# Modelling Downgrading in Information Flow Security

A. Bossi, C. Piazza, and S. Rossi

Dipartimento di Informatica
Università Ca' Foscari di Venezia

{bossi, piazza, srossi}@dsi.unive.it

CSFW'04, Asilomar, Pacific Grove, CA.

# Information Flow Security

- *Information Flow Security* aims at characterizing the *complete absence* of any information flow from high level entities to low level ones
- *Noninterference* [Goguen-Meseguer'82]: information does not flow from high to low if the high behavior has no effect on what can be observed at low level
- *Total Noninterference* can hardly be achieved in real systems: in order to deal with real applications, it is often necessary to admit mechanisms for downgrading or declassifying information

# Downgrading

- The term *downgrading* is used to refer to those situations in which trusted entities are permitted to move information from a higher to a lower security level.

- *Example*: there is a downgrading when the classification of a previously sensitive file is turned to unclassified by a security officer.

# Plan of the Talk

- the specification language SPA, syntax and semantics
- the security properties NDC and BNDC and P_BNDC
- a generalized unwinding condition for total noninterference
- a generalized unwinding condition admitting downgrading
- compositionality
- decidability

# The SPA syntax

| | | | |
|---|---|---|---|
| $E$ | $::=$ | $\mathbf{0}$ | *empty process* |
| | $\mid$ | $a.E$ | *prefix* |
| | $\mid$ | $E + E$ | *nondeterministic choice* |
| | $\mid$ | $E \mid E$ | *parallel composition* |
| | $\mid$ | $E \setminus v$ | *restriction* |
| | $\mid$ | $E[f]$ | *relabelling* |
| | $\mid$ | $Z$ | *constant* |

- each constant $Z$ has to be associated to a definition $Z \stackrel{\text{def}}{=} E$
- $H$ high actions and $L$ low actions

# The SPA semantics

- Semantics given through transition relations

Input $$\frac{}{a.E \xrightarrow{a} E}$$ Output $$\frac{}{\bar{a}.E \xrightarrow{\bar{a}} E}$$

Parallel $$\frac{E_1 \xrightarrow{a} E_1'}{E_1|E_2 \xrightarrow{a} E_1'|E_2} \qquad \frac{E_1 \xrightarrow{a} E_1' \quad E_2 \xrightarrow{\bar{a}} E_2'}{E_1|E_2 \xrightarrow{\tau} E_1'|E_2'}$$

- Behavioral equivalences, e.g., trace equivalence $\approx_T$ and weak bisimilarity $\approx_B$

# Noninterference for SPA processes

▷ *A general definition* [Focardi-Gorrieri '95]

$$\forall \text{ high level process } \Pi, \quad E \sim^l (E|\Pi)$$

▷ $\sim$ - equivalence relation over SPA processes

▷ $\sim^l$ - equivalence relation on low level actions

$$E \sim^l F \text{ if } E \setminus Comp(L) \sim F \setminus Comp(L)$$

where $Comp(L)$ is the complementary set of low actions $L$.

# The security properties NDC and BNDC

- *NDC: Non-Deducibulity on Compositions*

$$\forall \text{ high level process } \Pi, \quad E \approx^l_T (E|\Pi)$$

- *BNDC: Bisimulation-based Non-Deducibulity on Compositions*

$$\forall \text{ high level process } \Pi, \quad E \approx^l_B (E|\Pi)$$

- $\approx^l_T$ - trace equivalence on low actions, $\approx^l_B$ - weak bisimilarity

$$E \approx^l_* F \text{ if } E \setminus H \approx_* F \setminus H$$

# Persistent Information Flow security

- Properties NDC and BNDC are difficult to use in practice
  - NDC is PSPACE complete
  - BNDC: decidability is still an open problem
- Persistent_BNDC [Focardi-Rossi '02] is a sufficient condition for BNDC and it is decidable in polynomial time.
- Generalized Unwinding Condition [Bossi-Focardi-Piazza-Rossi'03]: a general framework for defining persistent information flow security properties

