DAC and MAC

Prof. Ravi Sandhu
Executive Director and Endowed Chair

January 22, 2016

ravi.sandhu@utsa.edu
www.profsandhu.com
Access Control Models

- Discretionary Access Control (DAC)
  - Owner controls access but only to the original, not to copies
- Mandatory Access Control (MAC)
  - Same as Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels propagate to copies
- Role-Based Access Control (RBAC)
  - Access based on roles
  - Can be configured to do DAC or MAC

Numerous other models but only 3 successes

- What’s next?
  - Attribute-Based Access Control (ABAC)
  - Relationship-Based Access Control (ReBAC)
  - Usage Control (UCON)
PEI Models

Idealized
Enforceable
(Assume Approximate)
Codeable
Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

Attribute Based Access Control (ABAC), ????

© Ravi Sandhu
World-Leading Research with Real-World Impact!
**Access Control**

- **Fixed policy**
  - Discretionary Access Control (DAC), 1970
  - Role Based Access Control (RBAC), 1995
  - Attribute Based Access Control (ABAC), ???

- **Flexible policy**
  - Mandatory Access Control (MAC), 1970
Access Control

Enterprise Oriented

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ????

Mandatory Access Control (MAC), 1970

Beyond Enterprise

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ??

Administration Driven

Automated Adaptive

© Ravi Sandhu

World-Leading Research with Real-World Impact!
**DAC: ACCESS MATRIX MODEL**

<table>
<thead>
<tr>
<th></th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>r w own</td>
<td>r</td>
</tr>
<tr>
<td>V</td>
<td>r w own</td>
<td>rights</td>
</tr>
</tbody>
</table>

The diagram illustrates the DAC (Discretionary Access Control) model with subjects and objects (and subjects) represented as U and V. The matrix shows the rights (r) allowed between different combinations of subjects and objects.
each column of the access matrix is stored with the object corresponding to that column
E model

U: F/r, F/w, F/own, G/r

V: G/r, G/w, G/own

each row of the access matrix is stored with the subject corresponding to that row
### ACCESS CONTROL TRIPLES

<table>
<thead>
<tr>
<th>Subject</th>
<th>Access</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>r</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>w</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>own</td>
<td>F</td>
</tr>
<tr>
<td>U</td>
<td>r</td>
<td>G</td>
</tr>
<tr>
<td>V</td>
<td>r</td>
<td>G</td>
</tr>
<tr>
<td>V</td>
<td>w</td>
<td>G</td>
</tr>
<tr>
<td>V</td>
<td>own</td>
<td>G</td>
</tr>
</tbody>
</table>

**commonly used in relational database management systems**
DAC: TROJAN HORSE VULNERABILITY

ACL

File F
A:r
A:w

File G
B:r
A:w

B cannot read file F
DAC: TROJAN HORSE VULNERABILITY

A executes

Program Goodies

Trojan Horse

read

File F

write

File G

ACL

A:r
A:w

B:r
A:w

B can read contents of file F copied to file G
DAC CHALLENGES

- Owner unrestricted DAC versus restricted DAC
- Safety in restricted DAC
  - Undecidable
  - NP-Hard, PSpace-Hard
- Transfer of ownership
- Multiple ownership
- Cascading grants and revokes
- Negative authorizations and conflict resolution
  - Worse with groups and hierarchies
- DAC policy limits
  - You can give only what you have
  - How about user administration?
- Practical DAC deployments
  - Ownership consolidated in a single administrator
  - Can lead to inadvertent cascading revokes
LBAC: LATTICE STRUCTURES

P model

dominance \geq \text{can-flow}

Top Secret
Secret
Confidential
Unclassified

World-Leading Research with Real-World Impact!
LBAC: LATTICE STRUCTURES

Hierarchical Classes with Compartments

© Ravi Sandhu
World-Leading Research with Real-World Impact!
SIMPLE-SECURITY

Subject S can read object O only if

- label(S) dominates label(O)

STAR-PROPERTY (LIBERAL)

Subject S can write object O only if

- label(O) dominates label(S)

STAR-PROPERTY (STRICT)

Subject S can write object O only if

- label(O) equals label(S)
EQUIVALENCE OF BLP AND BIBA

P model

HI (High Integrity) \[\Rightarrow\] LI (Low Integrity)

LI (Low Integrity) \[\Rightarrow\] HI (High Integrity)

BIBA LATTICE

EQUIVALENT BLP LATTICE

Information flow downwards

Information flow upwards

World-Leading Research with Real-World Impact!
EQUIVALENCE OF BLP AND BIBA

P model

HS (High Secrecy) \(\Rightarrow\) LS (Low Secrecy)

BLP LATTICE
Information flow downwards

EQUIVALENT BIBA LATTICE
Information flow upwards

© Ravi Sandhu

World-Leading Research with Real-World Impact!
COMBINATION OF DISTINCT LATTICES

P model

<table>
<thead>
<tr>
<th>HS</th>
<th>LI</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS</td>
<td>HI</td>
</tr>
</tbody>
</table>

BLP  BIBA

⇒  

HS, HI  LS, HI

⇒  

HS, LI  LS, LI

Information flow upwards

Information flow upwards

GIVEN

EQUIVALENT BLP LATTICE

© Ravi Sandhu

World-Leading Research with Real-World Impact!

20
LBAC: LATTICE STRUCTURES

High User

Information is leaked unknown to the high user

High Trojan Horse Infected Subject

COVERT CHANNEL

Low Trojan Horse Infected Subject

Low User

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Discuss figures from LBAC93 paper