = 5;
```

Again, there is an **implicit information flow**. If we observe a crash (no value for \( i \)), we know that \( s = 0 \).

**Program 3**: non-interference **satisfied**

```c
i = 0 * s;
```

There is **no information flow**. Indeed, \( i \) is 0 regardless...

In the following, we need to **formalize and characterize non-interference** before we can actually reason about it.
Non-interference

A couple of caveats:

- **termination** may change observation (though we cannot positively observe non-termination)
- **errors** may change observation too

For the sake of simplicity, we ignore these and consider **termination insensitive non-interference** and assume no error may arise and restrict to terminating executions.

In the following, we still call this notion **non-interference**.

**Observation point**: we search whether public variables observed at end point $l_\top$ reveal anything about private variables observed at entry point $l_\bot$.

**Non-interference (formal definition)**

We say that a program $P$ satisfies the **non-interference** property defined by $X_{\text{pub}}/l_\top, X_{\text{sec}}/l_\bot$ if and only if for all memory states $m_0, m_1 \in \mathcal{M}$,

\[
\left( \forall x \in X_{\text{pub}}, \ m_0(x) = m_1(x) \right) \implies \left( \forall x \in X_{\text{pub}}, \ \lceil P \rceil_{\mathcal{F}[l_\top, l_\bot]}(m_0)(x) = \lceil P \rceil_{\mathcal{F}[l_\bot, l_\top]}(m_1)(x) \right)
\]
Non-interference: about the definition

Non-interference (formal definition)

We say that a program $P$ satisfies the **non-interference** property defined by $\mathbf{X}_{\text{pub}} / \ell \vdash, \mathbf{X}_{\text{sec}} / \ell \dashv$ if and only if for all memory states $m_0, m_1 \in \mathbb{M}$,

\[
(\forall x \in \mathbf{X}_{\text{pub}}, \ m_0(x) = m_1(x)) \implies (\forall x \in \mathbf{X}_{\text{pub}}, \ \llbracket P \rrbracket_{\mathcal{F}[\ell \vdash, \ell \dashv]}(m_0)(x) = \llbracket P \rrbracket_{\mathcal{F}[\ell \vdash, \ell \dashv]}(m_1)(x))
\]

- **Non-determinism**: taken into account by the definition; $\llbracket P \rrbracket$ may return a set made of several elements

- **Non-termination**: when modifying the secret may change termination, non-interference may still hold provided the same set of possible terminating outputs can be observed... option: augment the semantics and return a special state/value $\omega$ in case of non-termination

- **Probabilistic behavior ignored**: would require considering distributions over states/values
Dependence

When non interference does not hold, we may also say there exists a dependence.

**Dependences** have **many applications** beyond security:

- program understanding and maintenance:
  explain how some specific variable is computed
  slicing tools

- split a program into several independent programs:
  e.g., for parallelization

(we do not discuss these today)
Outline

1. Introduction
2. Non-interference
3. Specificities of security properties
   - Properties as sets
   - Significant sets of properties
   - Non interference is not a trace property
4. Hyperproperties
5. Dependence analysis for non-interference
6. Relational reasoning over non-interference
7. Conclusion
Semantics

We have seen three semantics, that are comparable:

- **trace semantics** is the most precise and informative, i.e., the denotational semantics can be computed from it
- then **denotational semantics** is more precise than reachable states, i.e., the reachable states semantics can be computed from it

Before we formalize and study non-interference, we recall a few important points about trace properties.

To study hierarchies of properties, the most expressive semantics is more adapted.

Recall:

- **finite traces semantics** $[P]_{T^*} \subseteq S^*$
  expressed as a least fixpoint
- **infinite traces semantics** $[P]_{T^\omega} \subseteq S^\omega$
  expressed as a greatest fixpoint
- **all traces semantics** $[P]_{T^{*\omega}} \subseteq S^{*\omega} = S^* \cup S^\omega$
  ($[P]_{T^{*\omega}} = [P]_{T^*} \cup [P]_{T^\omega}$)
  can also be expressed as a fixpoint, by fixpoint combination technique
Semantic properties as sets of behaviors

We consider the following model:

- A semantic property is described by the set of behaviors that are compliant with.
- A program satisfies such a property if and only if all the behaviors of the program are compliant with the property, i.e., are elements of the set describing the property.

Direct formalization:

**Definition: semantic property (or verification goal)**

Assuming **program behaviors** range in set $S$, a **semantic property** is a set $G \subseteq S$.

Given program $P$, then $P$ satisfies $G$ if and only if:

$$\forall b \in [P]_S, \ b \in G$$

or equivalently,

$$[P]_S \subseteq G$$

Let us see some examples...
Examples

**Unreachability of certain states** $Q \subseteq S$:

- set property $S \setminus Q$
  
  *i.e.*, we want to show $[P]_{\mathcal{R}} \subseteq S \setminus Q$

- trace property $(S \setminus Q)^{\omega}$
  
  *i.e.*, we want to show $[P]_{\mathcal{T}^{\omega}} \subseteq (S \setminus Q)^{\omega}$

- classical case 1: $Q$ corresponds to error states or dangerous states (**absence of runtime errors**)

- classical case 2: $Q$ corresponds to exit state that violate some exit condition (**partial correctness**)

**Termination:**

- trace property $(S)^{\ast}$
  
  *i.e.*, we want to show $[P]_{\mathcal{T}^{\ast}} \subseteq (S)^{\ast}$

  or, equivalently that $[P]_{\mathcal{T}^{\omega}} \subseteq \emptyset$ (*i.e.*, $P$ has no infinite trace)

Depending on property kinds, specific **proof methods/analysis methods** apply...
Outline

1. Introduction

2. Non-interference

3. Specificities of security properties
   - Properties as sets
   - Significant sets of properties
   - Non interference is not a trace property

4. Hyperproperties

5. Dependence analysis for non-interference

6. Relational reasoning over non-interference

7. Conclusion
Safety properties

Informal definition:

A safety property is a semantic property such that, when it does not hold, it admits a finite counter-example trace.

