Discretionary Access Control (DAC)

Nicola Zannone
Outline

Access Control

Discretionary Access Control

Safety Problem

DAC weaknesses
Access Control

Discretionary Access Control

Safety Problem

DAC weaknesses
Computer Security Objectives

- **Confidentiality**
  - Information disclosed only to principals authorized to know it
  - **Privacy**:
    - right to be let alone (Warren and Bradeis, 1890)
    - right of the individual to decide when, what, why and who manage his personal information (Westin, 1970)
    - freedom from unreasonable constraints on the construction of one’s own identity (Agre, 1999)

- **Integrity**
  - Information modified only by authorized principals and in authorized ways

- **Availability**
  - Information accessible when it is needed (No denial of service)
Access Control

- **Goal**: Protect confidentiality and integrity of information
- Control what a subject can do to prevent damage to the system
- Regulate the operations that can be executed by a subject on data and resources
- Typically provided as part of operating systems and of database management systems
The basic idea of access control is that there is an active subject requiring access to a passive object to perform some specific access operation.

A reference monitor grants or denies access.
Subjects

- Active entity performing operations in the system

- Subjects can be:
  - **users**: single individuals connecting to the system
  - **groups**: sets of users
  - **roles**: a function or a position within an organization
  - **processes**: executing programs on behalf of users

- Relations may exist among the various types of subject
Objects

- Any system resource
  - file, printer, etc.

- *Protection objects*: objects controlled by access control system

- Note: not all resources managed by a system need to be protected

- Advanced Objects: subjects
Access Rights

- Operations that a subject can execute on protection objects

- Each type of operation corresponds to an access right
  - access control must be able to control the specific type of operation

- The most simple example of access rights is:
  - read: look at the contents of an object
  - write: change the contents of an object

- Other types of rights depending on the resources to be protected
  - execute, select, insert, update, delete, etc.

- Advanced Rights: ownership, delegate, remove
Subjects, Objects, Access Rights in Unix

- **Subjects**: users, groups
- **Objects**: files, directories
- **Access rights**: read, write, execute
  - For files
    - read: reading from a file
    - write: writing to a file
    - execute: executing a (program) file
  - For directories
    - read: list the files within the directory
    - write: create, rename, or delete files within the directory
    - execute: enter the directory
Access Control vs. Authentication

Access Control

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication

Access Control vs. Authentication
Access Control vs. Authentication

- Completely different things

- Authentication:
  - Establishing who you are
    - whether a user possesses a certain pseudonym/attribute or not

- Access Control:
  - Establishing if a user has the right of doing a certain operation

- Authentication is necessary for access control
Policies, Models, Mechanisms

- **Policy**: define (high-level) guidelines and rules describing the accesses to be authorized by the system
- **Model**: formally define the access control specification and enforcement
- **Mechanism**: implement the policies via low level (software and hardware) functions
Separation between policies and mechanisms

- Discuss access requirements independently from their implementation.
- Compare different access control policies as well as different mechanisms that enforce the same policy.
- Design mechanisms able to enforce multiple policies.
Security policies

- **Access control** policies: define who can access a resource
  - Discretionary (DAC)
  - Mandatory (MAC)
  - Role-based (RBAC)
  - Attribute-based (ABAC)

- **Administrative** policies: define who can specify access control policies
  - Usually coupled with DAC, RBAC and ABAC
In summary

Access control systems should answer questions like:

1. Can Alice read file “/users/Bob/readme.txt”?
2. Can Bob open a SSH connection with “myserver.com”?
   ▶ If yes, access is granted,
   ▶ If not, access is denied.

Looks like a simple enough mechanism to implement?
Key challenges for an access control system

- **Expressiveness**: Does the access control model allow to completely express high level access requirements in terms of access control policies?

- **Efficiency**: Access requests need to be dealt with quickly.

- **Full Mediation**: How do you know you have not forgotten some checks?

- **Safety**: How do you know your access control policy captures your access requirements?
Discretionary Access Control

Outline

Access Control

Discretionary Access Control

Safety Problem

DAC weaknesses
Discretionary Access Control (DAC)

▶ **Intuitions:**
  ▶ The owner of a resource decides who can access it
  ▶ Access rights can be delegated to other users

▶ **Intended Environment:**
  ▶ Operating systems in the late 60s
  ▶ Users are members of the same community: objective is to protect data from mistakes of others (cd /; rm -fr *)
  ▶ Still used in many corporate environments
The basis for DAC is that an individual user (or program on its behalf) is allowed to specify explicitly the types of access other users (or programs on their behalf) may have to information under the user’s control.

