

# 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 Elkiær  
Christensen

### Introduction

1

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

### Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

# 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  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion



# Who is the enemy?

## CHINESE WALL

Mikael Elkjær  
Christensen

1

### Introduction

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

### Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion



## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

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"

## CHINESE WALL

Mikael Elkjær  
Christensen

Introduction

Background

**Relevance**

3

Bell-LaPadula

Terminology

Access rules

Example

- ▶ 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

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

## Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

4

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

# Terminology

## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

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)

17



# Access rules

## CHINESE WALL

Mikael Elkiær  
Christensen

### Introduction

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

6

### Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

**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  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

(TOP SECRET, {CRYPTO, FOREIGN})

(TOP SECRET, {CRYPTO})

(TOP SECRET, {})

(SECRET, {CRYPTO, FOREIGN})

(SECRET, {CRYPTO})

(SECRET, {})

(UNCLASSIFIED, {})

## Example (2)

### CHINESE WALL

Mikael Elkiær  
Christensen

#### Introduction

Background  
Relevance

#### Bell-LaPadula

Terminology  
Access rules

#### Example

8

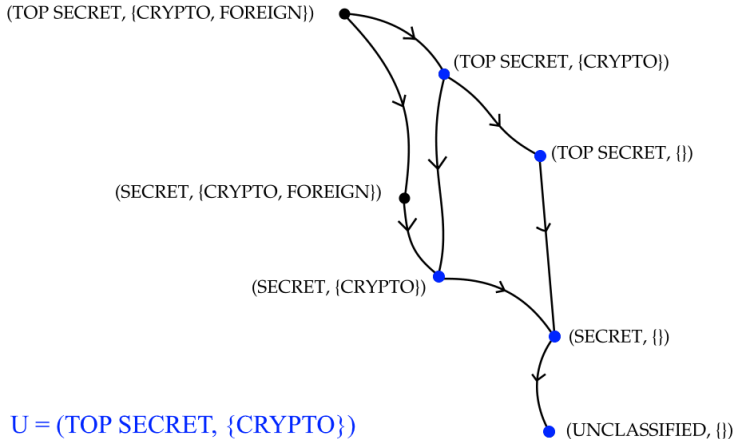
#### Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

#### Relevance today

#### Conclusion

17



# Fundamentals

## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

- ▶ Terminology
  - ▶ **Object**
  - ▶ **Subject**
  - ▶ **Company Dataset (CD)**
  - ▶ **Conflict of Interest Class (COIC)**
- ▶ Two important properties
  - ▶ **Mandatory**
  - ▶ **Free Choice**

9

17



# Abstract Example

## CHINESE WALL

Mikael Elkiær  
Christensen

### Introduction

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

### Chinese Wall

**Abstract Example**  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

10

Blackboard time...

17

# Hierarchical Example

## CHINESE WALL

Mikael Elkiær  
Christensen

### Introduction

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

### Chinese Wall

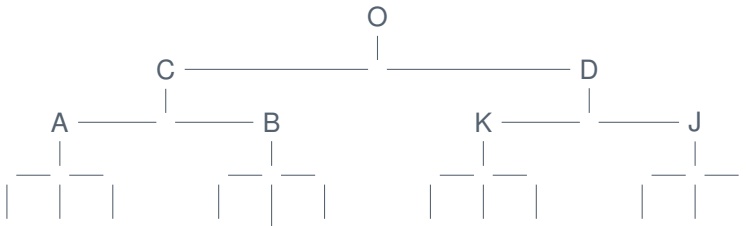
Abstract Example  
**Hierarchical Example**  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

11

Users X, Y



17

## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

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.

17

## CHINESE WALL

Mikael Elkjær  
Christensen

Introduction

Background  
Relevance

Bell-LaPadula

Terminology  
Access rules  
Example

Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules

Sanitization  
Comparison with BLP  
Clark and Wilson

Relevance today

Conclusion

- ▶ Not all data within a company is sensitive
- ▶ It can be necessary to share data between users
- ▶ Assumed possible by de-privatizing
- ▶ Simply solved by adding extra CD within its own COIC

13

17





# Comparison with BLP

## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

Relevance today

Conclusion

- ▶ Important to show power of CW, compared to BLP
- ▶ Two important properties: mandatory and free choice
- ▶ It is possible to use BLP, but it cannot satisfy both properties

14

17



# Clark and Wilson

## CHINESE WALL

Mikael Elkiær  
Christensen

Introduction

Background

Relevance

Bell-LaPadula

Terminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Example

Access rules

Sanitization

Comparison with BLP

Clark and Wilson

15

Relevance today

Conclusion

- ▶ General rules for commercial data processing
- ▶ Important distinction between *users* and *processes*



# Relevance today

## CHINESE WALL

Mikael Elkiær  
Christensen

### Introduction

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

### Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

- ▶ Business
- ▶ Cloud computing (think servers and VMs)
- ▶ Basically anywhere there can be conflicts of interest

16

17

# Conclusion

## CHINESE WALL

Mikael Elkiær  
Christensen

### Introduction

Background  
Relevance

### Bell-LaPadula

Terminology  
Access rules  
Example

### Chinese Wall

Abstract Example  
Hierarchical Example  
Access rules  
Sanitization  
Comparison with BLP  
Clark and Wilson

### Relevance today

### Conclusion

- ▶ Important in its own right
- ▶ Differs from previous models
- ▶ Provable integrity

17

17

Questions?



**AALBORG UNIVERSITY**  
DENMARK