Intuitively, we can test a safety property on a trace and be able to say after a finite session whether this trace is a counter-example or not.

Definition: safety property

A trace property $G \subseteq S^*\omega$ is a safety property if and only if:

$$\forall T \subseteq S^*\omega, T \not\subseteq G \implies \exists \sigma \in S^*, \exists \sigma' \in S^*\omega, \sigma \cdot \sigma' \in T, \land \forall \sigma'' \in S^*, \sigma \cdot \sigma'' \not\in G$$

If we let $T = [P]_{T^*\omega}$, we recover the informal definition.

Remarks:

- infinite traces do not matter, thus we can consider $[P]_{T^*}$ instead of $[P]_{T^*\omega}$;
- if we could enumerate all finite traces of $P$ we can decide whether it satisfies safety property $G$.  

Examples of safety properties

**State properties are safety properties:**
- let us consider the state property $G \subseteq S$
- then if we consider traces,

$$[P]_R \subseteq G \iff [P]_{T^*} \subseteq G^*$$

which is safety

proof left as exercise

**consequence:**
absence of runtime errors and functional correctness are safety

But **many interesting safety properties are not state properties:**
- let $\sigma \in S$
- consider $G$ defined by $\langle \sigma_0, \ldots, \sigma_n \rangle \in G \iff \text{Card}(\{i \in \mathbb{N} \mid \sigma_i = \sigma\}) \leq 1$

*i.e.*, a trace is correct if and only if it cannot visit $\sigma$ twice
- we can show that $G$ is a safety property
- based on the states it visits, one cannot say whether a trace meets it
Proof method for safety

We consider a program $P$ with initial states $S_i$ and transition relation $\rightarrow$:

**Principle of invariance proofs**

Let $I$ be a set of finite traces; it is said to be an invariant if and only if:

- $\forall \sigma \in S_I, \langle \sigma \rangle \in I$
- $\forall \langle \sigma_0, \ldots, \sigma_n \rangle \in I, \forall \sigma_{n+1} \in S, \sigma_n \rightarrow \sigma_{n+1} \implies \langle \sigma_0, \ldots, \sigma_{n+1} \rangle \in I$

It is stronger than $G$ if and only if $I \subseteq G$.

The **by invariance** proof method is based on finding an invariant that is stronger than $T$.

This proof method always works (theorem proof left as an exercise):

**Theorem: soundness and completeness**

A safety property $G$ holds if and only if there exists an invariant stronger than $G$.

But, finding a suitable invariant $I$ is often **very difficult** (especially automatically)
Liveness properties

Informal definition, a form of dual of safety:

A **liveness property** is a semantic property such that any finite execution may be extended into a correct one; thus, it has **no finite counter-example**

Canonical example: **termination**
- after finitely many steps of an unfinished execution, we cannot say for sure whether the program is about to terminate or will never terminate...
- **consequence**: testing will not produce counterexample for termination
  - **hack**: search for repeating states in finite executions
    - but this is changing the problem and will not capture all cases of NT

**Definition: liveness property**
A trace property $G \subseteq S^{*\omega}$ is a **liveness property** if and only if:

$$\forall \sigma \in S^*, \exists \sigma' \in S^{*\omega}, \sigma \cdot \sigma' \in G$$

**Termination:**
$G = S^*$, i.e., there should be no infinite trace
Proof method for liveness

There exists also a proof method for liveness properties, which is also sound and complete.

We only sketch the case of termination since the general proof principle is long to describe and similar in spirit...

**Definition: ranking function**

A ranking function for program $P$ is a function $\phi: S^* \rightarrow E$, where $E$ with partial order $\preceq$ is a well-founded ordering (no infinite decreasing chains) and the ranking property below holds:

$$\forall \langle \sigma_0, \ldots, \sigma_n \rangle, \forall \sigma_{n+1} \in S,$$

$$\sigma_n \rightarrow \sigma_{n+1} \implies \phi(\langle \sigma_0, \ldots, \sigma_{n+1} \rangle) \prec \phi(\langle \sigma_0, \ldots, \sigma_n \rangle)$$

This is the basis for proof methods that reduce the search of a variant (like a ranking function) to that of an invariant, but for a different program.
Decomposition of trace properties

Theorem: decomposition (see [Alpern & Schneider 87])

Let \( G \subseteq S^\omega \); it can be decomposed into the **conjunction** of a safety property \( G_s \) and a liveness property \( G_l \):

\[
G = G_s \cap G_l
\]

**Proof:**
- it is actually **systematic** and **constructive**
  - *i.e.*, it describes precisely how both \( G_s \) and \( G_l \) can be defined
- see the paper for details (part of recommended reading assignment)

**Application:** how to verify any trace property \( G \)

1. **decompose** it into \( G = G_s \cap G_l \) where \( G_s \) is a safety property and \( G_l \) a liveness property
2. **search for an invariant** to prove \( G_s \)
3. **search for a variant** to prove \( G_l \)

**Example:** total correctness

\( G_s \): absence of crashes + partial correctness and \( G_l \): termination
Status so far

- **Trace properties**
  - total correctness

- **Safety properties**
  - never reach $s_0$ before $s_1$

- **State properties**
  - absence or runtime errors
  - partial correctness

- **Liveness properties**
  - termination

- actually there is a small interaction between safety and liveness
- proof methods exist for all these
- we can search for invariants by static analysis...
Outline

1. Introduction

2. Non-interference

3. Specificities of security properties
   - Properties as sets
   - Significant sets of properties
   - Non interference is not a trace property

4. Hyperproperties

5. Dependence analysis for non-interference

6. Relational reasoning over non-interference

7. Conclusion
Refinement: monotonicity over behaviors and properties

Monotonicity over properties

Let $T_0, T_1$ be two trace properties such that $T_0 \subseteq T_1$.
Let $P$ be a program. Then:

If $P$ satisfies $T_0$, then $P$ satisfies $T_1$.

- obvious consequence of the definition using $\subseteq$
- intuitively, a property that consist of fewer behaviors is stronger

Monotonicity over program behaviors

Let $P_0, P_1$ be two programs such that $\llbracket P_0 \rrbracket_{T^\omega} \supseteq \llbracket P_1 \rrbracket_{T^\omega}$.
