Security and Trust Convergence: Attributes, Relations and Provenance

Prof. Ravi Sandhu

Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security
University of Texas at San Antonio

Colorado State University
Fort Collins
Sept. 15, 2014

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

State of Cyber Security

State of Cyber Security

- About as good or as bad as it is going to get
- Not too bad
- Big crime is a real threat but criminals can only defraud so many
- Big government/big business are real threats

State of Cyber Security

- Cyber should be “controllable”
  Nuclear, chemical, biological have been “controlled”
- New arena for researchers
- Highly asymmetric, includes offense, clandestine
- Dual conflicting goals: strong offense, strong defense
- Need game-changing technologies

A New Threat Grows Amid Shades of 9/11
The nation remains largely unaware of the potential for disaster from cyberattacks.
By TOM KEAN and LEE HAMILTON
WALL STREET JOURNAL, 9/11/2014

State of Cyber Security

- Escalating reputational and even existential threat against mass theft of consumer information
- Even the most iconic high tech companies are breachable
- Cost of clean-up after a mass theft far exceeds aggregate actual loss of money
- There are many scarier scenarios than mass data breach of consumer data
- Some of this scarier stuff has happened

State of Cyber Security

Who has the Initiative?

Who has the Initiative?

Federal R&D priorities 2011:

- Tailored Trustworthy Spaces
- Moving Target
- Designed-In Security
- Cyber Economic Incentives
- Science of Security

Who has the Initiative?

DoD R&D priorities 2011:
- Assuring Effective Missions
- Agile Operations
- Resilient Infrastructure
- Trust

Federal R&D priorities 2011:
- Tailored Trustworthy Spaces
- Moving Target
- Designed-In Security
- Cyber Economic Incentives
- Science of Security

Who has the Initiative?

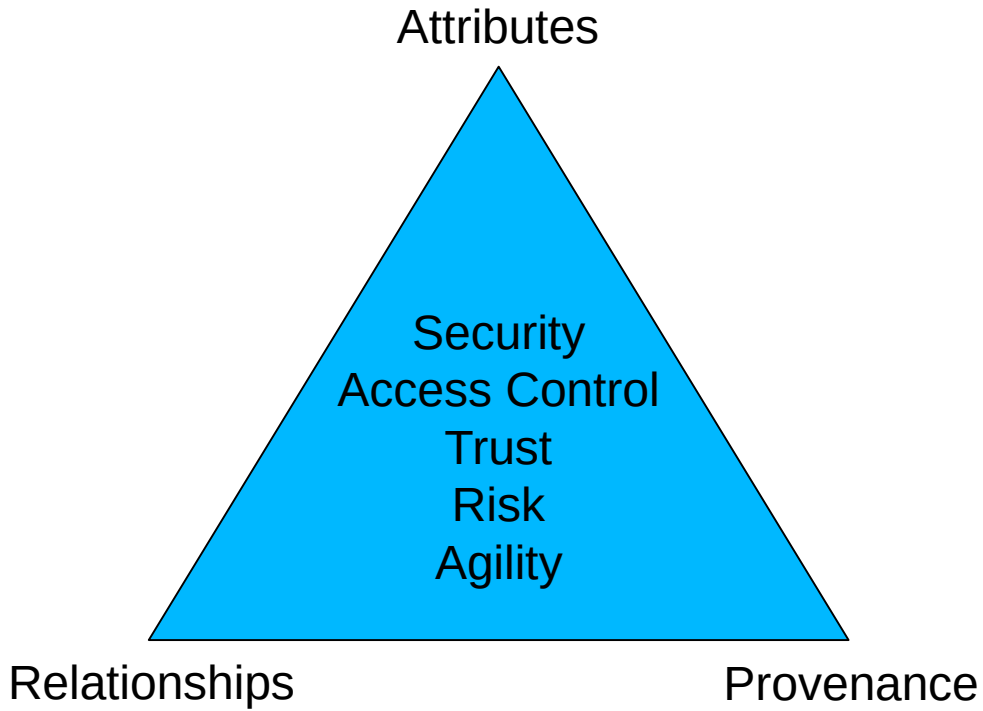
DoD R&D priorities 2011:

- Assuring Effective Missions
- **Agile Operations**
- Resilient Infrastructure
- **Trust**

