Trust Evidence in Heterogeneous Environments: Towards a Research Agenda

Ravi Sandhu
Executive Director and Endowed Professor
May 2010

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

Application and Technology Context

- Basic premise
  - **There is no security without application context**
  - **There is no application context without some technology context**
- Opposite premise
  - Orange Book and Rainbow Series Era (1983-1994)
    - Application context makes high-assurance impossible
      - Good-enough security is good enough
      - Mission-assurance not information-assurance
    - Towards the end of this era applications had to be addressed: Trusted Database Interpretation (TDI)

Application and Technology Context

- Basic premise
  - ~~There is no security without application context~~ **trust**
  - **There is no application context without some technology context**
- Opposite premise
  - Orange Book and Rainbow Series Era (1983-1994)
    - Application context makes high-assurance impossible
      - Good-enough security is good enough
      - Mission-assurance not information-assurance
    - Towards the end of this era applications had to be addressed: Trusted Database Interpretation (TDI)

Application Context

Software Architect	Project	% Time	Label
Alice	Win7	25%	U
Alice	SecureWin7	75%	S
Bob	Vista	100%	U

- What precisely is Secret?
  - There exists a SecureWin7 project
  - Alice works on SecureWin7
  - Alice's effort on SecureWin7 is 75%
  - All or some of the above
- How do we maintain integrity of the database
  - Depends

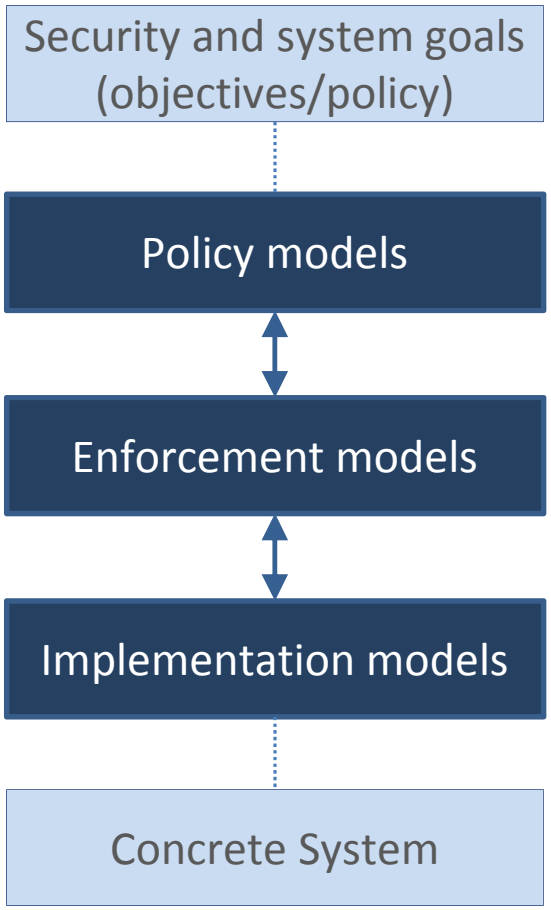
· **Data and security model are intertwined**
· **Much work and $$$ by researchers and vendors, late 80's-early 90's**

Application Centric Security

- Modern applications
  - Multi-party
  - Different objectives and responsibilities, often in conflict
- Ongoing projects at ICS
  - Secure information sharing
  - Social networking
  - Critical infrastructure assurance
  - SaaS in the Cloud/Intercloud
  - Smart grid
- New ACM Conference on Data and Application Security and Privacy (CODASPY)
  - Feb 21-23, 2011, San Antonio, Texas
  - www.codaspy.org, www.sigsac.org
  - Papers due: Sept 15th 2010

The future is application centric

PEI Models



What?

How?

How?

Necessarily informal

Specified using users, subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.

Security analysis (objectives, properties, etc.).

Approximated policy realized using system architecture with trusted servers, protocols, etc.