Let $T$ be a trace property. Then:

If $P_0$ satisfies $T$, then $P_1$ satisfies $T$.

- again, obvious consequence of the definition using $\subseteq$
- intuitively, a program with fewer behaviors satisfies more properties.

Monotonicity over program behaviors also holds if we consider $\llbracket . \rrbracket_R$ or $\llbracket . \rrbracket_{\mathcal{F}[\ldots]}$ instead of $\llbracket . \rrbracket_{T^\omega}$.
Two (contrived) examples programs and non-interference

A few simplifying assumptions (it is hard to do simpler...):
- only two variables s, x, with s private and x public
  thus $X_{pub} = \{x\}$ and $X_{sec} = \{s\}$
- only two values $V = \{0, 1\}$
- for clarity we write $(m(s), m(x))$ for the memory state $m$

We consider $P_0, P_1$ with the denotational semantics below

$$
\llbracket P_0 \rrbracket_{\mathcal{F}[\ell_-, \ell_-]} : 
\begin{align*}
(0, 0) & \mapsto M \\
(0, 1) & \mapsto M \\
(1, 0) & \mapsto M \\
(1, 1) & \mapsto M
\end{align*}
$$

$$
\llbracket P_1 \rrbracket_{\mathcal{F}[\ell_-, \ell_-]} : 
\begin{align*}
(0, 0) & \mapsto M \\
(0, 1) & \mapsto M \\
(1, 0) & \mapsto \{(1, 1)\} \\
(1, 1) & \mapsto \{(1, 1)\}
\end{align*}
$$

Observations:
- $P_0$ satisfies non-interference:
  whatever the private input, the public output is always 1, thus there is no way to learn anything about the secret
- $P_1$ violates non-interference:
  when the public output is 0, we know the private input cannot be 1
Specificities of security properties

Non interference is not a trace property

Let us put it all together:

- $P_0$ has more behaviors than $P_1$
- $P_0$ satisfies non-interference
- thus, if non-interference was a trace property then $P_1$ should satisfy non-interference
- but $P_1$ violates non-interference

Conclusion:

Non-interference is not a trace property.

i.e., we cannot characterize non-interference by a set of “non-interfering” executions...

Consequences:

- we cannot decompose it into safety/liveness and apply existing proof methods, and apply directly previously shown static analysis methods
- we need to study different techniques
Outline

1. Introduction
2. Non-interference
3. Specificities of security properties
4. Hyperproperties
5. Dependence analysis for non-interference
6. Relational reasoning over non-interference
7. Conclusion
Hyperproperties

Moving to sets of sets of behaviors

We first search for **how to characterize** non-interference (and related security properties):

**Definition: semantic hyperproperty**

Assuming **program behaviors** range in set $S$ a **semantic hyperproperty**, a semantic property is a set of sets $\mathcal{G} \subseteq \mathcal{P}(S)$.

Given program $P$, then $P$ satisfies $\mathcal{G}$ if and only if:

$$[P]_S \in \mathcal{G}$$

**Important differences** with everything we have seen so far:

- all executions of the program are considered **at once**
  *i.e.*, adding or removing one trace may invalidate the property of the whole set

- known proof methods/static analysis techniques **break**
  *i.e.*, we cannot check execution traces one by one (by testing)
  *i.e.*, we cannot rely on an over-approximation of $[P]_S$
  (that could be computed by static analysis)
Lemma

Any trace property can be described by a semantically equivalent hyperproperty.

Indeed, let \( T \subseteq \Sigma^\omega \) be a trace property and \( P \) a program. Then:

\[
P \text{ satisfies } T \iff [P]_{T^\omega} \subseteq T \iff [P]_{T^\omega} \in \mathcal{P}(T)
\]

Thus \textbf{property} \( T \) describes the same program as \textbf{hyperproperty} \( \mathcal{P}(T) \) (powerset induces a downwards closure on hyperproperties).

Note that:

- the monotonicity results \textbf{do not hold for hyperproperties}
- for specific pairs of hyperproperties, we may of course observe a monotone behavior, \textit{e.g.} for hyperproperties induced by properties.
Non-interference

To express non-interference on traces we need to **abstract traces into input-output functions**:

\[ \Phi : S^* \omega \rightarrow (M \rightarrow \mathcal{P}(M)) \]
\[ T \mapsto \lambda m \cdot \{ m' \in M, (l, m), \ldots, (l, m') \in T \} \]

We can now define **non-interference** as an **hyperproperty**:

\[ \mathcal{N} = \{ T \in \mathcal{P}(S^* \omega) | \forall m_0, m_1 \in \mathbb{M}, (\forall x \in X_{pub}, m_0(x) = m_1(x)) \implies \forall x \in X_{pub}, \Phi(T)(m_0)(x) = \Phi(T)(m_1)(x) \} \]

This definition captures the non-interference property:

- whenever two initial memories agree on public variables
  - then corresponding final states should agree on private variables.

**Examples (continued):**

- \([P_0] T^* \omega \in \mathcal{N}\)
- \([P_1] T^* \omega \notin \mathcal{N}\)
Average execution time

We temporarily make a few **limiting assumptions** on programs:
- we consider **only terminating programs**
- we consider **only programs with finitely many complete executions**

complete executions: from entry control state $\ell_\top$ to exit control state $\ell_\bot$

Given a set of traces $T \in \mathcal{P}(\mathcal{S}^*)$, we define:

$$\text{Avg\_len}(T) = \frac{1}{|T|} \sum_{\sigma \in T} \text{length}(\sigma)$$

where $\text{length}$ returns the length of a trace.

**Average execution time lower than $k \in \mathbb{N}$** (clearly not a trace property):

$$A_k = \{ T \in \mathcal{P}(\mathcal{S}^*) \mid \text{Avg\_len}(T) \leq k \}$$

**Generalization:**
- with some **measure theory**, we can extend similar properties to **infinite sets of program traces**
- we can also **let programs have some infinite traces**, and consider only the finite ones
Interesting families of hyperproperties

Can we divide the set of hyperproperties in interesting sub-classes?

