# THE CHINESE WALL SECURITY POLICY

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

November 06, 2015

Mikael Elkiær Christensen michrill@student.aau.dk

Department of Computer Science
Alborg University
Denmark





# Who is the enemy?

### CHINESE WALL

Mikael Elkiær Christensen

#### Introduction

Backgroun Relevance

## Bell-LaPadula

Access rules

#### Access rules

Chinese Wall

#### Austraut Example

Hierarchical Exam

Sanitization



# Who is the enemy?

### CHINESE WALL

Mikael Elkiær Christensen

## Introduction

Background Relevance

## Bell-LaPadula

Access rules

## Chinese Wall

Abstract Example
Hierarchical Example
Access rules
Sanitization





# Who is the enemy?

## CHINESE WALL

Mikael Elkiær Christensen

#### Introduction

Backgroun Relevance

### Bell-LaPadula

Terminology Access rules

### Chinese Wall

Abstract Example Hierarchical Example Access rules Sanitization







# Background

#### CHINESE WALL

Mikael Elkiær Christensen

Introducti

## Background

Relevano

#### Bell-LaPadul

Terminology Access rules

#### \_\_\_\_

Abstract Example

Hierarchical Examp Access rules

Sanitizatio

# ► 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"



Mikael Elkiær Christensen

ntroductio

Backgrou

Relevance

Bell-LaPadu

Don Lar ado

Access rules

Abstract Evenne

Hierarchical Exampl

Access rules

Sanitizati

► 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



Mikael Elkiær Christensen

ntroductio

Backgrour Relevance

### Bell-LaPadula

Terminology Access rules

#### Chinese Wall

Abstract Example

Hierarchical Exam

Access rules

Sanitizatio

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

Department of Computer Science Aalborg University Denmark



#### Mikael Elkiær Christensen

#### Introductio

Backgroun Relevance

#### Bell-LaPadı

#### Terminology

F.......

#### Chinasa W

Abstract Example

Hierarchical Examp

Access rules

- 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)

Mikael Elkiær Christensen

Introduction

Backgroun Relevance

Bell-LaPadu

Torminology

Access rules

Chinese Wall

Abstract Example

Hierarchical Examp

Access rules

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.



#### Mikael Elkiær Christensen

straduatio

Backgrour Relevance

#### Bell-LaPadu

Terminology

Access rules

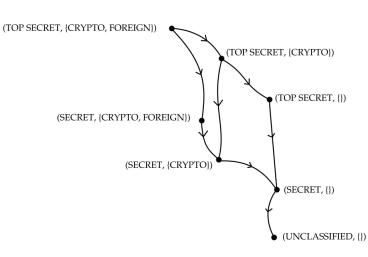
#### Example

#### Chinese Wall

Abstract Example

Hierarchical Examp

Caritiantian





# Example (2)

#### CHINESE WALL

#### Mikael Elkiær Christensen

Backgrour Relevance

#### Bell-LaPadu

Terminology

Access rules

#### Example

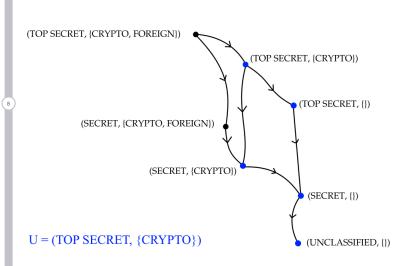
#### Chinese Wall

Abstract Example

Hierarchical Exam

Access rules

0 11 11



Department of Computer Science Aalborg University Denmark



# **Fundamentals**

#### CHINESE WALL

#### Mikael Elkiær Christensen

ntroductio

Backgroun Relevance

#### Bell-LaPac

Terminology

Access rule

#### Chinese Wall

Abstract Example

Access rules

Sanitization

# Terminology

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



# Abstract Example

#### CHINESE WALL

#### Mikael Elkiær Christensen

#### straduatio

Backgroun Relevance

## Bell-LaPadula

Access rule

# Chinese Wall

### Abstract Example

Hierarchical Example Access rules See blackboard...



# Hierarchical Example

### CHINESE WALL

Mikael Elkiær Christensen

## Chinese Wall

#### Hierarchical Example

Users X, Y

Department of Computer Science Aalborg University Denmark

13

Mikael Elkiær Christensen

#### Introductio

Backgroun Relevance

#### Bell-LaPadu

Torminology

reminiology

Example

### Chinese Wall

Abstract Example

#### Access rules

Sanitizatio

# Simple security

Access is only granted if the object requested

- 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

- 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.



# Sanitization

#### CHINESE WALL

#### Mikael Elkiær Christensen

#### ntroductio

Backgroun Relevance

#### Bell-LaPadı

Terminology

Access rule

#### 01::----

Abstract Evampl

Hierarchical Ev

Access rules

Sanitization

- ▶ 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

# Questions?