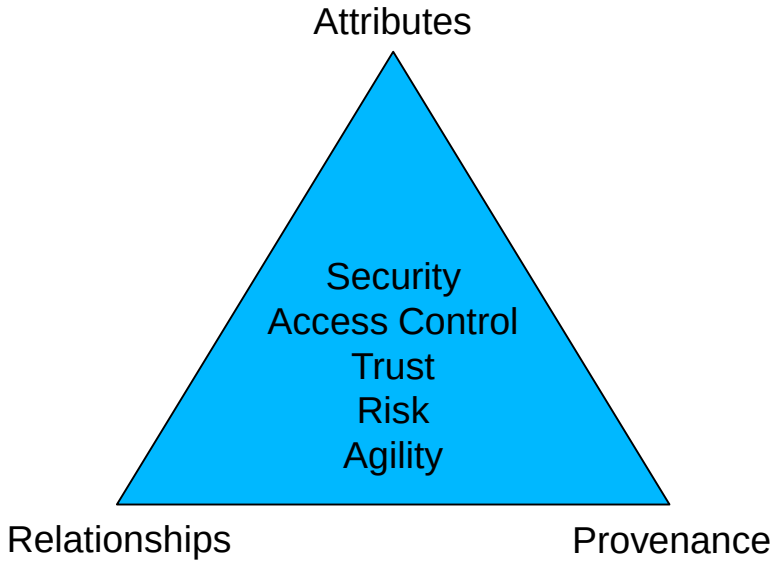
Federal R&D priorities 2011:

- **Tailored Trustworthy Spaces**
- Moving Target
- Designed-In Security
- Cyber Economic Incentives
- Science of Security

Security and Trust

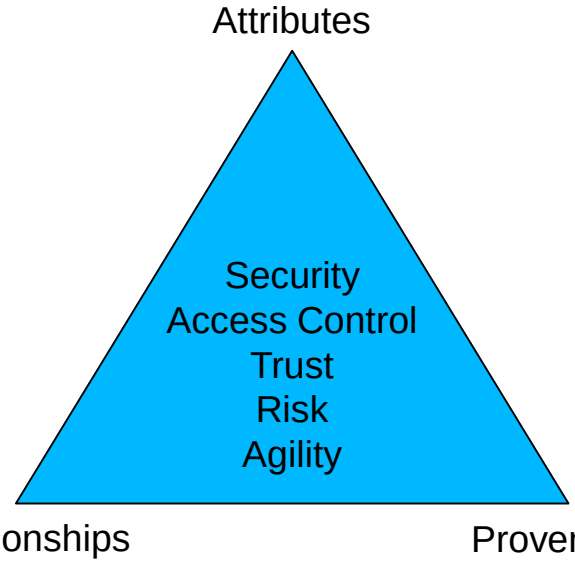


Security and Trust



Least Privilege
Privilege Abstraction
Separation of Duty
Constrained Administration