Hierarchy inspired by the safety/liveness division, and more precisely how can a hyperproperty be disproved:

- **hypersafety**: can always be disproved using a finite set of finite traces

- **$k$-safety**: can always be disproved using a set of at most $k$ finite traces
  
  Clearly:
  
  - $k$-safety hyperproperties are also $k+1$-safety
  - $k$-safety hyperproperties are also hypersafety

- **hyperliveness**: disproving them requires looking at infinite traces or infinite sets of traces

We now formalize some of these sets more in detail...
Hypersafety

The idea is to extend safety, except that the observation is limited to finite sets finite traces, instead of just finite traces.

**Extension of an observation:**
Given $T, T' \subseteq S^*\omega$, we say that $T'$ extends $T$ and note $T \leq T'$ if and only if:
$$\forall \sigma \in T, \exists \sigma' \in S^*\omega, \sigma \cdot \sigma' \in T'$$

**Definition: hypersafety**
Let $G \in \mathcal{P}(\mathcal{P}(S^*\omega))$ be a hyperproperty. Then, we say that $G$ is a **hypersafety** property if and only if for all $T \in \mathcal{P}(S^*\omega)$, if $T$ does not satisfy $G$, then
$$\exists M \subseteq S^*, \left\{ \begin{array}{l}
M \text{ is a finite set} \\
\land M \leq T \\
\land \forall T' \subseteq S^*\omega, M \leq T' \implies T' \notin G
\end{array} \right.$$  

**Examples:**
- absence of runtime errors (counter-example: one crashing trace)
- non-interference (counter-example: two traces revealing leak)
Hyperproperties

$k$-safety

Hypersafety is **not very specific**, as counter-examples can be **arbitrarily large**.
Additional (parametric) restriction: the number of traces in the counter-example.

**Definition: $k$-safety**

Let $\mathcal{G} \in \mathcal{P}(\mathcal{P}(\mathcal{S}))$ be a hyperproperty. Then, we say that $\mathcal{G}$ is a **$k$-safety** property if and only if for all $T \in \mathcal{P}(\mathcal{S}^\omega)$, if $T$ does not satisfy $\mathcal{G}$, then

$$\exists M \subseteq \mathcal{S}^*, \begin{cases} M \text{ has at most } k \text{ elements} \\ \land M \leq T \\ \land \forall T' \subseteq \mathcal{S}^\omega, M \leq T' \implies T' \notin \mathcal{G} \end{cases}$$

**Interesting examples:**

- **all safety properties** are **1-safety**
  
  *i.e.*, counter-examples consist only of one offending finite trace this includes the absence of runtime errors

- **non-interference:**
  
  *i.e.*, by the definition a counter-example is made of two finite traces

- **$k$-safety is included in $k + 1$-safety**
Hyperliveness

Intuition behind liveness: finite observations are not counter-examples.

We can extend this intuition here, except that a finite observation is now any finite set of finite execution traces:

**Definition: hyperliveness**

Let $G \in \mathcal{P}(\mathcal{P}(S))$ be a hyperproperty. Then, we say that $G$ is a **hyperliveness** property if and only if

$$\forall T \subseteq \mathcal{P}(S^*\omega), \ T \text{ finite} \implies \exists T' \subseteq \mathcal{P}(S^*\omega), \ \left\{ \begin{array}{l} T \leq T' \\ T' \in G \end{array} \right.$$  

**Example:**

- the average run-time is less than $N$ steps
- indeed, any finite set of executions may be extended with enough short ones to bring down the average.
Hyperproperties

Decomposition of hyperproperties

We can also extend the Alpern & Schneider decomposition theorem:

**Decomposition theorem**

Let $G \in \mathcal{P}(\mathcal{P}(S^{*\omega}))$ be a hyperproperty. Then, there exist

- a hypersafety property $G_s$ and
- a hyperliveness property $G_l$

such that:

$$G = G_s \cap G_l$$

- see [Clarkshon & Schneider 2008]
- no general proof method for hyperproperties... unlike the framework of trace properties
- in the following of this class, though **2-safety is enough**
Outline

1. Introduction
2. Non-interference
3. Specificities of security properties
4. Hyperproperties
5. Dependence analysis for non-interference
   - Semantics for non-interference
   - Hypercollecting semantics
   - Dependence abstraction and analysis
6. Relational reasoning over non-interference
7. Conclusion
Observations so far:

- typical semantics describe **sets of behaviors** and are based on **fixpoint definitions**
- abstract interpretation builds upon abstraction and fixpoint definition hence, it allows to over-approximate **sets of behaviors**
- in the case of non-interference, **over-approximating sets of behaviors** is **not useful**
- the same goes for any hyperproperty that is not a trace property...

