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

Terminology

Access rule

Chinese Wall

hetraet Evamo

Hierarchical Examp

Access rules

-

Comparison with E

Clark and Wilse

Relevance today

Conclusion

Department of Computer Science Aalborg University Denmark



Who is the enemy?

CHINESE WALL

Mikael Elkiær Christensen

Introduction

Relevance

Bell-LaPadula

Access rules

Chinese Wall

Abstract Example

Hierarchical Examp

Access rules

Comparison with E

Clark and Wilson

Relevance today

Conclusio





Who is the enemy?

CHINESE WALL Mikael Elkiær Christensen

Introduction

Background Relevance

Bell-LaPadula

Access rules

Chinese Wall

Abstract Example

Access rules

Comparison with Bl

Relevance today

Conclusion







Mikael Elkiær Christensen

ntroductio

Background

Relevanc

Bell-LaPadu

Terminology Access rules

Chinese Wal

Abstract Exampl

A -----

Access rules

Comparison with B

Relevance today

Conclusio

- ► 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"

Department of Computer Science Aalborg University Departs



Mikael Elkiær Christensen

Introductio

Relevance

Relevance

Bell-LaPadu

Terminology

Access rules

Chinese Wall

Abstract Example

Hierarchical Example
Access rules

Sanitization

Comparison with Bl Clark and Wilson

Relevance today

Conclusion

- ► 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

Department of Computer Science Aalborg University Depmark

17

Mikael Elkiær Christensen

ntroductio

Backgroui

Bell-LaPadula

Terminology Access rules

Chinese Wall

Abstract Example

Hierarchical Exam

Access rules

Comparison with B

Relevance today

Conclusion

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

Department of Computer Science Aalborg University Denmark

17



Mikael Elkiær Christensen

Introduction

Backgroun Relevance

Bell-LaPadi

Terminology

Evennel

.

Hierarchical Examp

Access rules

Sanitization

Clark and Wilso

Relevance today

Conclusion

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

Introductio

Backgroun Relevance

Bell-LaPad

Terminology

Access rules

Chinese Wa

Abstract Exampl

Hierarchical Exam

Access rules

Comparison with

Relevance toda

Conclusi

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

ntroductio

Backgroun Relevance

Bell-LaPadu

Torminology

Access rules

Example

Chinese Wall

Abstract Example

Hierarchical Examp

Access rules

Comparison with E

Relevance today

Conclusio

(TOP SECRET, {CRYPTO, FOREIGN}) (TOP SECRET, {CRYPTO}) (TOP SECRET, {}) (SECRET, {CRYPTO, FOREIGN}) (SECRET, {CRYPTO}) (SECRET, {}) (UNCLASSIFIED, {})



Example (2)

CHINESE WALL

Mikael Elkiær Christensen

ntroductio

Backgrour Relevance

Bell-LaPadu

Terminology

Access rules

Example

Chinese Wall

Abstract Example

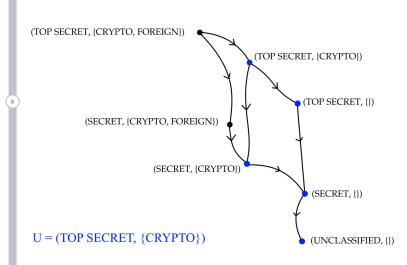
Hierarchical Examp

Access rules

Comparison with E

Relevance today

Conclusio





Fundamentals

CHINESE WALL

Mikael Elkiær Christensen

atroductio

Backgroun Relevance

Bell-LaPac

Terminology

Access rule

Evennele

Chinese Wall

Abstract Example

Hierarchical Exam

Access rules

Comparison with B

Clark and Wilso

Relevance today

Conclusio

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



Abstract Example

CHINESE WALL

Mikael Elkiær Christensen

straduatio

Backgrour Relevance

Bell-LaPadu

ierminology Access rule

Access rule

Chinese Wall

Abstract Example

Hierarchical Example
Access rules

Sanitization

Clark and Wilso

Relevance today

Conclusio

Blackboard time...

Department of Computer Science Aalborg University Denmark



Hierarchical Example

CHINESE WALL

Mikael Elkiær Christensen

Backgroun

Bell-LaPadu

Terminology Access rules

Chinese Wall

Abstract Examp

Hierarchical Example

Access rules

Comparison with E

Relevance toda

Users Johnny, NotJohnny

All objects

Banks — Petrol

OKB COB F04

DKB — ' — SOB F24 — ' — Q8

Conclusion

Department of Computer Science Aalborg University Depmark

Mikael Elkiær Christensen

ntroductio

Backgroun Relevance

Bell-LaPadu

Terminology

Terminology

Access rules

Obines Mal

Abstract Example

Access rules

Comparison with B

Relevance today

Conclusi

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.

Department of Computer Science Aalborg University



Mikael Elkiær Christensen

ntroductio

Backgroun Relevance

Bell-LaPadi

Terminology

Access rules

Example

Chinese Wall

Abstract Examp

Hierarchical Examp

Sanitization

Comparison with E

Clark and Wilson

Relevance today

Conclusio

- ▶ 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



Comparison with BLP

CHINESE WALL

Mikael Elkiær Christensen

ntroductio

Backgroun Relevance

Bell-LaPadi

Terminology

Access rules

01::----

Officese vva

Abstract Examp

Access rules

Sanitization

Comparison with BLP

Clark and Wilso

Relevance today

Conclusio

- 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

Department of Computer Science Aalborg University Denmark



Clark and Wilson

CHINESE WALL

Mikael Elkiær Christensen

ntroductio

Backgroun Relevance

Bell-LaPadu

Access rule

Access rul

Chinaga W

Crimese wan

Abstract Example

nierarchical Exam

Access rule

Sanitization

Clark and Wilson

Relevance today

Conclusio

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

Department of Computer Science Aalborg University Denmark

17



Relevance today

CHINESE WALL

Mikael Elkiær Christensen

ntroductio

Backgroun Relevance

Bell-LaPad

Terminology

Access rul

Abstract Examp

Hierarchical Exam

Access rules

Sanitization

Comparison with B

Relevance today

Conclusion

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

Department of Computer Science Aalborg University Departs

17



Conclusion

CHINESE WALL

Mikael Elkiær Christensen

atroductio

Backgroun Relevance

Bell-LaPad

Terminology

Access rul

7100000 1011

Chinese Wall

Abstract Examp

Hierarchical Exam

Access rules

Sanitization

Clark and Wilson

Relevance today

Conclusion

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

Department of Computer Science Aalborg University Denmark

Questions?

