

# **Non-Interference For Weak Observers**

**David Clark (Kings College)**

**Sebastian Hunt (City University)**

**Pasquale Malacaria (Queen Mary)**

---

## Motivation

- NI for programming languages typically assumes (for each security level) variables are partitioned into High and Low
  - Assumption is that attackers can see all of the data in Low variables
  - But what if they can't?
    - \* **Weak Observers** - cannot see all low-security data
- [Giacobazzi & Mastroeni, POPL 2004] show how abstract interpretation can be used to model weak observers
  - We explore the idea instead using equivalence relations
  - We consider probabilistic issues
  - No formal connection attempted (**partitioning closures** [Mastroeni]...?)

---

## Overview

- Standard NI
- WNI: Possibilistic NI for Weak Observers
- PWNI: Probabilistic NI for Weak Observers
- Conclusions and Future Work

---

## Standard NI

- Assume programs denote functions  $f : D \rightarrow D$
- Assume  $D = H \times L$
- $f$  is NI if,  $\forall h_1, h_2 \in H, \forall l \in L$ :

$$f(h_1, l) =_L f(h_2, l)$$

---

## Standard NI: Relational Presentation

- Assume programs denote functions  $f : D \rightarrow D$
- Assume  $L$  is an equivalence relation on  $D$
- $f$  is NI if,  $\forall x_1, x_2 \in D$ :

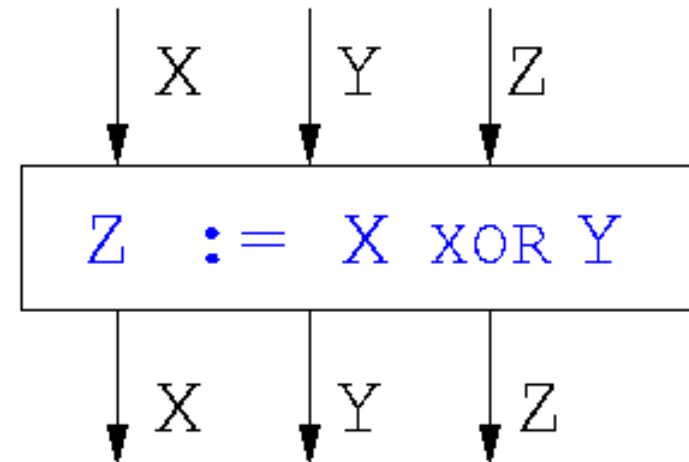
$$x_1 L x_2 \Rightarrow f(x_1) L f(x_2)$$

- Equivalent to previous definition when  $L$  is  $=_L$ 
  - Note no explicit mention of  $H$  in this presentation

---

## Example: XOR

- Suppose  $X$  contains a secret and the observer can see  $Z$  but not  $X$  or  $Y$
- (Arguably!) the program is secure:  
for each possible observed value of  $Z$  on output, both  $X = 0$  and  $X = 1$  are possible inputs, since  $Y$  is unknown
- But however we classify  $Y$  (Low or High) the program fails to satisfy NI



---

## Possibilistic NI for Weak Observers

- We drop the assumption that anything which is not observable must be a secret
- High and Low are now defined by separate equivalence relations  $H, L$
- We call this version of NI a **possibilistic** condition because, for a weak observer, the system appears to behave non-deterministically even for a fixed choice of  $h \in D/H$  and  $l \in D/L$  (variation within  $h \cap l$ )
- The definition requires that for a given  $L$ -equivalence class of inputs, the **set** of observable outputs should not change as we move from one  $H$ -equivalence class to another
  - cf Generalized Non-Interference [McCullough, 1987]

---

## WNI: Possibilistic NI for Weak Observers

- Given equivalence relations  $H$  and  $L$ , say that  $f$  is WNI if,  $\forall h_1, h_2 \in D/H, \forall l \in D/L$ :

$$h_1 \cap l \neq \emptyset \wedge h_2 \cap l \neq \emptyset \Rightarrow f^*(h_1 \cap l) L^* f^*(h_2 \cap l)$$

where  $D/R$  is the set of equivalence classes of  $R$  and  $_*$  denotes lifting to sets:

$$f^*(X) \stackrel{\text{def}}{=} \{f(x) | x \in X\}$$
$$X_1 L^* X_2 \text{ iff } \{[x]_L | x \in X_1\} = \{[x]_L | x \in X_2\}$$

---

## NI and WNI Compared

- Say that  $H$  and  $L$  **split**  $D$  if  $h \cap l$  is singleton for all  $h \in D/H, l \in D/L$
- When  $H$  and  $L$  split  $D$ ,  $D$  is isomorphic to  $(D/H) \times (D/L)$
- Proposition: if  $H$  and  $L$  split  $D$  then NI and WNI are equivalent.
- WNI corresponds to **abstract non-interference** in [Giacobazzi & Mastroeni]

---

## WNI Example: XOR

- Take  $H$  to be  $=_X$  and  $L$  to be  $=_Z$
- Then this program satisfies WNI
- Check:

