PANEL
Solving the Access Control Puzzle:
Finding the Pieces and Putting Them Together

Ravi Sandhu
Executive Director
Endowed Professor
June 2010

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu

Questions

1. A research direction or area within the access control space that you think merits more attention;

2. Another research direction or area within this space that you feel has been sufficiently mined and can be set aside, or for which you think that isolated research has reached a point of diminishing returns;

3. Two or more research directions that you think should be studied jointly or have good potential for synergy.

Questions

1. A research direction or area within the access control space that you think merits more attention;

Automation

2. Another research direction or area within this space that you feel has been sufficiently mined and can be set aside, or for which you think that isolated research has reached a point of diminishing returns;

3. Two or more research directions that you think should be studied jointly or have good potential for synergy.

Questions

1. A research direction or area within the access control space that you think merits more attention;

Automation

2. Another research direction or area within this space that you feel has been sufficiently mined and can be set aside, or for which you think that isolated research has reached a point of diminishing returns;

SELinux

3. Two or more research directions that you think should be studied jointly or have good potential for synergy.

Questions

1. A research direction or area within the access control space that you think merits more attention;

Automation

2. Another research direction or area within this space that you feel has been sufficiently mined and can be set aside, or for which you think that isolated research has reached a point of diminishing returns;

SELinux

3. Two or more research directions that you think should be studied jointly or have good potential for synergy.

Access Control meets Mission Assurance

or

Mission-Aware Access Control

Automation

- Computers excel at automation.
  That's why they were invented.
- Users have zero interest in configuring access control.
- Value of fine-grained access control and least privilege are oversold.
- Why can't access control systems:
  - Time out privileges automatically
  - Automatically renew
  - Limit usage rates to human versus machine
  - Provide meaningful review
  - Meaningfully combine core ideas of LBAC (MAC), DAC, RBAC, UCON (including ABAC)
  - Be usable by application developers let alone end users

SELinux

- Simply mashing LBAC (MAC), DAC, RBAC, DTE produces a mess versus a thing of beauty
- Principles reinforced by failure of SELinux to achieve them:
  - Simple things should be simple to do
  - Overly complex things should never be done
  - Multi-user OS's are passe. We are in the age of multi-device and multi-OS users!
  - Start with a coherent model before rushing into implementation. Think P (Policy), E (Enforcement), I (Implementation)
  - Forget about DTE

Mission-Aware Access Control

- How to put intelligence into access control
  - across P (Policy), E (Enforcement), I (Implementation)
  - so mission needs can be taken into account in adapting access control
  - automatically with minimal human intervention