# P_BNDC

- *P_BNDC: Persistent Bisimulation-based Non-Deducubulity on Compositions*

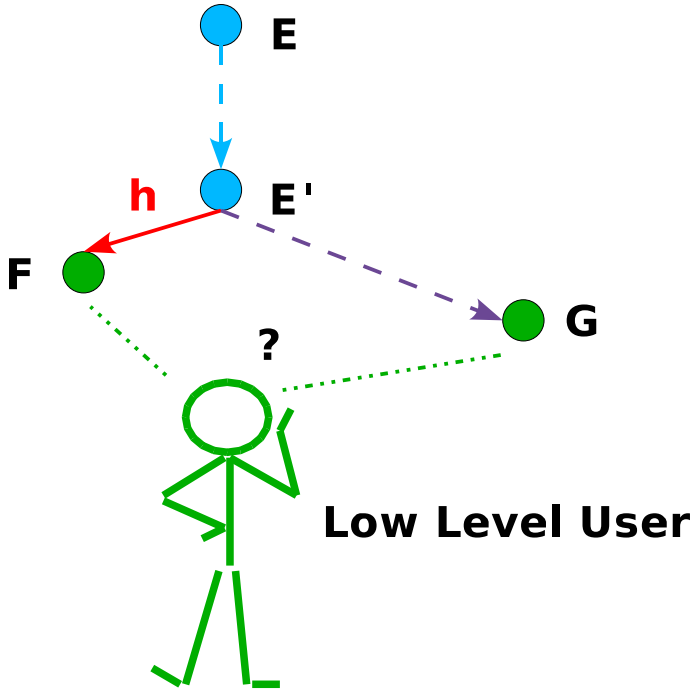
**P_BNDC**: $\forall\, E'$ reachable from $E$, $\forall$ high level process $\Pi$

$$E' \approx^{l}_{B} E'|\Pi$$

$\approx^{l}_{B}$: weak bisimilarity on low level actions

# P_BNDC and Unwinding

If $E$ reaches a state $E'$ which can perform a high level action $h$ reaching $F$ then $E'$ may also perform a sequence of invisible actions reaching $G$ such that $F$ and $G$ are indistinguishable for the low level user




**P_BNDC**: $\forall\, E'$ reachable from $E$, if $E' \xrightarrow{h} F$ then $E' \stackrel{\hat{\tau}}{\Longrightarrow} G$ and $F \approx^{l}_{B} G$

# Generalized Unwinding Condition

Let $\sim^l$ be a low level observational equivalence

Let $\dashrightarrow$ be a reachability relation

**Generalized Unwinding Condition**

$$\mathcal{W}(\sim^l, \dashrightarrow) = \{E \mid \forall E' \in Reach(E), \text{ if } E' \xrightarrow{h} F \text{ then } \exists G \text{ such that } E' \dashrightarrow G \text{ and } F \sim^l G\}$$

# Security as Unwinding Condition

- The notion of *generalized unwinding* on SPA entails a complete absence of information fbw from $H$ to $L$ since

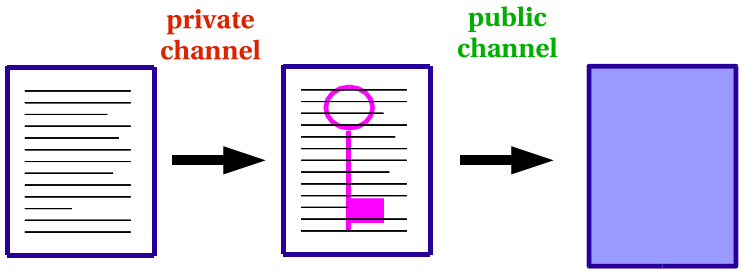
> all the high level actions ($\xrightarrow{h}$) are required to be simulated ($\dashrightarrow$) in a way which is transparent to the low level users ($\sim^{l}$).

# Downgrading - Motivation

- The notion of noninterference is too demanding when dealing with practical applications:
  - no real policy ever calls for total absence of information flow over any channel.
- In many practical applications confidential data can flow from high to low provided that the flow is not direct and it is controlled by the system, i.e., a trusted part of the system can control the downgrading of sensitive information.

# Downgrading - an Example

- A high level user edits a file and sends it through a private channel to an encrypting protocol
- the encrypting protocol encrypts the file and sends it through a public channel




- the encryption ensures that the low users cannot read the data.
- the encrypting protocol represents the trusted part of the system which controls the flow from high to low.

# Noninterference and Downgrading

**Question:** How Noninterference can be modified in order to deal with processes admitting downgrading ?

We need to extend the SPA language with a set of downgrading actions which are used to model the behavior of a trusted component

**Intransitive noninterference:** noninterference under an intransitive security policy

$$H \rightsquigarrow D \quad D \rightsquigarrow L \quad \text{but} \quad H \not\rightsquigarrow L$$

# The SPA$^{D}$ Language

- The SPA$^{D}$ language is obtained from CCS by partitioning the set of visible actions into
  - H - set of high level actions
  - L - set of low level actions
  - D - set of of downgrading actions
- It is reasonable to assume that an attacker cannot simulate the trusted part of the system, i.e., it cannot perform the actions in $D$.
- Moreover, we can assume that the low level users cannot observe the actions performed by the trusted part.

