A Decentralized Model for Information Flow Control Andrew C. Myers and Barbara Liskov, 1997

September 23, 2015

Mikael Elkiær Christensen michrill@student.aau.dk

Department of Computer Science Aalborg University Denmark

AAUgraphics/aau₁ogonew

Introduction

Decentralized Label Model

> Mikael Elkiær Christensen

Introduction

What it is not What it is How it differs

DLM Basics

Terminology

Key Principl

Example

Advanced

Future Works

The result of this paper is a model for controlling information flow: Decentralized Label Model (DLM).

Decentralized Label Model

Mikael Elkiær Christensen

What it is not

What it is How it diff

OLM Basic

DLM Basic

Labels

Key Principl

Example Code Example

Advanced

Future Works

It is not:

Department of Computer Science Aalborg University

Decentralized Label Model

Mikael Elkiær Christensen

What it is not

How it differ

DLM Basics

Labels

Key Principle

Example Code Example

Advanced

Future Works

It is not:

Access Control

Decentralized Label Model

> Mikael Elkiær Christensen

Introduction What it is not

How it differ

DLM Basics

Labels

Key Princip

Code Example

Advanced

Future Works

It is not:

- ► Access Control
- ► Authentication, Authorization, Confidentiality, Integrity.

Department of Computer Science Aalborg University Departs

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is How it differ

DLM Basics

Terminolog

Labels

Key Princip

Evennele

Code Exan

Advanced

Conclusion

It is not:

- ► Access Control
- ► Authentication, Authorization, Confidentiality, Integrity.

This means that DLM will not ensure:

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is

DLM Basic

Terminolog

Labels Vau Drinair

Example

Advanced

Conclusion
Future Works

It is not:

- ► Access Control
- ► Authentication, Authorization, Confidentiality, Integrity.

This means that DLM will not ensure:

secure communication between applications

Department of Computer Science Aalborg University Departs

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is

DLM Basic

Terminolog

Labels Vou Brinnin

Example

Code Exam

Advanced

Future Works

It is not:

- ► Access Control
- ► Authentication, Authorization, Confidentiality, Integrity.

This means that DLM will not ensure:

- secure communication between applications
- ► limited access to data once released

Decentralized Label Model

> Mikael Elkiær Christensen

Untroduction What it is no

What it is

How it differs

DLM Basic

Labels

Example

Advanced

Future Works

It is:

Department of Computer Science Aalborg University Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is

How it differs

DLM Basics

Labels

Example

Code Example

Advanced

Eutura Marka

It is:

► Information Flow Control

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is

How it diffe

DLM Basics

Labels

Key Principl

Example

Code Example

Advanced

(3)

It is:

- ► Information Flow Control
- Decentralized

Decentralized Label Model

Mikael Elkiær Christensen

Introduction

What it is not

What it is not

How it diffe

DLM Basics

Torminology

Labels

Key Principl

Example

Advanced

Euturo Works

3 It is:

- ► Information Flow Control
- Decentralized

This means that DLM will help ensuring:

Decentralized Label Model

Mikael Elkiær Christensen

What it is

DLM Basics

Advanced

It is:

- Information Flow Control
- Decentralized

This means that DLM will help ensuring:

not releasing sensitive data

Decentralized Label Model

Mikael Elkiær Christensen

What it is

Advanced

It is:

- ▶ Information Flow Control
- Decentralized

This means that DLM will help ensuring:

- not releasing sensitive data
- not implicitly releasing sensitive data

Decentralized Label Model

Mikael Elkiær Christensen

What it is

Advanced

It is:

- Information Flow Control
- Decentralized

This means that DLM will help ensuring:

- not releasing sensitive data
- not implicitly releasing sensitive data
- not giving away hints of inner workings

Decentralized Label Model

> Mikael Elkiær Christensen

Introduction
What it is not
What it is

How it differs

How it differs

Terminology Labels

Key Principl

Example Code Example

Advanced

Future Works

Decentralized Label Model

> Mikael Elkiær Christensen

How it differs

DLM Basics

Advanced

DLM differs from previous solutions as it is:

decentralized

Decentralized Label Model

> Mikael Elkiær Christensen

Introduction
What it is not

How it differs

DLM Basics

Terminolog

Koy Princin

Example

Code Examp

Advanced

Future Works

- decentralized
- ► less restrictive of allowed computations

Decentralized Label Model

Mikael Elkiær Christensen

Introduction
What it is not
What it is

How it differs

How it differ

Labels

Key Princin

Example

Advanced

Auvanceu

Future Works

- decentralized
- less restrictive of allowed computations
- ▶ not completely disallowing inter-application communication

