

THE CHINESE WALL SECURITY POLICY

Dr. David F.C. Brewer and Dr. Michael J. Nash, 1989

November 06, 2015

Mikael Elkiær Christensen
michri11@student.aau.dk

Department of Computer Science
Aalborg University
Denmark



AALBORG UNIVERSITY
DENMARK



Who is the enemy?

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules

1

12

Who is the enemy?

CHINESE WALL

Mikael Elkiær
Christensen

Introduction

1

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules



Who is the enemy?

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

1

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules



CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

2

- ▶ Coined in 1929 following the Wall Street crash
- ▶ Chinese Wall policies are already in use
 - ▶ Not necessarily digital
 - ▶ Can have authority of law
- ▶ Other terms, as some find the original offensive
 - ▶ "Screen", "firewall", "cone of silence", and "ethical wall"



Relevance

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background

Relevance

3

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

- ▶ Before 1989, most security policies were military
 - ▶ E.g. Bell-LaPadula (more about this later)
- ▶ Need of something that holds up in court
- ▶ Relevant anywhere conflicts of interest can exist

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules

4

- ▶ Proposed by Bell and LaPadula in 1973
- ▶ Security policy model
- ▶ Designed for military use

CHINESE WALL

Mikael Elkiær
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

5

- ▶ **Security Label**
- ▶ **Object** – Data or program
 - ▶ **Classification** – Minimum security level
 - ▶ **Category** – Security group(s)
- ▶ **Subject** – Person or program
 - ▶ **Clearance** – Maximum security level
 - ▶ **Need-to-know** – Security group(s)

12

Access rules

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

6

Simple security: access is granted only if the subject's clearance is *greater* than the object's classification and the subject's need-to-know *includes* the object's category(ies)

***-property:** write access is granted only if the output object's classification is *greater* than the classification of all input objects, and its category *includes* the category(ies) of all input objects.

Example

CHINESE WALL

Mikael Elkiær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

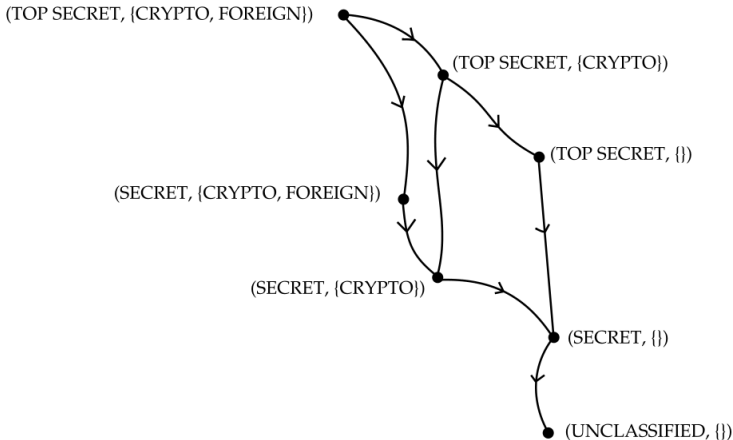
Terminology
Access rules

Example

7

Chinese Wall

Abstract Example
Hierarchical Example
Access rules



Example (2)

CHINESE WALL

Mikael Elkiær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

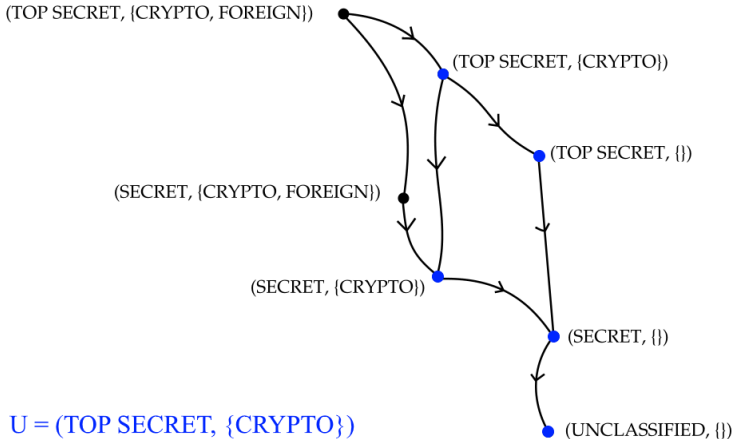
Terminology
Access rules

Example

8

Chinese Wall

Abstract Example
Hierarchical Example
Access rules





Fundamentals

CHINESE WALL

Mikael Elkiær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules

9

- ▶ Terminology
 - ▶ Object
 - ▶ Subject
 - ▶ Company Dataset (CD)
 - ▶ Conflict of Interest Class (COIC)
- ▶ Main difference: At most one CD in each COIC, starting with free choice

12



Abstract Example

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules

10

12



Hierarchical Example

CHINESE WALL

Mikael Elkjær
Christensen

Introduction

Background
Relevance

Bell-LaPadula

Terminology
Access rules
Example

Chinese Wall

Abstract Example
Hierarchical Example
Access rules

11

12

CHINESE WALL

Mikael Elkiær
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

12

Simple security

Access is only granted if the object requested

1. is in the *same company dataset* as an object already accessed by that subject, i.e. within the Wall, *or*
2. belongs to an *entirely different conflict of interest class*.

*-property

Write access is only permitted if

1. access is permitted by the simple security rule, and
2. no object can be read which is in a different company dataset to the one for which write access is requested and contains unsanitized information.

Questions?



AALBORG UNIVERSITY
DENMARK