NCSC (National Computer Security Center)
Discretionary Access Control (DAC)

- **Entities:**
  - **Subjects**: who have privileges and can do operations on objects
  - **Objects**: files, resources, programs
  - **Access Rights**: what a subject can do on an object

- **Main Features**
  - **Ownership**: Users have full control over the objects they create
    - When users create objects, they own them
  - **Delegation**: Users can give certain rights to other users
    - Users can grant rights they have, to others
    - Users that have control can remove rights
DAC Models

- Graham-Denning (1972)
- Lampson (1974)
- Harrison-Ruzzo-Ullman (1976)
- Griffiths-Wade (1976)
- Take-grant protection model (1977)
- Originator control (1989)
Lampson: Access Matrix

- Set of **subjects** $S$

- Set of **objects** $O$
  - Subjects can be considered as objects, i.e. $S \subseteq O$

- **Access Matrix** $A (S \times O)$
  - Entries contain sets of rights
    - **access rights**: read, write, call, etc.
    - **administration rights**: own, control
    - **delegation rights**: flags “*” and “+”
Sample Access Matrix

<table>
<thead>
<tr>
<th></th>
<th>Subject 1</th>
<th>Subject 2</th>
<th>Subject 3</th>
<th>File 1</th>
<th>File 2</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject 1</td>
<td>own</td>
<td>own</td>
<td>*call</td>
<td>own</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>control</td>
<td>control</td>
<td></td>
<td>*read</td>
<td>*write</td>
<td></td>
</tr>
<tr>
<td>Subject 2</td>
<td></td>
<td>call</td>
<td></td>
<td>write</td>
<td></td>
<td>wakeup</td>
</tr>
<tr>
<td>Subject 3</td>
<td></td>
<td></td>
<td>own</td>
<td>read</td>
<td></td>
<td>own</td>
</tr>
</tbody>
</table>

- “own” can *add* any rights
- “control” is the right to *remove* rights from a subject (in Lampson’s work; in other models ownership implies control)
- “*” flag can *delegate* rights to other subjects
<table>
<thead>
<tr>
<th></th>
<th>Subject 1</th>
<th>Subject 2</th>
<th>Subject 3</th>
<th>File 1</th>
<th>File 2</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject 1</td>
<td>own control</td>
<td>own control</td>
<td>*call</td>
<td>own</td>
<td>*read</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*write</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject 2</td>
<td></td>
<td>call</td>
<td></td>
<td>write</td>
<td>wakeup</td>
<td></td>
</tr>
<tr>
<td>Subject 3</td>
<td></td>
<td>own control</td>
<td>read</td>
<td>own</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What they are allowed to do?
## Answer

A table summarizing discretionary access control:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Subject 1</th>
<th>Subject 2</th>
<th>Subject 3</th>
<th>File 1</th>
<th>File 2</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject 1</td>
<td>own control</td>
<td>own control</td>
<td>*call</td>
<td>own</td>
<td>*read</td>
<td>*write</td>
</tr>
<tr>
<td>Subject 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>write</td>
<td></td>
</tr>
<tr>
<td>Subject 3</td>
<td></td>
<td></td>
<td>own control</td>
<td>read</td>
<td></td>
<td>own</td>
</tr>
</tbody>
</table>

- **control**: S1 can remove any right of S2
- ***read**: S1 can give any subject the right to read F1
- **own**: S3 can give any right on F2 to every subject
Access Matrix: Implementation

Matrix is generally large and sparse
- Storing the entire matrix is waste of memory space

Alternative approaches
- **Authorization table**: store table of non-null triples \((s, o, a)\)
  - used in DBMS
- **Access control lists (ACLs)**: Stored by column
- **Capability lists**: Stored by row
### Authorization Tables

<table>
<thead>
<tr>
<th>Subject</th>
<th>Access mode</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject 1</td>
<td>own</td>
<td>Subject 1</td>
</tr>
<tr>
<td>Subject 1</td>
<td>control</td>
<td>Subject 1</td>
</tr>
<tr>
<td>Subject 1</td>
<td>own</td>
<td>Subject 2</td>
</tr>
<tr>
<td>Subject 1</td>
<td>control</td>
<td>Subject 2</td>
</tr>
<tr>
<td>Subject 1</td>
<td>call</td>
<td>Subject 3</td>
</tr>
<tr>
<td>Subject 1</td>
<td>own</td>
<td>File 1</td>
</tr>
<tr>
<td>Subject 1</td>
<td>read</td>
<td>File 1</td>
</tr>
<tr>
<td>Subject 1</td>
<td>write</td>
<td>File 1</td>
</tr>
<tr>
<td>Subject 2</td>
<td>call</td>
<td>Subject 3</td>
</tr>
<tr>
<td>Subject 2</td>
<td>read</td>
<td>File 1</td>
</tr>
<tr>
<td>Subject 2</td>
<td>write</td>
<td>File 3</td>
</tr>
<tr>
<td>Subject 2</td>
<td>wakeup</td>
<td>Process 1</td>
</tr>
</tbody>
</table>
Access control lists vs. Capability lists
Access control lists vs. Capability lists

Access control lists
- Objects are the starting point (per-object basis)
- Require authentication of subjects
- Superior for access control and revocation on per-object basis

Capability lists
- Subject are the starting point (per-subject basis)
- Require control of propagation of capabilities
- Superior for access control and revocation on per-subject basis

The per-object basis usually more convenient
Most systems based on ACLs
Harrison-Ruzzo-Ullman (HRU) Model

Define authorization system

- **State** \((S, O, A)\)
  - \(S\) set of subjects
  - \(O\) set of objects
    - Subject can be considered as objects (i.e., \(S \subseteq O\))
  - \(A\) access matrix \((S \times O)\)
    - rows correspond to subjects
    - columns correspond to objects
    - \(A[s, o]\) indicates the privilege of \(s\) on \(o\)

- **State transitions** described by commands
  - commands defined as sequences of primitive operations
  - **enter** \(r\) into \(A[s, o]\), **delete** \(r\) from \(A[s, o]\), **create subject** \(s'\), **destroy subject** \(s'\), **create object** \(o'\), **destroy object** \(o'\)
### Primitive operations (1)