Decentralized Label Model

Mikael Elkiær Christensen

Introduction
What it is not
What it is

How it differs

DI M Rasi

Termino

Labelo

Example

Code Examp

Advanced

Future Works

- decentralized
- less restrictive of allowed computations
- ► not completely disallowing inter-application communication
- meant to extend current programming languages with data flow annotations

DLM Basics

Decentralized Label Model

Mikael Elkiær Christensen

Introduction

What it is How it differ

DLM Basics

Terminology Labels

Example

Example Code Exampl

Advanced

Future Works

DLM provides both static and dynamic checking of data flow.

Department of Computer Science Aalborg University Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Introduction
What it is not
What it is

DLM Basics

Terminology

Key Principle

Example Code Example

Advanced

Future Works

Principals represent users and other authoritative entities (e.g. groups or roles).

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is How it differs

DLM Basics Terminology

Labels

Evample

Code Example

Advanced

Future Works

Principals represent users and other authoritative entities (e.g. groups or roles).

Values are entities computations can manipulate.

Decentralized Label Model

Mikael Elkiær Christensen

Introduction
What it is no

What it is How it differs

DLM Basics

Terminology

Key Principle

Example Code Examp

Advanced

Future Works

Principals represent users and other authoritative entities (e.g. groups or roles).

Values are entities computations can manipulate.

Slots are value-holders (e.g. variables, objects, and other storage locations).

Decentralized Label Model

Mikael Elkiær Christensen

What it is not

How it differs

DLM Basics Terminology

Labels

Key Principl

Example Code Example

Advanced

riavarioca

Principals represent users and other authoritative entities (e.g. groups or roles).

Values are entities computations can manipulate.

Slots are value-holders (e.g. variables, objects, and other storage locations).

Input channels are read-only sources that allow information to enter the system.

Decentralized Label Model

Mikael Elkiær Christensen

What it is not

How it differ

DLM Basics Terminology

Labels

Key Principle

Code Example

Advanced

Future Works

Principals represent users and other authoritative entities (e.g. groups or roles).

Values are entities computations can manipulate.

Slots are value-holders (e.g. variables, objects, and other storage locations).

Input channels are read-only sources that allow information to enter the system.

Output channels are information sinks that transmit information outside the system.

Decentralized Label Model

Mikael Elkiær Christensen

What it is now What it is

How it differs

Terminology

Key Principle

Example Code Example

Advanced

Conclusion
Future Works

Principals represent users and other authoritative entities (e.g. groups or roles).

Values are entities computations can manipulate.

Slots are value-holders (e.g. variables, objects, and other storage locations).

Input channels are read-only sources that allow information to enter the system.

Output channels are information sinks that transmit information outside the system.

Labels are attached to values, slots or channels (more to follow).

DLM Basics

Decentralized Label Model

Mikael Elkiær Christensen

What it is not What it is

DLM Basics Terminology

Labels

Key Princip

Example
Code Example

Advanced

Future Works

A label ${\bf L}$ is a set of owners, where each owner denotes its readers, e.g.:

$$\{o_1:r_1,r_2;o_2:r_2,r_3\}$$

where o_1, o_2, r_1, r_2, r_3 are principals.

DLM Basics

Decentralized Label Model

Mikael Elkiær Christensen

Untroduction
What it is not
What it is
How it differs

How it differs

DLM Basics

Terminology

Labels Key Principle

Example

Advanced

....

Future Works

A label ${\bf L}$ is a set of owners, where each owner denotes its readers, e.g.:

$$\{o_1: r_1, r_2; o_2: r_2, r_3\}$$

where o_1, o_2, r_1, r_2, r_3 are principals.

The effective reader set of a label is the intersection of every reader, for L it is $\{r_2\}$.

Decentralized Label Model

Mikael Elkiær Christensen

Introduction

What it is not

DLM Basics

Terminology

Kev Principles

Example Code Example

Advanced

Future Works

► Labels are comparable:

▶ $L_1 \sqsubseteq L_2$ signifies that L_2 is at least as restrictive as L_1 .