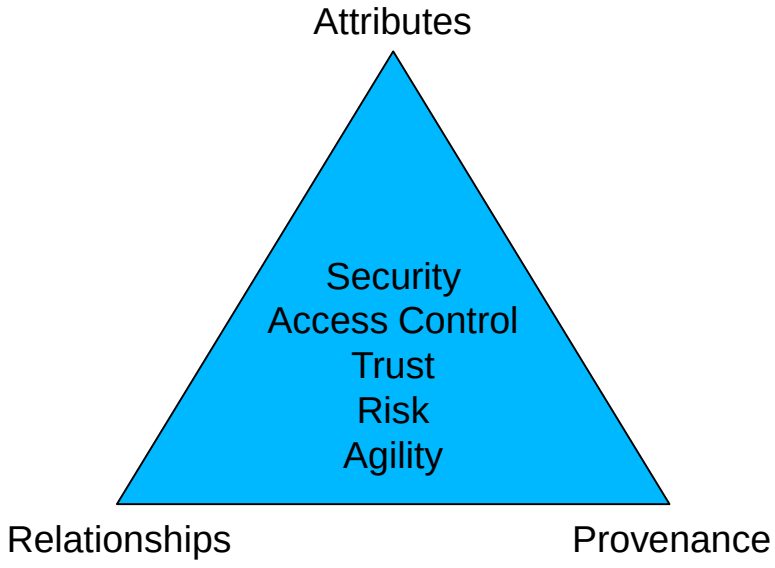
Security and Trust



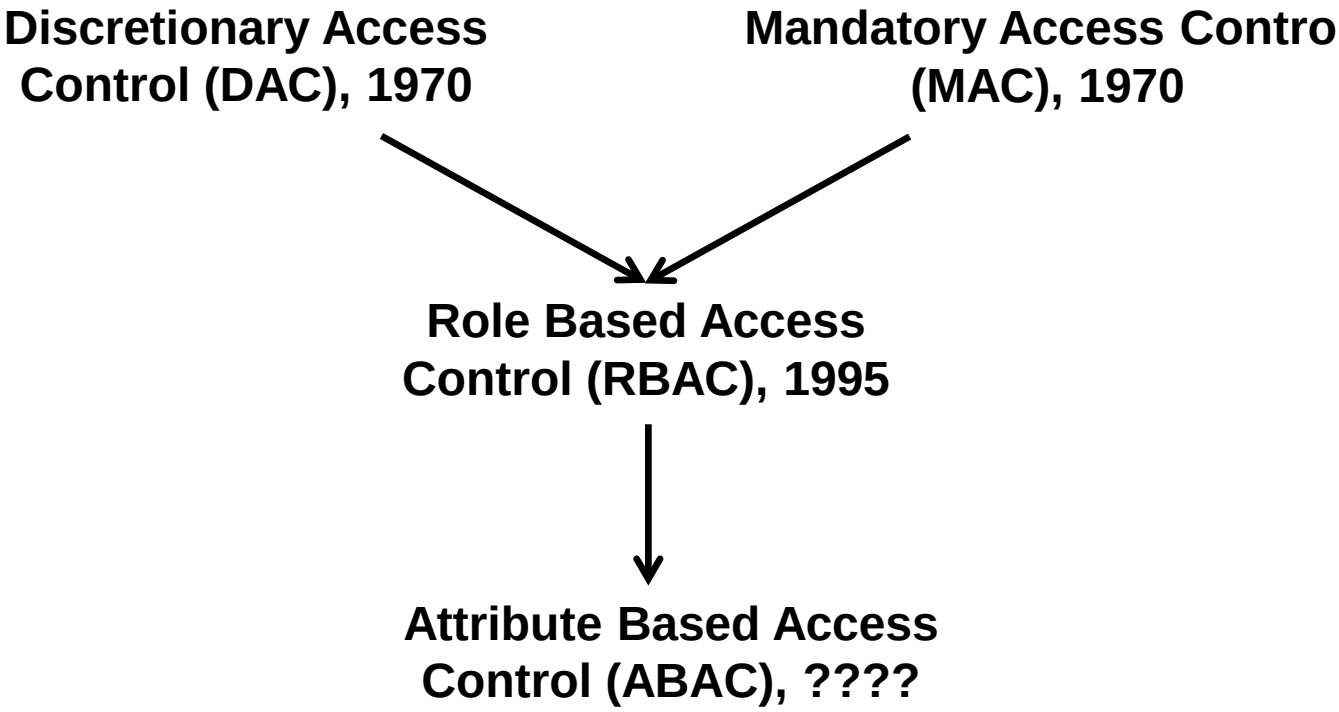
Least Privilege
Privilege Abstraction
Separation of Duty
Constrained Administration