We need a technique to conservatively reason over hyperproperties

We are going to consider **two approaches**:

1. **lifting the semantics** to sets of sets of traces
2. **re-expressing** the hyperproperties that we are interested in

Each will yield some interesting kinds of analyses
A very basic language

In the following, we study a very basic imperative language, to describe a static analysis based on a semantics defined in terms of sets of sets:

- as before, we assume finitely many variables $X$ and a set set of base type values $V$
- expressions:
  \[
  e ::= v \quad \text{base type value} \\
  \quad | \quad x \quad \text{variable} \\
  \quad | \quad e_0 \oplus e_1 \quad \text{binary operation} \oplus
  \]
- commands:
  \[
  s ::= x := e \quad \text{assignment} \\
  \quad | \quad \text{skip} \quad \text{do nothing} \\
  \quad | \quad s_0; s_1 \quad \text{sequence} \\
  \quad | \quad \text{if}(e_0) \ s_1 \ \text{else} \ s_2 \quad \text{condition} \\
  \quad | \quad \text{while}(e_0) \ s_1 \quad \text{loop}
  \]

- non-determinism occurs only at the beginning of program execution
  once the initial state is set up, no non-determinism occurs
Dependence analysis: intuition

**Example:**

\[ x = \ldots; \]
\[ y = 2 \times x + 3; \]
\[ z = a + b; \]
\[ t = y \times x; \]

- y is computed from x;
- t is computed from x and y, also computed from x so t depends only on x
- z is computed from a and b, which have no connection with x so z does not depend on x

**Basic idea of dependence analysis**

For each variable, **compute a set of variable that it may depend on.**

As usual, we compute an **over-approximation** of actual dependencies
Denotational semantics

**Semantics of expressions** \([\llbracket e \rrbracket : M \rightarrow V]\):

- \([V](m) = v\)
- \([x](m) = m(x)\)
- \([e_0 \oplus e_1](m) = [e_0](m) \oplus [e_1](m)\)

**Semantics of commands** \(\llbracket s\rrbracket_D : S \cup \{\bot\} \rightarrow S \cup \{\bot\}\):

- \(\llbracket s\rrbracket_D(\bot) = \bot\)
- \(\llbracket x := e\rrbracket_D(m) = m[x \mapsto [e](m)]\)
- \(\llbracket \text{skip} \rrbracket_D(m) = m\)
- \(\llbracket s_0; s_1\rrbracket_D(m) = \llbracket s_1 \rrbracket_D \circ \llbracket s_0 \rrbracket_D(m)\)
- \(\llbracket \text{if}(e_0) s_1 \text{ else } s_2 \rrbracket_D(m) = \begin{cases} \llbracket s_1 \rrbracket_D(m) & \text{if } [e](m) = \text{true} \\ \llbracket s_2 \rrbracket_D(m) & \text{if } [e](m) = \text{false} \end{cases}\)
- \(\llbracket \text{while}(e_0) s_1 \rrbracket_D(m) = (\text{lfp } F)(m)\) where
  \[F(\phi) : \begin{cases} \bot & \iff \bot \\ m & \mapsto \begin{cases} \phi \circ \llbracket s_1 \rrbracket_D(m) & \text{if } [e](m) = \text{true} \\ m & \text{if } [e](m) = \text{false} \end{cases} \end{cases}\]

**Exercise:** which lattice to use for iteration?
A second semantics, computing relations

We are interested in **input-output** relations:

- **standard** \([s]_D\): maps input memory state into output memory state
- to obtain **more general statements**: functions over such pairs

1. \([P]_{rel}\) inputs \((m_0, m_1)\), assumes that a previous run from \(m_0\) led to \(m_1\)
2. it computes the effect of \(P\) from there, we assume the result is \(m_2\)
3. then, it returns the new pair \((m_0, m_2) \in F = M \times M\)

**Semantics of commands** \(([s]_F : F \cup \{\bot\} \rightarrow F \cup \{\bot\})\):

\[
\begin{align*}
[s]_F(\bot) &= \bot \\
[x := e]_F(m_0, m_1) &= (m_0, m_1[x \mapsto [e](m_1)]) \\
[skip]_F(m_0, m_1) &= (m_0, m_1) \\
[s_0; s_1]_F(m_0, m_1) &= [s_1]_F \circ [s_0]_F(m_0, m_1) \\
[if(e_0) s_1 \ else \ s_2]_F(m_0, m_1) &= \begin{cases} 
[s_1]_F(m_0, m_1) & \text{if } [e](m_1) = \text{true} \\
[s_2]_F(m_0, m_1) & \text{if } [e](m_1) = \text{false} 
\end{cases} \\
[while(e_0) s_1]_F(m_0, m_1) &= \text{lfp } G \\
\end{align*}
\]

where \(G\) is left as an exercise
Relation between semantics

We have defined:

- A semantics on states:
  \[ [s]_F : \mathbb{S} \cup \{\bot\} \rightarrow \mathbb{S} \cup \{\bot\} \]

- A semantics on relations:
  \[ [s]_F : \mathbb{F} \cup \{\bot\} \rightarrow \mathbb{F} \cup \{\bot\} \]

Properties

- If \([s]_D(m_1) = m_2\), then \([s]_F(m_0, m_1) = (m_0, m_2)\)
- If \([s]_D(m_1) = \bot\), then \([s]_F(m_0, m_1) = (m_0, \bot)\)
Non-interference

We can express **non-interference** directly.
Assumption: $X_{pub}, X_{sec}$ are given.

We let the following equivalence relation describe **memory agreement** on any given set of variables $X$:

- notation: $m_0 \equiv_X m_1$
- condition:

\[
m_0 \equiv_X m_1 \iff \forall x \in X, \ m_0(x) = m_1(x)
\]

**Non-interference at the relational semantics level**

Program $P$ satisfies non-interference if and only if

\[
\forall m_0, m'_0, m_1, m'_1 \in \mathbb{M}, \quad \begin{cases}
m_0 \equiv_{X_{pub}} m'_0 \\
\llbracket P \rrbracket F(m_0, m_0) = (m_0, m_1) \\
\llbracket P \rrbracket F(m'_0, m'_0) = (m'_0, m'_1) \end{cases} \implies m_1 \equiv_{X_{pub}} m'_1
\]

**Remark**: we could work out similar definitions with full traces rather than relations...
Outline

1 Introduction

2 Non-interference

3 Specificities of security properties

4 Hyperproperties

5 Dependence analysis for non-interference
   - Semantics for non-interference
   - Hypercollecting semantics
   - Dependence abstraction and analysis

6 Relational reasoning over non-interference

7 Conclusion
Towards a non-standard semantics

**Base semantics:**
- we have defined \([s]_F : F \cup \{ \perp \} \rightarrow F \cup \{ \perp \}\)
- let \(\delta_M = \{(m, m) \mid m \in M\}\)
- then, \([s]_F(\delta_M)\) describes exactly the input/output pairs of \(s\) as observed, over-approximating this set of pairs is of **no use** to prove non-interference, thus we turn to a new semantics

**Hypercollecting semantics:**
- goal: compute a set of set of pairs...