**Current state:** \((S, O, A)\)

<table>
<thead>
<tr>
<th>OPERATION ((op))</th>
<th>CONDITIONS</th>
<th>NEW STATE ((Q' = (S', O', A')))</th>
</tr>
</thead>
</table>
| **create subject** \(s'\) | \(s' \notin O\) | \(S' = S \cup \{s'\}\)  
\(O' = O \cup \{s'\}\)  
\(A'[s, o] = A[s, o]\) \(\forall s \in S, o \in O\)  
\(A'[s', o] = \emptyset\) \(\forall o \in O'\)  
\(A'[s, s'] = \emptyset\) \(\forall s \in S'\) |
| **create object** \(o'\) | \(o' \notin O\) | \(S' = S\)  
\(O' = O \cup \{o'\}\)  
\(A'[s, o] = A[s, o]\) \(\forall s \in S, o \in O\)  
\(A'[s, o'] = \emptyset\) \(\forall s \in S'\) |
| **enter** \(r\) into \(A[s, o]\) | \(s \in S\), \(o \in O\) | \(S' = S\)  
\(O' = O\)  
\(A'[s, o] = A[s, o] \cup \{r\}\)  
\(A'[s, o] = A[s, o]\) \(\forall (s_i, o_i) \neq (s, o)\) |
## Primitive operations (2)

### Current state: \((S, O, A)\)

<table>
<thead>
<tr>
<th>OPERATION ((op))</th>
<th>CONDITIONS</th>
<th>NEW STATE ((Q' = (S', O', A')))</th>
</tr>
</thead>
</table>
| **delete** \(r\) from \(A[s, o]\) | \(s \in S\)  
\(o \in O\) | \(S' = S\)  
\(O' = O\)  
\(A'[s, o] = A[s, o] \setminus \{r\}\)  
\(A'[s_i, o_j] = A[s_i, o_j] \quad \forall (s_i, o_i) \neq (s, o)\) |
| **destroy subject** \(s'\) | \(s' \in S\) | \(S' = S \setminus \{s'\}\)  
\(O' = O \setminus \{s'\}\)  
\(A'[s, o] = A[s, o] \quad \forall s \in S', o \in O'\) |
| **destroy object** \(o'\) | \(o' \in O\)  
\(o' \notin S\) | \(S' = S\)  
\(O' = O \setminus \{o'\}\)  
\(A'[s, o] = A[s, o] \quad \forall s \in S', o \in O'\) |
Commands

Changes to the system state modeled by commands of the form

\[
\text{command } c(x_1, \ldots, x_k) \\
\quad \text{if } r_1 \text{ in } A[x_{s_1}, x_{o_1}] \text{ and} \\
\quad r_2 \text{ in } A[x_{s_2}, x_{o_2}] \text{ and} \\
\quad \ldots \\
\quad r_m \text{ in } A[x_{s_m}, x_{o_m}] \\
\quad \text{then } op_1 \\
\quad \quad op_2 \\
\quad \quad \ldots \\
\quad \quad op_n \\
\quad \text{end}
\]

with \( r_1, \ldots, r_m \) rights and \( op_1, \ldots, op_n \) primitive operations
**Commands – Examples**

**command** \textit{CREATE}(s, o)

create object o

enter own into A[s, o] \textbf{end}.

**command** \textit{CONFER}_{\text{read}}(s_1, s_2, o)

if own in A[s_1, o]

\textit{then enter read into} A[s_2, o] \textbf{end}.

**command** \textit{REVOKE}_{\text{read}}(s_1, s_2, o)

if own in A[s_1, o]

\textit{then delete read into} A[s_2, o] \textbf{end}.
Transfer of privileges

Delegation of authority by attaching flags to privileges (e.g., * copy flag, + transfer-only flag)

- **copy flag (*)**: subject can transfer privilege to others

  command \(\text{TRANSFER}_{\text{read}}(s_1, s_2, o)\)
  
  if *read in \(A[s_1, o]\)
  
  then enter read into \(A[s_2, o]\) end.

- **transfer-only flag (+)**: subject can transfer privilege to others (and the flag on it), but he loses the privilege

  command \(\text{TRANSFER-ONLY}_{\text{read}}(s_1, s_2, o)\)
  
  if +read in \(A[s_1, o]\)
  
  then delete +read into \(A[s_1, o]\)
  
  enter +read into \(A[s_2, o]\) end.
Exercise

Write a command which allows a process $p$ to create a new process $q$ where parent and child processes can signal (read/write) each other.
**Solution**

`command spawn_process(p, q)
create subject q
enter own into A[p, q]
enter r into A[p, q]
enter w into A[p, q]
enter r into A[q, p]
enter w into A[q, p]`

`end`
A state \( Q = (S, O, A) \) yields a state \( Q' = (S', O', A') \) under

\[ \text{command } c(x_1, \ldots, x_k) \]
\[ \text{if } r_1 \text{ in } A[x_{s_1}, x_{o_1}] \text{ and } \ldots \text{ and } r_m \text{ in } A[x_{s_m}, x_{o_m}] \]
\[ \text{then } \text{op}_1, \ldots, \text{op}_n \]
\[ \text{end} \]

with arguments \( a_1, \ldots, a_k \), denoted \( Q \Rightarrow c(a_1, \ldots, a_k) \) \( Q' \), provided