Automation
Adaptation

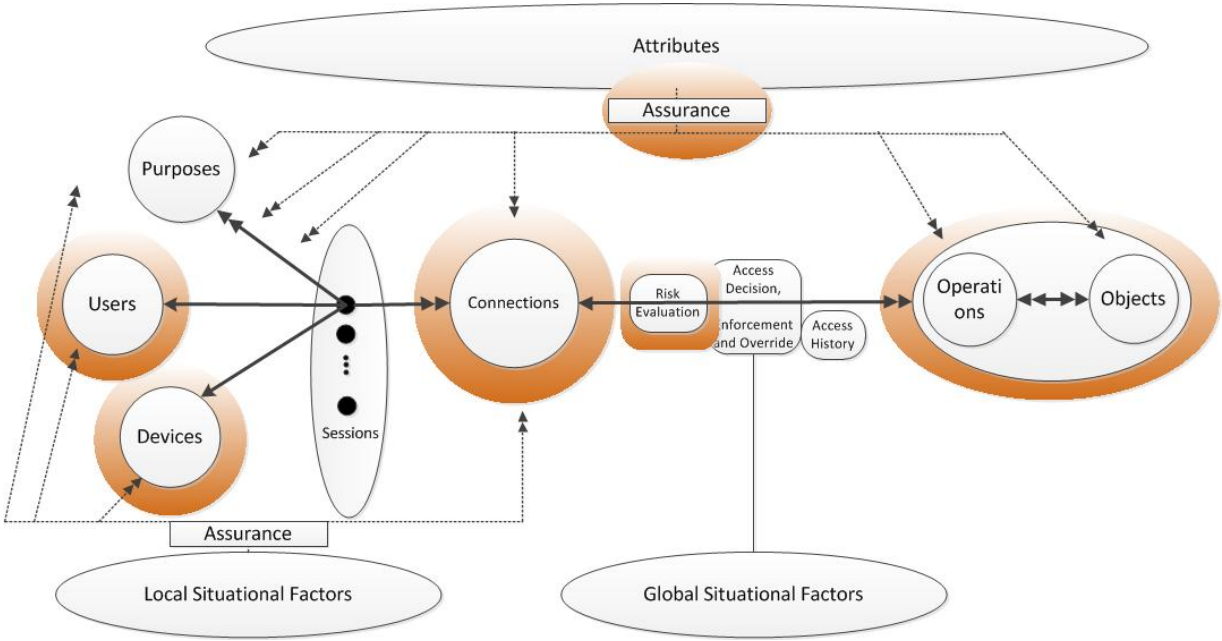
Security and Trust



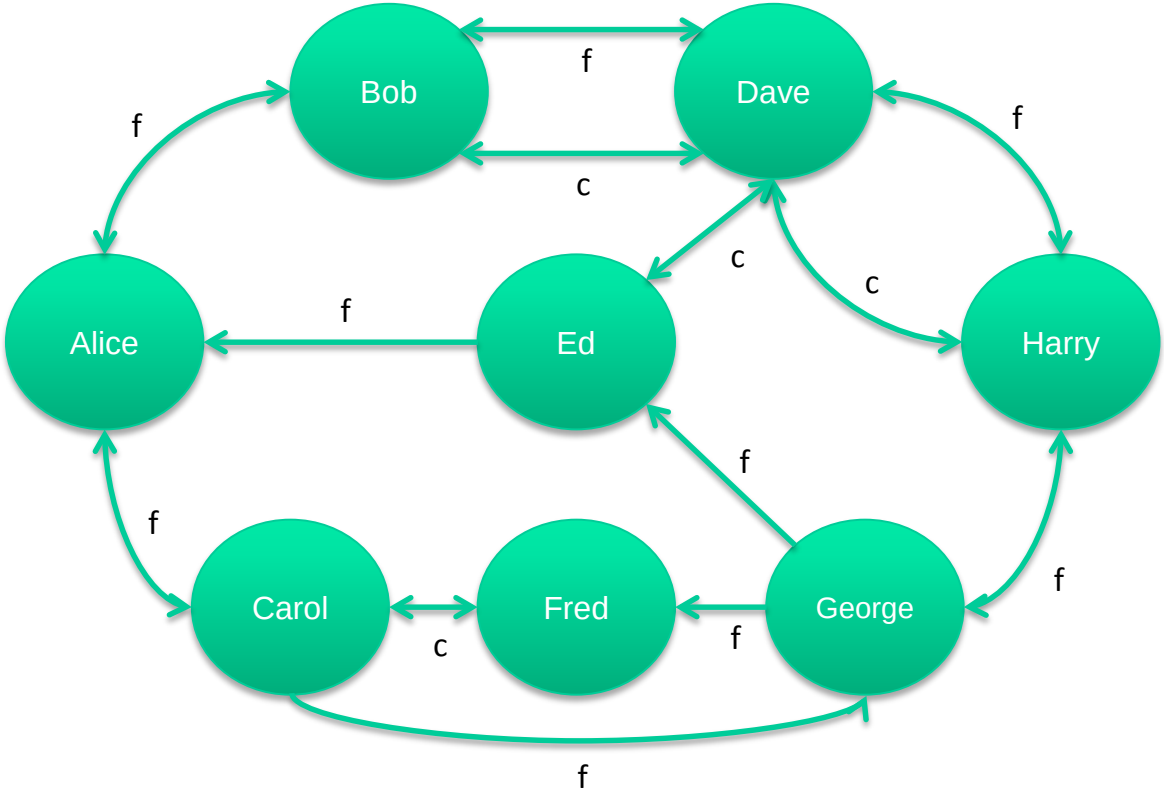
Automation
Adaptation


Discretionary Access Control (DAC), 1970
Mandatory Access Control (MAC), 1970
Role Based Access Control (RBAC), 1995
Attribute Based Access Control (ABAC), ????

Attributes



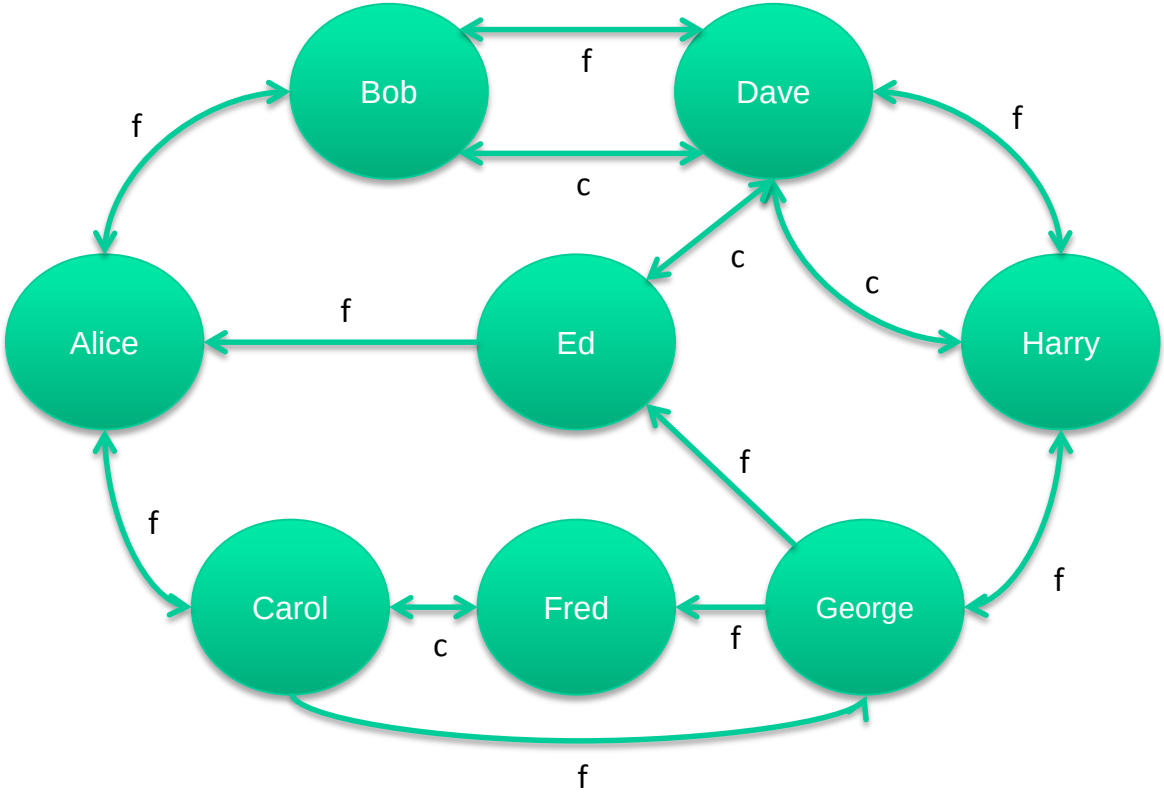
Relationships



Provenance

- Anyone can upload a homework.
- A user can replace a homework if she uploaded it and the homework is not submitted yet.
- A user can submit a homework if she uploaded it and the homework is not submitted already.
- A user can review a homework if she is not the author of the homework, the user did not previously review the homework, and the homework is submitted already but not graded yet.
- A user can grade a homework if the homework is reviewed but not graded yet.

Relationships, Attributes and Provenance



Final Thoughts