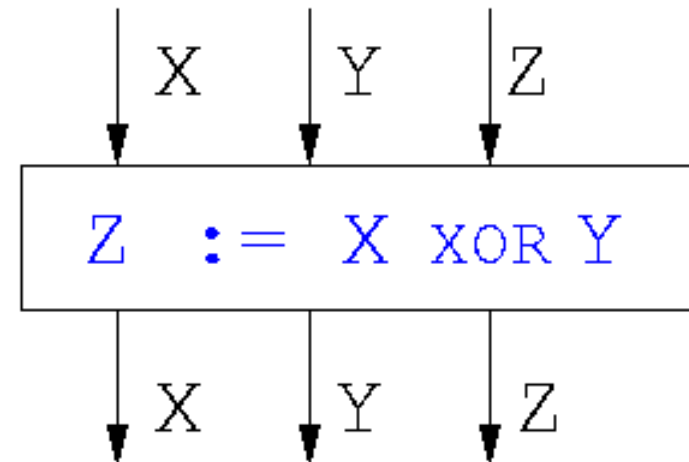
$$D/H = \{0**, 1**\}$$

$$D/L = \{**0, **1\}$$

$$f^*(0** \cap **0) = f^*(0*0)$$

$$= \{000, 011\} L^* \{110, 101\}$$

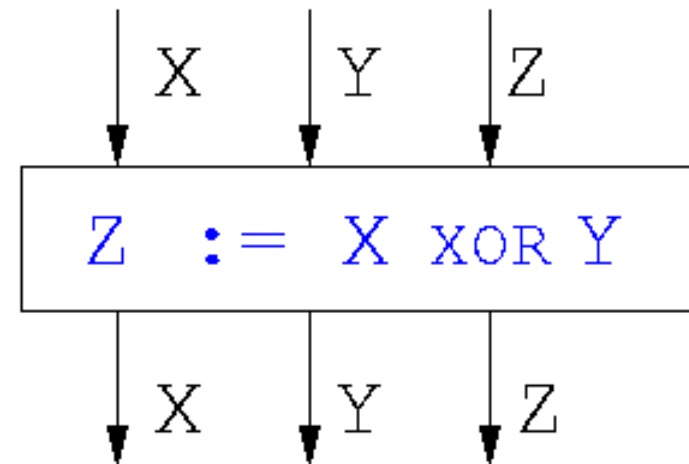
$$= f^*(1*0) = f^*(1** \cap **0), \text{ etc}$$



---

## Limitations of WNI

- WNI suffers from the usual problem of possibilistic NI conditions: it allows probabilistic information flow
- Suppose that the input values of  $Y$  are not uniformly distributed (eg  $P(Y = 0) = 0.9$ )
- Now, 90% of the time, the output value of  $Z$  will equal the input value of  $X$



---

## PWNI: Probabilistic NI for Weak Observers

- Suppose given a distribution  $\mu$  on  $D$  (assumed finite)
- Given equiv. relations  $H$  and  $L$ , say that  $f$  is PWNI if,  $\forall h_1, h_2 \in D/H, \forall l \in D/L$ :

$$\mu(h_1 \cap l) > 0 \wedge \mu(h_2 \cap l) > 0 \Rightarrow f^\dagger(\mu|_{h_1 \cap l}) L^\dagger f^\dagger(\mu|_{h_2 \cap l})$$

where  $\mu|_X$  is the distribution on  $X$  such that  $\mu|_X(x) = \mu(x)/\mu(X)$ , and  $_^\dagger$  denotes lifting to distributions:

$$f^\dagger(\delta)(x) \stackrel{\text{def}}{=} \delta(f^{-1}(x))$$
$$\delta_1 L^\dagger \delta_2 \text{ iff } \forall X \in D/L. \delta_1(X) = \delta_2(X)$$

---

## PWNI (Counter-) Example: XOR

- Take  $H$  to be  $=_X$  and  $L$  to be  $=_Z$ ; assume  $X, Y, Z$  independent on input
- This program fails PWNI for  $\mu(*0*) = 0.9$ :

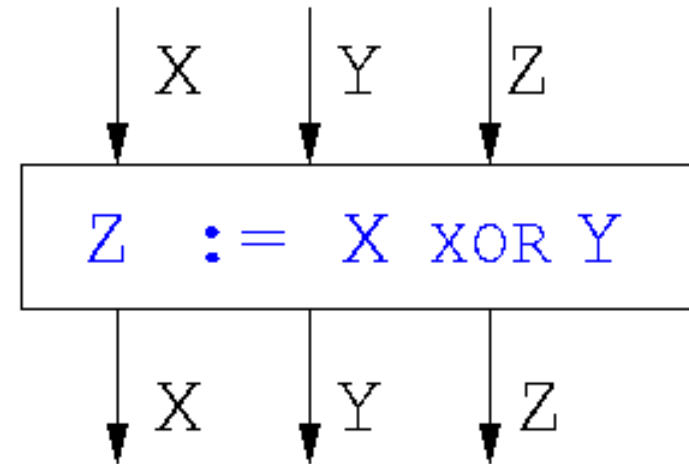
$$D/H = \{0**, 1**\}$$

$$D/L = \{**0, **1\}$$

$$f^\dagger(\mu_{|0**\cap**0})(**0) = f^\dagger(\mu_{|0*0})(**0) = 0.9$$

$$f^\dagger(\mu_{|1**\cap**0})(**0) = f^\dagger(\mu_{|1*0})(**0) = 0.1$$

- This program satisfies PWNI for  $\mu(*0*) = 0.5 = \mu(*1*)$ :
  - perfect encryption with uniform key  $Y$



---

## Conclusions and Future Work

- Distinguishing “unknown” from “secret” may allow less conservative NI properties
- Necessary to distinguish between possibilistic and probabilistic NI even for deterministic programs
- Analysis? [Giacobazzi & Mastroeni]
- Compositionality?
- Quantitative approach: use Information Theory to quantify distance from PWNl
  - Language-based analysis of use of “noise” to limit bandwidth of covert channels