- \( Q' = Q \) if one of the conditions of \( c \) is not satisfied
- \( Q' = Q_n \) otherwise, where there exist states \( Q_0, Q_1, \ldots, Q_n \) such that \( Q = Q_0 \) and \( Q_n = Q' \) and for each \( i \), with \( 0 \leq i \leq n \),

\[ Q_i \Rightarrow \text{op}_{i+1}[a_j/x_j] \ Q_{i+1} \]

where \( \text{op}_{i+1}[a_j/x_j] \) denotes the primitive operation \( \text{op}_{i+1} \), substituting \( a_1, \ldots, a_k \) for variables \( x_1, \ldots, x_k \).
Exercise

Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(\text{Alice}, \text{File3})$
2. $\text{CONFER}_{+\text{read}}(\text{Alice}, \text{Bob}, \text{File3})$
3. $\text{CREATE}(\text{Charlie}, \text{File3})$
4. $\text{CONFER}_{+\text{read}}(\text{Charlie}, \text{David}, \text{File3})$
5. $\text{TRANSFER-ONLY}_{\text{read}}(\text{Bob}, \text{David}, \text{File3})$
6. $\text{TRANSFER}_{\text{read}}(\text{Charlie}, \text{Alice}, \text{File2})$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Solution

Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(Alice, \text{File}3)$
2. $\text{CONFER}_{+\text{read}}(Alice, Bob, \text{File}3)$
3. $\text{CREATE}(Charlie, \text{File}3)$
4. $\text{CONFER}_{+\text{read}}(Charlie, David, \text{File}3)$
5. $\text{TRANSFER-ONLY}_{\text{read}}(Bob, David, \text{File}3)$
6. $\text{TRANSFER}_{\text{read}}(Charlie, Alice, \text{File}2)$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Solution

Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(Alice, \text{File3})$
2. $\text{CONFER}_{+\text{read}}(Alice, Bob, \text{File3})$
3. $\text{CREATE}(Charlie, \text{File3})$
4. $\text{CONFER}_{+\text{read}}(Charlie, David, \text{File3})$
5. $\text{TRANSFER-ONLY}_{\text{read}}(Bob, David, \text{File3})$
6. $\text{TRANSFER}_{\text{read}}(Charlie, Alice, \text{File2})$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td>own</td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(Alice, \text{File3})$
2. $\text{CONF}\text{ER}_{\text{+read}}(Alice, Bob, \text{File3})$
3. $\text{CREATE}(Charlie, \text{File3})$
4. $\text{CONF}\text{ER}_{\text{+read}}(Charlie, David, \text{File3})$
5. $\text{TRANSF}\text{ER}-\text{ONLY}_{\text{read}}(Bob, David, \text{File3})$
6. $\text{TRANSF}\text{ER}_{\text{read}}(Charlie, Alice, \text{File2})$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
<td>+read</td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(Alice, \text{File3})$
2. $\text{CONFER}_{+\text{read}}(Alice, Bob, \text{File3})$
3. $\text{CREATE}(Charlie, \text{File3})$
4. $\text{CONFER}_{+\text{read}}(Charlie, David, \text{File3})$
5. $\text{TRANSFER-ONLY}_{\text{read}}(Bob, David, \text{File3})$
6. $\text{TRANSFER}_{\text{read}}(Charlie, Alice, \text{File2})$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
<td>+read</td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Solution

Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(\text{Alice}, \text{File3})$
2. $\text{CONFER}_{+\text{read}}(\text{Alice}, \text{Bob}, \text{File3})$
3. $\text{CREATE}(\text{Charlie}, \text{File3})$
4. $\text{CONFER}_{+\text{read}}(\text{Charlie}, \text{David}, \text{File3})$
5. $\text{TRANSFER-ONLY}_{\text{read}}(\text{Bob}, \text{David}, \text{File3})$
6. $\text{TRANSFER}_{\text{read}}(\text{Charlie}, \text{Alice}, \text{File2})$

\begin{tabular}{|c|c|c|}
\hline
 & File 1 & File 2 & File 3 \\
\hline
Alice &  & own &  \\
Bob & own &  & +read \\
Charlie & own &  & \\
David &  &  & \\
\hline
\end{tabular}
Solution

Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(Alice, File3)$
2. $\text{CONFER}_{+\text{read}}(Alice, Bob, File3)$
3. $\text{CREATE}(Charlie, File3)$
4. $\text{CONFER}_{+\text{read}}(Charlie, David, File3)$
5. $\text{TRANSFER-ONLY}_{\text{read}}(Bob, David, File3)$
6. $\text{TRANSFER}_{\text{read}}(Charlie, Alice, File2)$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
<td>+read</td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td>+read</td>
</tr>
</tbody>
</table>
Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(\text{Alice}, \text{File3})$
2. $\text{CONFER}_{+\text{read}}(\text{Alice}, \text{Bob}, \text{File3})$
3. $\text{CREATE}(\text{Charlie}, \text{File3})$
4. $\text{CONFER}_{+\text{read}}(\text{Charlie}, \text{David}, \text{File3})$
5. $\text{TRANSFER-ONLY}_{\text{read}}(\text{Bob}, \text{David}, \text{File3})$
6. $\text{TRANSFER}_{\text{read}}(\text{Charlie}, \text{Alice}, \text{File2})$