Decentralized Label Model

Mikael Elkiær Christensen

Introduction

What it is not What it is

DLM Basics

Terminolo

Labels

Key Principles

Example

Code Example

Advanced

- ► Labels are comparable:
 - ▶ $L_1 \sqsubseteq L_2$ signifies that L_2 is at least as restrictive as L_1 .
- ► Labels can be joined:
 - L₁ ⊔ L₂ results in a join of owners and intersection of readers.

Decentralized Label Model

Mikael Elkiær Christensen

Introduction

What it is How it differs

DLM Basics

Lahale

Key Principles

Example

Code Exampl

Advanced

- ► Labels are comparable:
 - $\blacktriangleright \ L_1 \sqsubseteq L_2 \ \text{signifies that} \ L_2 \ \text{is at least as restrictive as} \ L_1.$
- ▶ Labels can be joined:
 - L₁ ⊔ L₂ results in a join of owners and intersection of readers.
- Principals can act for other principals.

Decentralized Label Model

Mikael Elkiær Christensen

Introductio

What it is How it differs

Terminolo

Labels

Key Principles

Example

Code Exampl

Advanced

- ► Labels are comparable:
 - ▶ $L_1 \sqsubseteq L_2$ signifies that L_2 is at least as restrictive as L_1 .
- ► Labels can be joined:
 - L₁ ⊔ L₂ results in a join of owners and intersection of readers.
- Principals can act for other principals.
- Relabeling can be done, further restricting or declassifying.

Example

Decentralized Label Model

Mikael Elkiær Christensen

What it is no

How it differs

DLM Basics

Labels

Key Principle

Example

Code Example

Advanced

Future Works

hospital_example.png

Department of Computer Science Aalborg University

Example Code Example

Decentralized Label Model

Mikael Elkiær Christensen

DLM Basics

Code Example

Advanced

passwordcheker_example.png

Department of Computer Science Aalborg University Denmark

Advanced

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is How it differs

DLM Basics

Terminolog

Key Princip

Example

Code Examp

Advanced

Conclusion Future Works

- Label polymorphism
- ► Run-time labels (1b type)
- ► Protected types (protected[T])
- Inferred labels

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

How it differs

DLM Basics

Terminolog

Kov Principle

Example

Code Exampl

Advanced

Conclusion Future Works ► Decentralized Label Model

Department of Computer Science Aalborg University

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is not

What it is How it differs

DLM Basics

Terminolog

Labels

Key Principl

Example Code Example

Code Example

Advanced

Conclusion

Future Works

- Decentralized Label Model
- ► Control of information flow

Department of Computer Science Aalborg University Denmark

Decentralized Label Model

Mikael Elkiær Christensen

DLM Basics

Advanced Conclusion

- Decentralized Label Model
- Control of information flow
- Static and dynamic label checking

Department of Computer Science Aalborg University Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is no

What it is How it differs

DLM Basics

Terminolog

Key Principl

Example Code Evens

Code Examp

Advanced Conclusion

Future Works

- Decentralized Label Model
- ► Control of information flow
- Static and dynamic label checking
- Possible to extend existing programming languages

Department of Computer Science Aalborg University Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Introduction What it is no

What it is How it differs

DLM Basics

Labels
Key Principles

Example

Code Examp

Advanced

Conclusion Future Works ► Actual implementation (JIF – dead)

Decentralized Label Model

Mikael Elkiær Christensen

What it is not What it is

DLM Basics

Labels

Key Principle

Example Code Examp

Code Exampl

Advanced

- ▶ Actual implementation (JIF dead)
- Support for user-defined data abstractions

Decentralized Label Model

Mikael Elkiær Christensen

What it is not What it is What it is

DLM Basics

Labels

Key Principle

Example

Advanced

Conducios

- ► Actual implementation (JIF dead)
- Support for user-defined data abstractions
- Formal proofs

Decentralized Label Model

Mikael Elkiær Christensen

What it is not What it is

DLM Basics

Labels

Key Principl

Example

Code Examp

Advanced

Conclusion Future Works

- ► Actual implementation (JIF dead)
- Support for user-defined data abstractions
- Formal proofs
- Network systems

Decentralized Label Model

Mikael Elkiær Christensen

What it is not
What it is
What it is

DLM Basics

Labels

Key Principle

Example

Code Examp

Advanced

Conclusion Future Works

- ► Actual implementation (JIF dead)
- Support for user-defined data abstractions
- Formal proofs
- ► Network systems
- ▶ Threading

Questions?

