A Decentralized Model for Information Flow Control

Andrew C. Myers and Barbara Liskov, 1997

September 23, 2015

Mikael Elkiær Christensen

michri11@student.aau.dk

Department of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

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

Decentralized Label Model

Mikael Elkiær Christensen

It is not:

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

It is not:

- Access Control

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

It is not:

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

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

It is not:

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

This means that DLM will not ensure:

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model
Mikael Elkiær Christensen

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
Denmark

Introduction
What it is not

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

It is:

Decentralized Label Model
Mikael Elkiær Christensen

It is:

- Information Flow Control

Department of Computer Science
Aalborg University
Denmark

It is:

- Information Flow Control
- Decentralized

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

It is:

- Information Flow Control
- Decentralized

This means that DLM will help ensuring:

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model
Mikael Elkiær Christensen

It is:

- Information Flow Control
- Decentralized

This means that DLM will help ensuring:

- not releasing sensitive data

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model
Mikael Elkiær Christensen

3

It is:

- Information Flow Control
- Decentralized

This means that DLM will help ensuring:

- not releasing sensitive data
- not implicitly releasing sensitive data

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

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

Department of Computer Science
Aalborg University
Denmark

Department of Computer Science
Aalborg University
Denmark

DLM differs from previous solutions as it is:

Decentralized Label Model

Mikael Elkiær Christensen

DLM differs from previous solutions as it is:

- decentralized

Department of Computer Science
Aalborg University
Denmark

DLM differs from previous solutions as it is:

- decentralized
- less restrictive of allowed computations

Decentralized Label Model

Mikael Elkiær Christensen

DLM differs from previous solutions as it is:

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

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model
Mikael Elkiær Christensen

DLM differs from previous solutions as it is:

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

Department of Computer Science
Aalborg University
Denmark

DLM Basics

DLM provides both static and dynamic checking of data flow.

Decentralized Label Model
Mikael Elkiær Christensen

Principals represent users and other authoritative entities.

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model
Mikael Elkiær Christensen

Principals represent users and other authoritative entities.

Values are entities computations can manipulate.

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Principals represent users and other authoritative entities.

Values are entities computations can manipulate.

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

Department of Computer Science
Aalborg University
Denmark

Principals represent users and other authoritative entities.

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

Principals represent users and other authoritative entities.

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.

Department of Computer Science
Aalborg University
Denmark

Principals represent users and other authoritative entities.

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).

Decentralized Label Model

Mikael Elkiær Christensen

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Department of Computer Science
Aalborg University
Denmark

Example

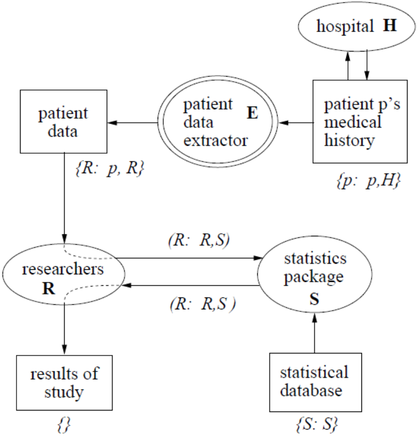

Figure 1: Medical Study Scenario

Example
Code Example

```
pinfo = record [ names, passwords: string{chkr: chkr} ]

check_password (db: array[pinfo{⊥}]{⊥},
                user: string {⊥},
                password: string{client: chkr})
    returns (ret: bool{client: chkr})
    % Return whether password is the password of user

    i: int {chkr: chkr} := 0                     % ⊥
    match: bool {client: chkr;                   %
                 chkr: chkr} := false            % ⊥
    while i < db.length() do                     % ⊥
      if db[i].names = user &                    % ⊥
        db[i].passwords = password then          %
          match := true                          % {client: chkr;
      end                                        %   chkr: chkr}
      i := i + 1                                 % ⊥
    end
    ret := false                                     % ⊥
    if_acts_for(check_password, chkr) then           % ⊥
      ret := declassify(match, {client: chkr})       % ⊥
    end
end check_password
```

Figure 6: Annotated password checker

Advanced

Department of Computer Science
Aalborg University
Denmark

Conclusion

Department of Computer Science
Aalborg University
Denmark

Decentralized Label Model

Mikael Elkiær Christensen

Department of Computer Science
Aalborg University
Denmark

Questions?

AALBORG UNIVERSITY
DENMARK