<table>
<thead>
<tr>
<th>User</th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
<td>+read</td>
</tr>
<tr>
<td>Charlie</td>
<td></td>
<td>own</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td>+read</td>
</tr>
</tbody>
</table>

Note: own does not assume all rights.
Solution

Compute the access matrix that results from the following initial state by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CREATE}(\text{Alice}, \text{File3})$
2. $\text{CONFER}_{+\text{read}}(\text{Alice}, \text{Bob}, \text{File3})$
3. $\text{CREATE}(\text{Charlie}, \text{File3})$
4. $\text{CONFER}_{+\text{read}}(\text{Charlie}, \text{David}, \text{File3})$
5. $\text{TRANSFER-ONLY}_{\text{read}}(\text{Bob}, \text{David}, \text{File3})$
6. $\text{TRANSFER}_{\text{read}}(\text{Charlie}, \text{Alice}, \text{File2})$

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
<td>+read</td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td>+read</td>
</tr>
</tbody>
</table>

Note: own does not assume all rights.
Outline

Access Control

Discretionary Access Control

Safety Problem

DAC weaknesses
Fundamental Questions

- How can we determine whether a system is secure?
  - Need to define what we mean by a system being “secure”

- Is there a generic algorithm that allows us to determine whether a computer system is secure?
Safety Property: nothing bad happens
  - the program will never produce a wrong result ("partial correctness")

Liveness Property: something good eventually happens
  - the program will produce a result ("termination")
Example: Safety and Liveness

C1: Whenever process P1 wants to enter the critical session, provided process P2 never stays in the critical session forever, P1 gets to enter eventually.

C2: It cannot happen that both processes are in their critical sessions simultaneously.
**Example: Safety and Liveness**

C1: Whenever process P1 wants to enter the critical session, provided process P2 never stays in the critical session forever, P1 gets to enter eventually.

**Liveness**

C2: It cannot happen that both processes are in their critical sessions simultaneously.

**Safety**
When is a system secure?

▶ A simple definition
A system is secure if it does not allow violations of security policies

▶ Alternative definition based on distribution of rights
No leakage of rights
When is a system secure?

- A simple definition
  - A system is secure if it does not allow violations of security policies

- Alternative definition based on distribution of rights
  - No leakage of rights
What is a secure system?

**Definition**

A state leaks a right $r$ if there is a command $c$ that enters $r$ into a position of the access matrix that previously did not contain $r$.

Intuitively, if there is $c$ such that $(S, O, A) \Rightarrow c (S', O', A')$ where $r \not\in A[s, o]$ and $r \in A'[s, o]$ for some $s$ and $o$

**Definition**

A state is secure with respect to a right $r$ if no sequence of commands can transform the access matrix into a state that leaks $r$. 
Exercise

Assume a system with the following two commands:

```
command grant_execute (s_1, s_2, o)
    if own in A[s_1, o]
    then enter exec into A[s_2, o]
end

command modify_own_right (s, o)
    if exec in A[s, o]
    then enter write into A[s, o]
end
```

Policy: Suppose Bob has developed an application program; he wants this program to be run by other users but not modified by them. Is the system secure? Why?
The system is NOT secure with respect to the given policy

Consider the following sequence of commands:

1. Bob: grant\_execute \((Bob, Tom, p_1)\)
2. Tom: modify\_own\_right \((Tom, p_1)\)

\(A[Tom, p_1]\) contains the write access right
HRU: Safety Problem

**Safety problem:** Given an initial state $(S, O, A)$ and a right $r$, is there any sequence of commands leaking $r$?
HRU and Safety: “Desired” leaks

Leaks are not necessarily bad

▶ A system that allows sharing will of course have many leaks
▶ Subjects can intentionally transfer (leak) their rights to other trustworthy subjects

Leaks of rights to trustworthy subjects should be ignored when assessing the security of the system (i.e., ignoring “desired” leaks)
Exercise

Given initial state $Q = (S, O, A)$ with \( S = \{s_1, s_2, s_3, s_4, s_5\} \),
\( O = \{s_1, s_2, s_3, s_4, s_5\} \) and \( A = \emptyset \), and the sequence of commands $\alpha$

\[
\begin{align*}
&\text{CREATE}(s_3, o) \\
&\text{CONFER}_{read}(s_3, s_1, o) \\
&\text{CONFER}_{*read}(s_3, s_4, o) \\
&\text{TRANSFER}_{read}(s_2, s_5, o) \\
&\text{TRANSFER}_{read}(s_1, s_5, o) \\
&\text{REVOKE}_{read}(s_1, s_4, o) \\
&\text{TRANSFER}_{read}(s_4, s_5, o) \\
&\text{REVOKE}_{read}(s_3, s_5, o)
\end{align*}
\]

Determine the state $Q'$ after the execution of $\alpha$.