- thus, we let \([s]_H : P(P(F)) \rightarrow P(P(F))\) and \(\Delta_M = \{\delta_M \mid M \in P(M)\}\)
- then, \([s]_H(\Delta_M)\) computes the set of sets of input/output pairs, for any set of inputs

We will set up the definition of \([.]_H\) so as to meet the following two conditions:

1. for all \(s\) and for all \(F \in P(F)\), the definition of \([s]_H\) is such that
\(([s]_F(F) \cap F) \in [s]_H(\{F\})\)

2. \([.]_H\) is **adapted for abstract interpretation**, i.e., can be over-approximated in an inductive manner
Hypercollecting semantics

Hypercollecting semantics of tests:

\[
\begin{align*}
\llbracket e \rrbracket_{\mathcal{H}, \text{test}} : \mathcal{P}(\mathcal{P}(F)) & \rightarrow \mathcal{P}(\mathcal{P}(F)) \\
E & \mapsto \{(m_0, m_1) \in F \mid \llbracket e \rrbracket(m_1) = \text{true}\} \mid F \in \mathcal{E}
\end{align*}
\]

Hypercollecting semantics of commands:

\[
\begin{align*}
\llbracket e \rrbracket_{\mathcal{H}} : \mathcal{P}(\mathcal{P}(F)) & \rightarrow \mathcal{P}(\mathcal{P}(F)) \\
\llbracket x := e \rrbracket_{\mathcal{H}}(\mathcal{E}) & = \{(m_0, m_1[x \mapsto v]) \mid (m_0, m_1) \in F \\
& \quad \land \llbracket e \rrbracket(m_1) = v\} \mid F \in \mathcal{E}
\end{align*}
\]

\[
\begin{align*}
\llbracket \text{skip} \rrbracket_{\mathcal{H}}(\mathcal{E}) & = \mathcal{E} \\
\llbracket s_0; s_1 \rrbracket_{\mathcal{H}}(\mathcal{E}) & = \llbracket s_1 \rrbracket_{\mathcal{H}} \circ \llbracket s_0 \rrbracket_{\mathcal{H}}(\mathcal{E}) \\
\llbracket \text{if}(e_0) \ s_1\ \text{else}\ s_2 \rrbracket_{\mathcal{H}}(\mathcal{E}) & = \{\llbracket s_1 \rrbracket_{\mathcal{D}} \circ \llbracket e_0 \rrbracket_{\mathcal{H}, \text{test}}(F) \\
& \quad \cup \llbracket s_2 \rrbracket_{\mathcal{D}} \circ \llbracket \neg e_0 \rrbracket_{\mathcal{H}, \text{test}}(F) \mid F \in \mathcal{E}\}
\end{align*}
\]

\[
\begin{align*}
\llbracket \text{while}(e_0) \ s_1 \rrbracket_{\mathcal{H}}(\mathcal{E}) & = \llbracket e \rrbracket_{\mathcal{H}, \text{test}} \circ \text{lfp}_F \ G_{\mathcal{H}}(\mathcal{E})
\end{align*}
\]

where \(G_{\mathcal{H}}(\phi) = \llbracket \text{if}(e_0) \ s_1; \phi \text{ else skip} \rrbracket_{\mathcal{H}}\)
Hypercollecting semantics

Instantiation:

- starting from $\Delta_M = \{ \delta_M \mid M \in \mathcal{P}(M) \} = \{(m, m) \mid m \in M \mid M \in \mathcal{P}(M)\}$
- then, $[s]_H(\Delta_M) \in \mathcal{P}(\mathcal{P}(F))$ collects the set of all sets of runs of $s$, described by a pair made of an input memory and an output memory
- each of the hypercollecting semantics inputs such a set of sets of pairs

Induction:

- $[s]_H$ is defined by case analysis of $s$ but its definition is not exactly done by induction
- but we can prove by induction
  - that it is monotone
  - the inclusion
    $$([s]_F(F) \cap F) \in [s]_H(\{F\})$$
- the combination of these properties opens up inductive approximation
- see [Assaf et al 2017]
Outline

1 Introduction
2 Non-interference
3 Specificities of security properties
4 Hyperproperties
5 Dependence analysis for non-interference
   • Semantics for non-interference
   • Hypercollecting semantics
   • Dependence abstraction and analysis
6 Relational reasoning over non-interference
7 Conclusion
Dependence abstraction

We now set up an abstraction for $\llbracket s \rrbracket_H(\Delta_M) \in \mathcal{P}(\mathcal{P}(F))$, that describes dependences between inputs and outputs.

**Agreement relation:** if $X \subseteq X$, the equivalence relation $(\equiv_X) \subseteq M \times M$ is defined by

$$m_0 \equiv_X m_1 \iff \forall x \in X, \ m_0(x) = m_1(x)$$

**Dependence abstraction**

We let the **dependence abstract domain** be $\mathbb{D}_{dep}^\# = X \rightarrow \mathcal{P}(X)$ with the pointwise inclusion ordering, with the following concretization function:

$$\gamma_{dep}: \mathbb{D}_{dep}^\# \rightarrow \mathcal{P}(\mathcal{P}(F))$$

$$d \rightarrow \{ R \in \mathcal{P}(F) \mid \forall (m_0, m_1), (m'_0, m'_1) \in R, \ \forall x \in X, \ m_0 \equiv_d(x) \ m'_0 \Rightarrow m_1 \equiv \{x\} m'_1 \}$$

**Contraposition:** when a pair of executions lead to **distinct outputs**, there must be **disagreement in at least some of the dependence inputs**
Dependence analysis for non-interference

Dependence abstraction and analysis

Dependence abstraction: example

Back to some examples related to non-interference...

**Program 1:**

```c
// ... as before, s stores the secret
if ( s == 7 )
    i = 1;
else
    i = -1;
```

Non-interference: **violated**

Dependency:

```
i \rightarrow \{s\}
```

Indeed, modifying $s$ may cause distinct $i$ outputs

**Program 3:**

```c
i = 0 * s;
```

Non-interference: **satisfied**

Dependency:

```
i \rightarrow \emptyset
```

Indeed, $s$ ends up being 0 regardless...

Non-interference

Non-interference holds if and only if no public variable depends on a secret.
