On dynamic flow-sensitive floating-label systems

Pablo Buiras\textsuperscript{1}, Deian Stefan\textsuperscript{2},
and Alejandro Russo\textsuperscript{1}

\textsuperscript{1}CHALMERS \textsuperscript{1} \hspace{2cm} \textsuperscript{2}STANFORD UNIVERSITY

COINS PhD student seminar
Tromsø, October 2014
Security lattice

Arrows indicate **allowed** flows

\[ L \leq L \quad H \leq H \quad L \leq H \]
Logging and IFC

Flow-insensitive:
Fixed mapping from memory locations to security labels

Flow-sensitive:
Labels can change while the program runs
Our contributions

Flow Insensitive

Flow Sensitive

Dynamic

Static

Hunt, Sands POPL 06

Floating-label systems

Traditional Denning-style Type systems

LIO
Flow-insensitive LIO
Floating label

Flow insensitive:
Labels don’t change

\[ l_{\text{init}} \cup l_1 \sqsubseteq l_3 \]
Label creep

LIO COMPUTATION

$H \leq L$

$H \Leftarrow v_1 \rightarrow v_2 \rightarrow H, v_2 \rightarrow H, 0 \rightarrow L, 0$
Label creep (2)

LIO COMPUTATION

Fresh environment

\[ L \preceq L \]

\[ H \leq H \]

\[ L \leq L \]
Flow-sensitive LIO
Naïve flow-sensitivity

• Change label when writing to the reference

Label becomes a covert channel
Label on the label

• We must protect the label with another label!

Invariant: $LOL \leq Label$

• LOL = current label at creation time
• Upgrades must be done **before** raising the current label
• Explicit **upgrade** operation (as in e.g. [Hedin, Sabelfeld SAC 14])

Prevents sensitive upgrades (similar to NSU)
LIO COMPUTATION

\[ l_{init} \cup lol \]

\[ \text{labelOf} \]

\[ lol \quad l \quad v \]
Embedding

Flow-insensitive LIO

Flow-sensitive LIO
• We can do this in the FI fragment of LIO!
Embedding of read

LIO COMPUTATION

$l_{init} \cup lol \cup l$
What we got

LIO + FS

FI AND FS REFERENCES IN ONE SYSTEM
CONCURRENCY
SOUNDNESS FROM EMBEDDING
What we learnt

Flow sensitivity is tricky but

- First-class FI labelled references
- Fresh environments

flow sensitivity
Related Work

Flow Insensitive

Flow Sensitive

Dynamic

Static

LIO

NSU [Zdancewic 02]

PU [Austin, Flanagan PLAS 10]

Floating-label systems

Traditional Denning-style Type systems

JSFlow
Comparison with Related Work

- No-sensitive-upgrades [Zdancewic 02] can be encoded in a flow-insensitive enforcement.
- Hard to compare with permissive-upgrades [Austin, Flanagan PLAS 2010].
- *Label on the label*
  - Isomorphic to existence security labels [Hedin et al CSF 2012] [Rafnsson, Sabelfeld CSF 2013]