Does $\alpha$ leak access privileges? (Consider only $s_5$ to be untrusted)
Justify the answer.
Safety Problem

Solution

$CREATE(s_3, o)$
$CONFER_{read}(s_3, s_1, o)$
$CONFER_{*read}(s_3, s_4, o)$
$TRANSFER_{read}(s_2, s_5, o)$
$TRANSFER_{read}(s_1, s_5, o)$
$REVOKE_{read}(s_1, s_4, o)$
$TRANSFER_{read}(s_4, s_5, o)$
$REVOKE_{read}(s_3, s_5, o)$

<table>
<thead>
<tr>
<th></th>
<th>$S_1$</th>
<th>$S_2$</th>
<th>$S_3$</th>
<th>$S_4$</th>
<th>$S_5$</th>
<th>$o$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S_3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>$S_4$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S_5$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Safety Problem

Solution

CREATE\((s_3, o)\)
CONFER\_\text{read}(s_3, s_1, o)
CONFER\_\text{*read}(s_3, s_4, o)
TRANSFER\_\text{read}(s_2, s_5, o)
TRANSFER\_\text{read}(s_1, s_5, o)
REVOKE\_\text{read}(s_1, s_4, o)
TRANSFER\_\text{read}(s_4, s_5, o)
REVOKE\_\text{read}(s_3, s_5, o)

\[
\begin{array}{c|cccccc}
 & S_1 & S_2 & S_3 & S_4 & S_5 & O \\
\hline
S_1 &  &  &  &  &  & \text{read} \\
S_2 &  &  &  &  &  &  \\
S_3 &  &  &  &  &  & \text{own} \\
S_4 &  &  &  &  &  &  \\
S_5 &  &  &  &  &  &  \\
\end{array}
\]
Safety Problem

Solution

CREATE\( (s_3, o) \)
CONFER_{\text{read}}(s_3, s_1, o)
CONFER_{\ast, \text{read}}(s_3, s_4, o)
TRANSFER_{\text{read}}(s_2, s_5, o)
TRANSFER_{\text{read}}(s_1, s_5, o)
REVOKE_{\text{read}}(s_1, s_4, o)
TRANSFER_{\text{read}}(s_4, s_5, o)
REVOKE_{\text{read}}(s_3, s_5, o)

<table>
<thead>
<tr>
<th></th>
<th>S_1</th>
<th>S_2</th>
<th>S_3</th>
<th>S_4</th>
<th>S_5</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>S_2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S_3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>S_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
</tr>
<tr>
<td>S_5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Does \( \alpha \) leak access privileges? (Consider only \( S\_5 \) to be untrusted)

Yes, \( \alpha \) leaks access privileges. At a certain point, \( S\_5 \) had read privilege.
Solution

CREATE\((s_3, o)\)
CONFER_{\text{read}}(s_3, s_1, o)
CONFER_{\ast \text{read}}(s_3, s_4, o)
TRANSFER_{\text{read}}(s_2, s_5, o)
TRANSFER_{\text{read}}(s_1, s_5, o)
REVOKE_{\text{read}}(s_1, s_4, o)
TRANSFER_{\text{read}}(s_4, s_5, o)
REVOKE_{\text{read}}(s_3, s_5, o)

<table>
<thead>
<tr>
<th></th>
<th>\text{S}_1</th>
<th>\text{S}_2</th>
<th>\text{S}_3</th>
<th>\text{S}_4</th>
<th>\text{S}_5</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>S_2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S_3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>S_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
</tr>
<tr>
<td>S_5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Safety Problem

Solution

\[
\begin{align*}
\text{CREATE}(s_3, o) \\
\text{CONFERENCE}_{read}(s_3, s_1, o) \\
\text{CONFERENCE}_{*\text{read}}(s_3, s_4, o) \\
\text{TRANSFER}_{read}(s_2, s_5, o) \\
\text{TRANSFER}_{read}(s_1, s_5, o) \\
\text{REVOKE}_{read}(s_1, s_4, o) \\
\text{TRANSFER}_{read}(s_4, s_5, o) \\
\text{REVOKE}_{read}(s_3, s_5, o)
\end{align*}
\]

<table>
<thead>
<tr>
<th></th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
<th>S5</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>S2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>S4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
</tr>
<tr>
<td>S5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Solution

\[ CREATE(s_3, o) \]
\[ CONFER_{read}(s_3, s_1, o) \]
\[ CONFER_{*read}(s_3, s_4, o) \]
\[ TRANSFER_{read}(s_2, s_5, o) \]
\[ TRANSFER_{read}(s_1, s_5, o) \]
\[ REVOKE_{read}(s_1, s_4, o) \]
\[ TRANSFER_{read}(s_4, s_5, o) \]
\[ REVOKE_{read}(s_3, s_5, o) \]

<table>
<thead>
<tr>
<th></th>
<th>( s_1 )</th>
<th>( s_2 )</th>
<th>( s_3 )</th>
<th>( s_4 )</th>
<th>( s_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>( s_2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( s_3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>( s_4 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
</tr>
<tr>
<td>( s_5 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Does \( \alpha \) leak access privileges? (Consider only \( s_5 \) to be untrusted)

Yes, \( \alpha \) leaks access privileges. At a certain point, \( s_5 \) had read privilege.
### Solution

CREATE\((s_3, o)\)
CONFER_{read}(s_3, s_1, o)
CONFER_{*read}(s_3, s_4, o)
TRANSFER_{read}(s_2, s_5, o)
TRANSFER_{read}(s_1, s_5, o)
REVOKE_{read}(s_1, s_4, o)
TRANSFER_{read}(s_4, s_5, o)
REVOKE_{read}(s_3, s_5, o)