Dependence analysis of expressions

Principle of the dependency analysis of expressions:

- to be used for the analysis of commands
  e.g., assignment command $x = e$
  new dependency of $x$: whatever may change the result of $e$
- compute an over-approximation of the set of the variables that may make the evaluation result change

Definition of $[e]_{dep}^\# \in D_{dep}^\# \rightarrow \mathcal{P}(X)$:

$$
[v]_{dep}^\#(d) = \emptyset \\
[x]_{dep}^\#(d) = d(x) \\
[e_0 \oplus e_1]_{dep}^\#(d) = [e_0]_{dep}^\#(d) \cup [e_1]_{dep}^\#(d)
$$

It is approximate:

- expression $x \ast 0$ does not depend on $x$ in the concrete
- but $[x \ast 0]_{dep}^\# = \{x\}$
Soundness of the analysis of expressions

The analysis of expressions is sound in the following sense:

\[ \forall R \in \gamma_{\text{dep}}(d), \forall (m_0, m_1), (m'_0, m'_1) \in R, \]
\[ m_0 \equiv \llbracket e \rrbracket_{\text{dep}}(d) \quad m'_0 \rightarrow \llbracket e \rrbracket(m_1) = \llbracket e \rrbracket(m'_1) \]

- the proof proceeds by induction over the syntax of expressions
- **example 1:**
  let us assume that \( e \) is \( x + y \)
  and that \( d \) is \( x \mapsto \{x\}, y \mapsto \{x, t\}, t \mapsto \{z\} \):
  then, \( \llbracket e \rrbracket_{\text{dep}}(d) = \{x, t\} \) (this result is precise)
- **example 2:**
  let us assume that \( e \) is \( 0 \ast x \)
  and that \( d \) is \( x \mapsto \{x\}, \ldots : \)
  then, \( \llbracket e \rrbracket_{\text{dep}}(d) = \{x\} \) (this result is imprecise)
Dependence analysis of commands

**Principle:**
- Define a function $\llbracket s \rrbracket_{dep} : D_{dep} \rightarrow D_{dep}$ by induction over the syntax of statements.
- Ensure *soundness condition*
  \[
  \llbracket s \rrbracket \mathcal{H} \circ \gamma_{dep} \subseteq \gamma_{dep} \circ \llbracket s \rrbracket_{dep}
  \]
- Apply $\llbracket s \rrbracket_{dep}$ to $d_{id} = \lambda x \in X \cdot \{x\}$ (note that $\Delta_M \subseteq \gamma_{dep}(d_{id})$)
Dependence analysis of sequences and assignment commands

**Analysis of skip commands:** $\llbracket \text{skip} \rrbracket_{\text{dep}}(d) = d$
- since the concrete semantics is also the identity function

**Analysis of sequences:** $\llbracket s_0; s_1 \rrbracket_{\text{dep}}(d) = \llbracket s_1 \rrbracket_{\text{dep}} \circ \llbracket s_0 \rrbracket_{\text{dep}}(d)$
- since the concrete semantics is also a composition

**Analysis of assignment commands**, based on the previously defined $\llbracket e \rrbracket_{\text{dep}}$:

$$\llbracket x = e \rrbracket_{\text{dep}}(d) = \begin{cases} x & \text{if } y \neq x \\ \llbracket e \rrbracket_{\text{dep}}(d) & \text{if } d(y) \end{cases}$$
Dependence analysis of condition commands

Dependences induced by condition command \texttt{if}(e_0) \texttt{s}_1 \texttt{else} \texttt{s}_2:

1. dependences in assignments in \texttt{s}_1, \texttt{s}_2 as before
2. any variable modified in either \texttt{s}_1 or \texttt{s}_2 also depends on the condition \texttt{e}_0

Modified variables \( M(s) \in P(X) \):

\[
M(x := e) = \{x\} \quad M(\texttt{if}(e_0) \texttt{s}_1 \texttt{else} \texttt{s}_2) = M(s_0) \cup M(s_1) \\
M(\texttt{skip}) = \emptyset \quad M(\texttt{while}(e_0) \texttt{s}_1) = M(s_1) \\
M(s_0; s_1) = M(s_0) \cup M(s_1)
\]

Dependency analysis of condition statement \( s ::= \texttt{if}(e_0) \texttt{s}_1 \texttt{else} \texttt{s}_2 \):

- we let \( d' = [s_1]_{\text{dep}}(d) \cup [s_2]_{\text{dep}}(d) \) (pointwise union)
- analysis function:

\[
[s]_{\text{dep}}(d) = \lambda(x \in X). \left\{ \begin{array}{ll}
d'(x) \cup [e_0]_{\text{dep}}(d) & \text{if } x \in M(s_1) \cup M(s_2) \\
d'(x) & \text{otherwise}
\end{array} \right.
\]

Case of loops: apply standard fixpoint techniques, left as an exercise
Soundness of the analysis of commands

**Analysis soundness**

For all statement, we have:

1. **soundness of the abstract semantics:**

\[
\underleftarrow{[s]} H \circ \gamma_{\text{dep}} \subseteq \gamma_{\text{dep}} \circ \underleftarrow{[s]}_{\text{dep}}
\]

2. **soundness of the analysis:**

\[
\underleftarrow{[s]} \mathcal{F}(\delta_M) \in \gamma_{\text{dep}} \circ \underleftarrow{[s]}_{\text{dep}}(d_{id})
\]

1. proof by induction over the syntax

2. composing inclusions:

\[
\underleftarrow{[s]} \mathcal{F}(\delta_M) \subseteq \underleftarrow{[s]} H(\{\delta_M\}) \\
\subseteq \underleftarrow{[s]} H(\Delta_M) \\
\subseteq \underleftarrow{[s]} H \circ \gamma_{\text{dep}}(d_{id}) \\
\subseteq \gamma_{\text{dep}} \circ \underleftarrow{[s]}_{\text{dep}}(d_{id})
\]
Dependence analysis: example explicit flows

\[
\begin{align*}
    z & = y - 1 + x; \\
    x & = s \ast s + 8; \\
    y & = x + 1;
\end{align*}
\]

Information flows

- There are information flows from \( s \) to \( x \) and to \( y \).
- There is no information flow from \( s \) to \( z \).