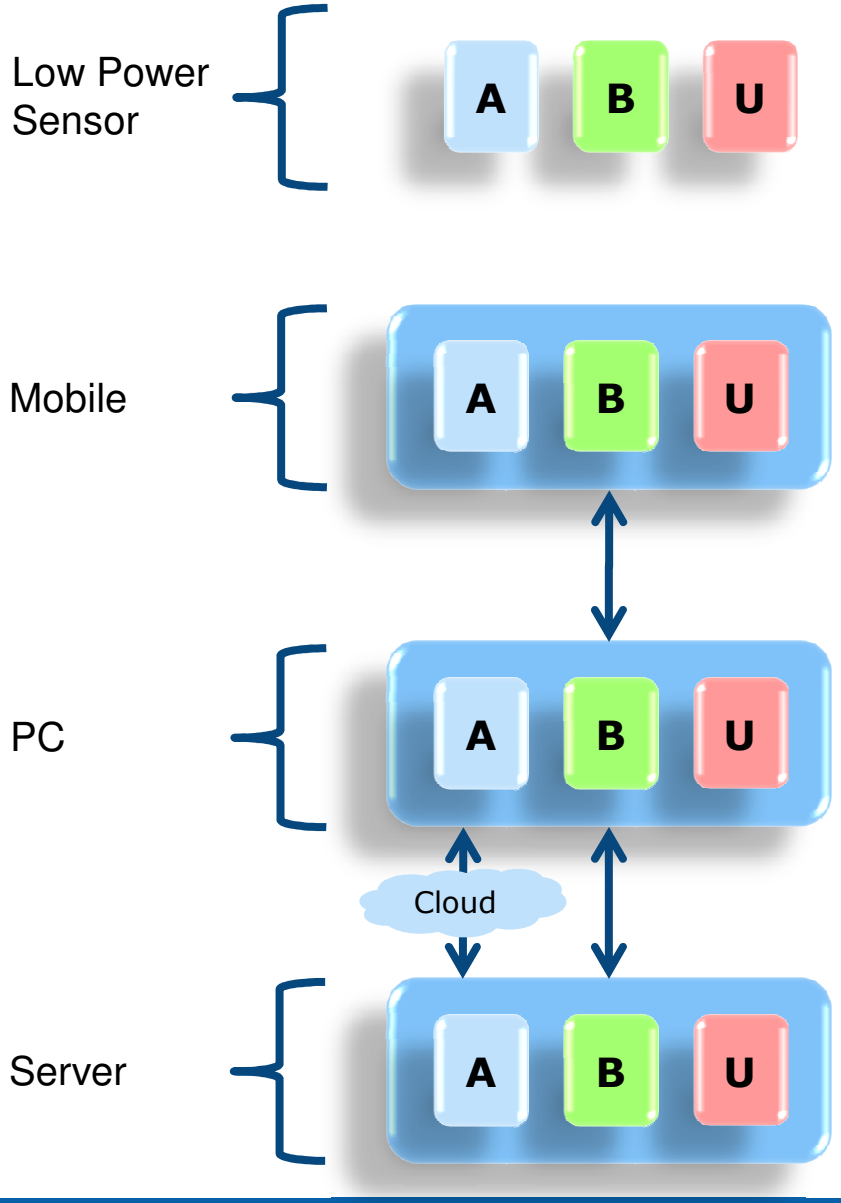
Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).

Technologies such as Cloud Computing, Trusted Computing, etc.

Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)