<table>
<thead>
<tr>
<th></th>
<th>S_1</th>
<th>S_2</th>
<th>S_3</th>
<th>S_4</th>
<th>S_5</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>read</strong></td>
</tr>
<tr>
<td>S_2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S_3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>own</strong></td>
</tr>
<tr>
<td>S_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*<strong>read</strong></td>
</tr>
<tr>
<td>S_5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>read</strong></td>
</tr>
</tbody>
</table>
Solution

CREATE\((s_3, o)\)

\(\text{CONFER}_{\text{read}}(s_3, s_1, o)\)

\(\text{CONFER}_{\ast \text{read}}(s_3, s_4, o)\)

\(\text{TRANSFER}_{\text{read}}(s_2, s_5, o)\)

\(\text{TRANSFER}_{\text{read}}(s_1, s_5, o)\)

\(\text{REVOKE}_{\text{read}}(s_1, s_4, o)\)

\(\text{TRANSFER}_{\text{read}}(s_4, s_5, o)\)

\(\text{REVOKE}_{\text{read}}(s_3, s_5, o)\)

\begin{center}
\begin{tabular}{|c|c|c|c|c|c|}
\hline
 & \(S_1\) & \(S_2\) & \(S_3\) & \(S_4\) & \(S_5\) & \\
\hline
\(S_1\) & & & & & \(\text{read}\) & \\
\hline
\(S_2\) & & & & & \(\text{own}\) & \\
\hline
\(S_3\) & & & & & \(\ast \text{read}\) & \\
\hline
\(S_4\) & & & & & & \\
\hline
\(S_5\) & & & & & & \\
\hline
\end{tabular}
\end{center}

Does \(\alpha\) leak access privileges? (Consider only \(s_5\) to be untrusted)

Yes, \(\alpha\) leaks access privileges. At a certain point, \(s_5\) had read privilege.
Solution

\[
\begin{align*}
&CREATE(s_3, o) \\
&CONFER_{\text{read}}(s_3, s_1, o) \\
&CONFER_{\ast\text{read}}(s_3, s_4, o) \\
&TRANSFER_{\text{read}}(s_2, s_5, o) \\
&TRANSFER_{\text{read}}(s_1, s_5, o) \\
&REVOKE_{\text{read}}(s_1, s_4, o) \\
&TRANSFER_{\text{read}}(s_4, s_5, o) \\
&REVOKE_{\text{read}}(s_3, s_5, o)
\end{align*}
\]

Does $\alpha$ leak access privileges? (Consider only $s_5$ to be untrusted)

<table>
<thead>
<tr>
<th></th>
<th>$s_1$</th>
<th>$s_2$</th>
<th>$s_3$</th>
<th>$s_4$</th>
<th>$s_5$</th>
<th>$o$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>$s_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$s_3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>$s_4$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
</tr>
<tr>
<td>$s_5$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Safety Problem

Solution

\[ CREATE(s_3, o) \]
\[ CONFER_{read}(s_3, s_1, o) \]
\[ CONFER_{*read}(s_3, s_4, o) \]
\[ TRANSFER_{read}(s_2, s_5, o) \]
\[ TRANSFER_{read}(s_1, s_5, o) \]
\[ REVOKE_{read}(s_1, s_4, o) \]
\[ TRANSFER_{read}(s_4, s_5, o) \]
\[ REVOKE_{read}(s_3, s_5, o) \]

<table>
<thead>
<tr>
<th></th>
<th>$S_1$</th>
<th>$S_2$</th>
<th>$S_3$</th>
<th>$S_4$</th>
<th>$S_5$</th>
<th>$O$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>$S_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$S_3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>own</td>
</tr>
<tr>
<td>$S_4$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
</tr>
<tr>
<td>$S_5$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>read</td>
</tr>
</tbody>
</table>

Does $\alpha$ leak access privileges? (Consider only $s_5$ to be untrusted)

Yes, $\alpha$ leaks access privileges. At a certain point, $s_5$ had read privilege.
Safety problem: Decidability

Safety problem: Given an initial state \((S, O, A)\) and a right \(r\), is there any sequence of commands leaking \(r\)?

Or does transfer of \(r\) violate security policies of the system?

Is there a generic algorithm that allows us to determine whether a computer system is secure?
Safety problem: Some bad news

**Theorem**

Verifying the security of an access matrix $A$ with respect to a right $r$ is undecidable.

The safety problem can be reduced to the halting problem of a Turing machine.
Safety problem: Good news?

A **mono-operational system** is a system in which every command consists of a single operation.

**Theorem**

Verifying the security of an access matrix $A$ with respect to a right $r$ is **decidable in a mono-operational system**.

**Bad news**

- Mono-operational systems are not useful
- If you create an object you cannot own it $\implies$ you cannot modify it

**Remark**: Decidability can also be proved for systems with a finite number of subjects and objects, or for systems where it is not possible to create new subjects and objects.
The more expressive the security model is, the more difficult it is to verify security.