Dependence analysis: example implicit flows

\[
\{x \mapsto \{x\}, y \mapsto \{y\}, s \mapsto \{s\}\}
\]

\[
x = s * s + 8;
\]

\[
\{x \mapsto \{s\}, y \mapsto \{y\}, s \mapsto \{s\}\}
\]

\[
\text{if}(x > 0) \{
\}
\]

\[
y = y + 1;
\]

\[
\{x \mapsto \{s\}, y \mapsto \{y\}, s \mapsto \{s\}\}
\]

\[
\text{else} \{
\}
\]

\[
y = y - 1;
\]

\[
\{x \mapsto \{s\}, y \mapsto \{s, y\}, s \mapsto \{s\}\}
\]

**Information flows**

There are information flows from \(s\) to \(x\) (explicit) and to \(y\) (implicit).
Outline

1. Introduction
2. Non-interference
3. Specificities of security properties
4. Hyperproperties
5. Dependence analysis for non-interference
6. Relational reasoning over non-interference
7. Conclusion
Another informal proof principle

We look again at the definition of non-interference:

**Non-interference**

Program $P$ satisfies the **non-interference** property defined by $X_{\text{pub}}/\ell_-, X_{\text{sec}}/\ell_-$ if and only if for all memory states $m_0, m_1 \in \mathbb{M}$,

\[
(\forall x \in X_{\text{pub}}, \ m_0(x) = m_1(x)) \implies (\forall x \in X_{\text{pub}}, \ [P]F[\ell_-,\ell_-](m_0)(x) = [P]F[\ell_-,\ell_-](m_1)(x))
\]

**Intuition:**

- we **run the program twice**, with two states that differ only in the value of one secrete variable
- if the outputs agree for all such pairs of runs, then **non-interference** is satisfied

We can turn this **into a symbolic composition**, to allow for the non-interference to be verified.
Proof by self-composition

**Notation**: to build self-composition, we need to make variables explicit
- we write $P[x, y]$ for a program that is defined over variables $x, y$, even though it may use only some of these;
- for example, we may let $P[x, y, z]$ stand for program **while**($x \leq y$)$\{x = x + 1\}$ ($z$ is included even though it is not used in the program)

**Definition**: proof by self-composition (see [Barthe & Rezk 2004])

Let $P[s_0, \ldots, s_k, x_0, \ldots, x_l]$ be a deterministic program, where $X_{\text{sec}} = \{s_0, \ldots, s_k\}$ and $X_{\text{pub}} = \{x_0, \ldots, x_l\}$. We let $s'_0, \ldots, s'_k, x'_0, \ldots, x'_l$ be **fresh** variables. We let $Q[s_0, \ldots, s_k, x_0, \ldots, x_l, s'_0, \ldots, s'_k, x'_0, \ldots, x'_l]$ be:

\[
\begin{align*}
&\text{assume}(x_0 == x'_0); \ldots; \text{assume}(x_l == x'_l); \\
&P[s_0, \ldots, s_k, x_0, \ldots, x_l]; \\
&P'[s'_0, \ldots, s'_k, x'_0, \ldots, x'_l]; \\
&\text{assert}(x_0 == x'_0); \ldots; \text{assert}(x_l == x'_l);
\end{align*}
\]

Then, $P[\ldots]$ satisfies non-interference if and only if $Q[\ldots]$ satisfies the final assertion.
Proof by self-composition

**Principle:** reduce a security question to a safety question but for a different program

- initial question: *is $P$ secure?*
- reduced question: *is $Q$ safe?* (where $Q$ is defined from $P$)
- then, classical analysis techniques for safety apply

**Specific issues:**

- **termination:**
  if $P$ may not terminate, the observation of termination or non-termination may reveal information on the secret

- **non-determinism:**
  if $P$ may contain some non-determinism, the final assertion of $Q$ may fail even when the non-interference is satisfied

Taking these into account **requires more care.**
A simple case:

Initial program:

\[ x = 8 \times y + 2; \]
\[ s = x + s; \]

Transformed program:

\[ \text{assume}( x0 == x1 ); \]
\[ x0 = 8 \times y0 + 2; \]
\[ s0 = x0 + s0; \]
\[ x1 = 8 \times y1 + 2; \]
\[ s1 = x1 + s1; \]
\[ \text{assert}( x0 == x1 ); \]

Verification of the assertion by static analysis:

- exercise 1: what are the results of dependence analysis?
- exercise 2: which abstract domain to use for verification by self-composition?
Examples

**A more subtle case** to rule out **deceptive implicit flows**:

- **Initial program:**
  
  ```java
  if( s == 1 ) x = s;
  else x = 1;
  ```

- **Transformed program:**
  
  ```java
  assume( x0 == x1 );
  if( s0 == 1 ) x0 = s0;
  else x0 = 1;
  if( s1 == 1 ) x1 = s1;
  else x1 = 1;
  assert( x0 == x1 );
  ```

**Verification of the assertion by static analysis:**

- exercise 1: what are the results of dependence analysis?
- exercise 2: which abstract domain to use for verification by self-composition?
Outline

1. Introduction
2. Non-interference
3. Specificities of security properties
4. Hyperproperties
5. Dependence analysis for non-interference
6. Relational reasoning over non-interference
7. Conclusion
Main points to remember

Security properties are a separate class of properties:
- expressing the property requires quantifying over pairs of executions
- hyperproperties ⊇ hypersafety ⊇ 2-safety
  many important security properties are 2-safety...

Static analysis with respect to hyperproperties:
- dependence analysis has to be proved with respect to a specific semantics, which can talk about pairs of executions
- deceptive implicit flows: conditions

Self-composition:
- technique based on the reduction to another property
Assignment: proofs and paper reading

**Recognizing Safety and Liveness.**
Bowen Alpern and Fred B. Schneider.

**Hyperproperties.**
Michael Clarkson and Fred B. Schneider.

**Hypercollecting semantics and its application to static analysis of information flow.**
Mounir Assaf, David A. Naumann, Julien Signoles, Eric Totel, Frédéric Tronel.

**Secure Information Flow by Self-Composition.**
Gilles Barthe, Pedro R. D’Argenio, Tamara Rezk.
In CSFW 2004: 100-114