# Towards a Generalization of Noninterference

- By generalizing the definition of Noninterference we obtain

$$\forall \text{ high level process } \Pi, \quad E \sim^l (E|\Pi)$$

- $\sim$ - equivalence relation over SPA$^{\mathrm{D}}$ processes
- $\sim^l$ - equivalence relation on low level actions

$$E \sim^l F \quad \text{if} \quad E\backslash HD \sim F\backslash HD$$

**Is this enough to prevent all uncontrolled flows ?**

# Example 1 - The encrypting protocol

$$Enc = file_h.enc_d.\overline{file_l}.\mathbf{0}$$

- If we consider any possible high level process $\Pi$ we get that

$$Enc \setminus HD \approx_B \mathbf{0} \approx_B (Enc|\Pi) \setminus HD$$

which means that $Enc$ satisfies BNDC in SPA$^D$.

# Example 2 - The encrypting protocol

$$Enc = file_h.enc_d.\overline{ok_h}.\overline{file_l}.\mathbf{0}$$

Again, for any possible high level process $\Pi$

$$Enc \setminus HD \approx_B \mathbf{0} \approx_B (Enc|\Pi) \setminus HD$$

i.e., $Enc$ satisfies BNDC in SPA$^D$.

- However, the action $\overline{ok_h}$ causes an uncontrolled information flow from high to low, but this flow is not revealed by BNDC.

# Generalized Unwinding in the SPA$^{D}$ language

Let $\sim^l$ be a low level observational equivalence

Let $\dashrightarrow$ be a reachability relation

**Generalized Unwinding**

$$\mathcal{W}^D(\sim^l, \dashrightarrow) = \{E \mid \forall E' \in Reach(E), \text{ if } E' \xrightarrow{h} F \text{ then } \exists G \text{ such that } E' \dashrightarrow G \text{ and } F \sim^l G\}$$

where $F \sim^l G$ is equivalent to $F \setminus HD \sim G \setminus HD$.

# Generalized Unwinding and Intransitive Noninterference

$H \rightsquigarrow D$ The fact that the low level observation equivalence $\sim^l$ does not care about the actions in $D$ implies that the flows from $H$ to $D$ are allowed

$D \rightsquigarrow L$ The fact that the unwinding condition imposes constraints only on the high level transitions ($\xrightarrow{h}$) implies that the flows from $D$ to $L$ are also allowed

# Compositionality

We proved general compositionality properties of our unwinding framework with respect to the SPA$^D$ operators. For instance:

Let $E, F$ be SPA$^D$ processes. If $E, F \in$ DP_BNDC, then

- $a.E \in$ DP_BNDC, for all $a \in L \cup \{\tau\}$;
- $E \backslash v \in$ DP_BNDC, for any set of visible actions $v$;
- $E[g] \in$ DP_BNDC, for all relabelling function $g$.

Moreover, if $E$ and $F$ cannot synchronize on downgrading actions then

- $E \mid F \in$ DP_BNDC.

# Secure Refi nement

- We studied conditions ensuring that the security properties obtained as instances of our unwinding framework are preserved under refinement
- we considered two forms of refinement:
  - horizontal refinement: i.e., preorders relations, such as trace inclusion, which aim at removing possible sources of nondeterminism
  - vertical refinement: replacement of abstract actions by processes which represent their implementation.

# Decidability and Complexity

Let $E$ be a SPA$^D$ process.

$$E \in \mathcal{W}^D(\sim^l, \dashrightarrow) \text{ iff } \forall E' \in Reach(E),\ E' \setminus D \in \mathcal{W}(\sim^l, \dashrightarrow).$$

- By exploiting this property it is possible to decide $E \in DP\_BNDC$ in time $O(n^3)$ and space $O(n^2)$, where $n$ is the number of states of the LTS associated to $E$.

# Conclusion

- We defined a general unwinding framework to model both transitive and intransitive noninterference properties
- We proved general compositionality properties of our unwinding framework with respect to the $\mathrm{SPA}^{D}$ operators
- We studied conditions ensuring that the security properties obtained as instances of our unwinding framework are preserved under refinement
- We proposed a decision procedure to check properties in polynomial time

**Future Work** : apply our generalized unwinding framework to different settings, e.g., process algebras for mobility, imperative and multi-threaded languages.

# Downgrading in the literature

- Downgrading for deterministic systems
  - *conditional noninterference* [Goguen-Messeguer'84, Haigh-Young'87]
  - *intransitive noninterference* [Rushby'92, Pinsky'95]
- Downgrading for distributed systems and based on traces
  - *intransitive noninterference* [Roscoe-Goldsmith'99, Mantel'01]
  - *intransitive probabilistic noninterference* [Backes-Pfitzmann'03]
  - *admissible flows* [Giambiagi-Dams'00, Mullins'00]
- Downgrading for distributed systems and based on stronger equivalences
  - *partial noninterference* [Rayn-Schneider'01]
  - *robust declassifi cation* [Zdancewic-Myers'01]
  - *bisimulation-based admissible interference* [Lafrance-Mullins'02]