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?

Who is the enemy?

Who is the enemy?

Background

- 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

- 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

Bell-LaPadula

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

Terminology

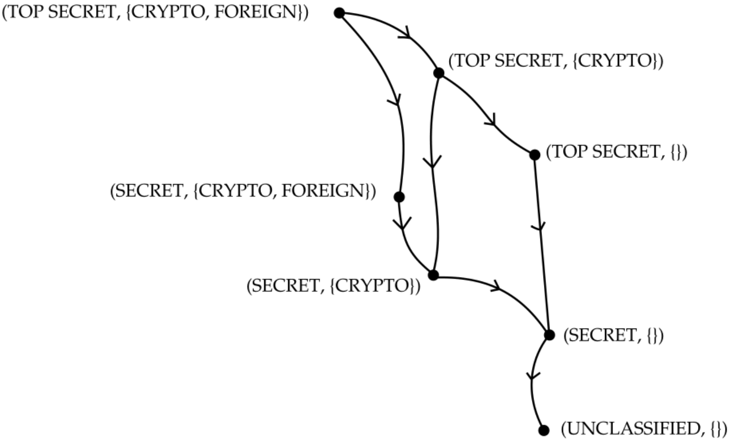
- **Security Label**
- **Object** – Data or program
  - **Classification** – Minimum security level
  - **Category** – Security group(s)
- **Subject** – Person or program
  - **Clearance** – Maximum security level
  - **Need-to-know** – Security group(s)

Access rules

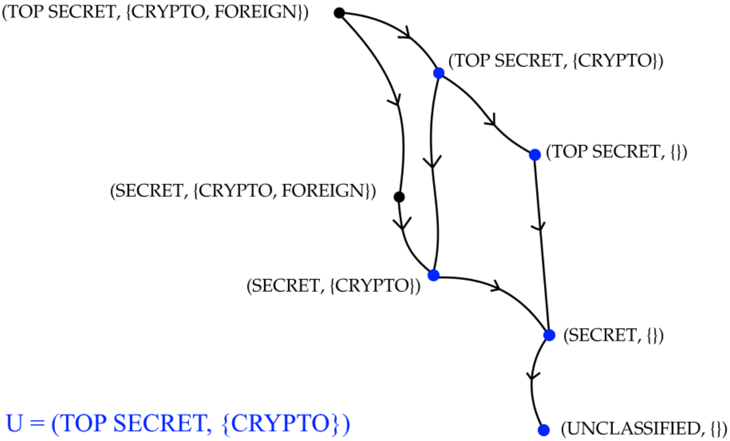
Simple security: access is granted only if the subject's clearance is *greater* than the object's classification and the subject's need-to-know *includes* the object's category(ies)

*-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.

Example


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

Example (2)



U = (TOP SECRET, {CRYPTO})

Fundamentals

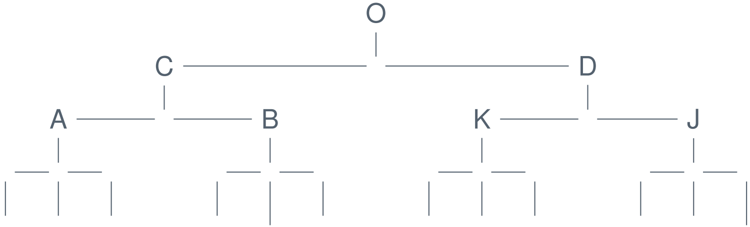
- Terminology
  - Object
  - Subject
  - Company Dataset (CD)
  - Conflict of Interest Class (COIC)
- Main difference: At most one CD in each COIC, starting with free choice

Abstract Example

See blackboard...

Hierarchical Example

Users *X*, *Y*



Access rules

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.

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?

AALBORG UNIVERSITY
DENMARK