- Is it better to have a very expressive policy language or a simple language where it is easier to check the impact of policy decision?
- In an expressive language, it is easier to capture the intended policy but more difficult to verify that the policy actually does what is supposed to do.
- In a simple language, it may not be possible to capture access requirements precisely, but there are effective ways to check what the policy does.
Outline

Access Control

Discretionary Access Control

Safety Problem

DAC weaknesses
DAC weaknesses

- DAC imposes constraints only on direct access
- No control on the information once released
  \[\Rightarrow\] DAC is vulnerable to Trojan horses
    - exploiting access privileges of calling subject

**Trojan horses**: a program (apparently harmless) which contains malicious or harmful code
Trojan horses – Example

contacts

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>06-12345678</td>
</tr>
<tr>
<td>Bob</td>
<td>06-23456781</td>
</tr>
</tbody>
</table>

(Alice, owner, contacts)
(Bob, read, contacts)
Trojan horses – Example

Bob invokes Application

contacts

Alice 06-12345678
Bob 06-23456781

(Alice,owner,contacts)
(Bob,read,contacts)
DAC weaknesses

Trojan horses – Example

Bob invokes Application

contacts

Alice  06-12345678
Bob  06-23456781

(Alice, owner, contacts)
(Bob, read, contacts)

stolen

(Bob, write, stolen)
(Charlie, read, stolen)
Trojan horses – Example

- Bob invokes Application
- Application contains code
- Malicious code steals contacts
- Contacts: Alice 06-12345678, Bob 06-23456781
- Stolen: (Bob, write, stolen) (Charlie, read, stolen)
DAC weaknesses

Trojan horses – Example

Bob invokes Application

read contacts
write stolen

code

malicious
code

contacts

Alice 06-12345678
Bob 06-23456781

(Alice, owner, contacts)
(Bob, read, contacts)

stolen

(Bob, write, stolen)
(Charlie, read, stolen)
Trojan horses – Example

- Bob invokes Application
  - read contacts
  - write stolen
  - contacts
  - stolen

  Alice  06-12345678
  Bob    06-23456781

  (Alice, owner, contacts)
  (Bob, read, contacts)

  Alice  06-12345678
  Bob    06-23456781

  (Bob, write, stolen)
  (Charlie, read, stolen)
Summary

- **Access control**: regulates the operations that can be executed on data and resources to be protected
- **DAC**: users can regulate the access to their resources
  - Lampson
  - HRU model
- **Safety Problem**: Given a configuration $Q$ and a right $r$, is there any sequence of commands that leaks $r$?
- **DAC vulnerabilities**: Trojan horses


Homework

1. Compute the access matrix that results from the following initial state

<table>
<thead>
<tr>
<th>File 1</th>
<th>File 2</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td>own</td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td>*read</td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

by executing the sequence of commands $\alpha$ defined as follows:

1. $\text{CONFER}^*_\text{read}(\text{Charlie}, \text{Alice}, \text{File}1)$
2. $\text{CONFER}_{\text{exec}}(\text{Bob}, \text{Alice}, \text{Process}1)$
3. $\text{CONFER}_{\text{write}}(\text{Charlie}, \text{Alice}, \text{File}1)$
4. $\text{CONFER}_{\text{read}}(\text{Bob}, \text{Bob}, \text{File}2)$
5. $\text{CONFER}_{\text{exec}}(\text{Bob}, \text{Charlie}, \text{Process}1)$
6. $\text{TRANSFER}_{\text{exec}}(\text{Alice}, \text{Charlie}, \text{Process}1)$
7. $\text{CONFER}^*_\text{write}(\text{Charlie}, \text{Bob}, \text{File}1)$
8. $\text{REVOKE}_{\text{read}}(\text{Bob}, \text{Charlie}, \text{File}2)$
9. $\text{REVOKE}_{\text{read}}(\text{Alice}, \text{Alice}, \text{File}1)$
10. $\text{TRANSFER}_{\text{read}}(\text{Alice}, \text{David}, \text{File}1)$
11. $\text{REVOKE}_{\text{read}}(\text{Charlie}, \text{David}, \text{File}1)$
12. $\text{CREATE}(\text{Charlie}, \text{File}3)$
13. $\text{CONFER}^*_\text{read}(\text{Charlie}, \text{Bob}, \text{File}3)$
14. $\text{TRANSFER}_{\text{read}}(\text{Bob}, \text{Alice}, \text{File}3)$
15. $\text{TRANSFER}_{\text{read}}(\text{Charlie}, \text{Bob}, \text{File}2)$
16. $\text{REVOKE}_{\text{read}}(\text{Charlie}, \text{Bob}, \text{File}3)$
17. $\text{TRANSFER}_{\text{read}}(\text{Charlie}, \text{David}, \text{File}2)$
18. $\text{REVOKE}_{\text{read}}(\text{Bob}, \text{David}, \text{File}2)$
19. $\text{CONFER}^*_\text{read}(\text{Bob}, \text{Charlie}, \text{File}2)$
20. $\text{TRANSFER}_{\text{write}}(\text{Charlie}, \text{Alice}, \text{File}1)$

Hints:

- Command $\text{CONFER}^*_\text{read}$ is equal to $\text{CONFER}_{\text{read}}$ but grants $^*\text{read}$ instead of $\text{read}$. Similar principle applies to $\text{CONFER}^*_\text{exec}$ and $\text{CONFER}^*_\text{write}$.
- Command $\text{REVOKE}_{\text{read}}$ removes both $\text{read}$ and $^*\text{read}$. Similar principle applies to $\text{REVOKE}_{\text{exec}}$ and $\text{REVOKE}_{\text{write}}$.

2. Is $\alpha$ leaking access privileges? (Consider only David to be untrusted) Justify the answer.