Software and Hardware

Sample Scenario



Applications

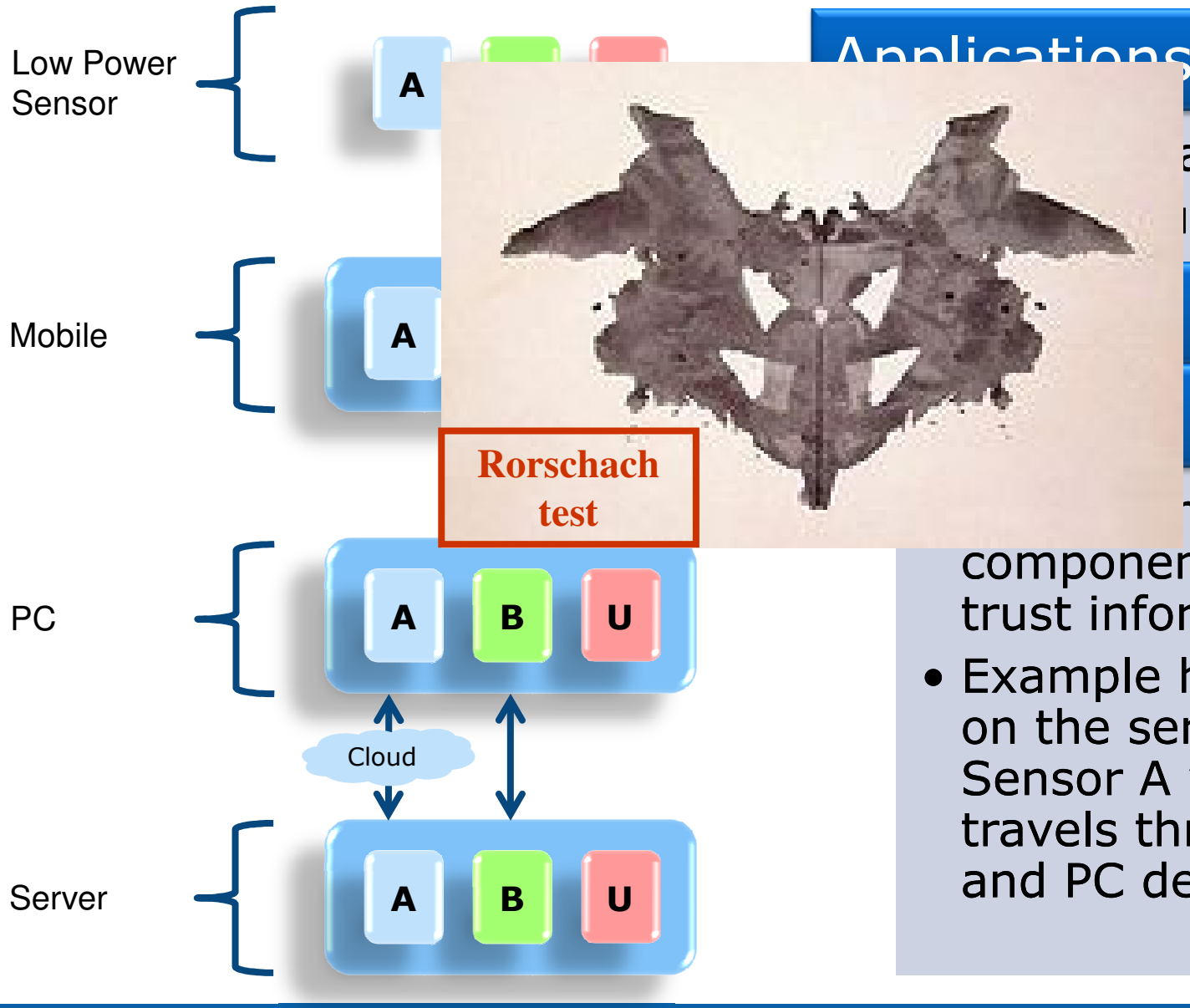
- 2 known apps (A&B)
- Multiple unknown apps (U)

Properties

Question

- How do the various components gain and pass trust information
- Example how does App A on the server gain trust in Sensor A when the data travels through the mobile and PC devices

Sample Scenario



Applications

apps (A&B)

nknown apps (U)

e various components gain and pass trust information

- Example how does App A on the server gain trust in Sensor A when the data travels through the mobile and PC devices

System Principles

- KISS vs TooMMP
  - Keep is Simple Stupid
  - Too Many Moving Parts
- Keep the user out of the loop
  - Smart grid: max 2 hours/year for end user in the loop
  - Alternately: don't move the misery around
- Future proof
  - Adjustable trust/assurance with minimal pain

Enforcement Principles

- Protect the root key
  - and thereby non-root keys
- Protect “what” can use a key
  - and thereby “who” can use the key
- Enforce usage limits
  - and thereby contain damage
- Run-time monitoring
  - Protection will be broken

- Decoys? Lies? Attack back? …
- Defense ecosystem? Reporting and patching? …

Sample Scenario: Explanation

- Applications A and B reside on various devices connected by diverse networks (as well as other apps we do not know about). This is a multi-domain setting. A & B will share information up and down the stack. We want to make sure that we can trust all the layers and that this information is properly handled and properly shared. The systems are dynamic, and the threats are also dynamic. Each device and domain have own sets of policies. Devices join and leave domains.

Multi-Tier Approach

- Applications
- Devices
- Domains
- Networks
- Stack
- Dynamic

- How do we organize this into tiers/layers?
- How does trust/assurance compose across tiers?
- What does trust/assurance means at different tiers?
- What does information sharing within/across applications mean, and how do we achieve it?

Some Research Challenges

- How does higher trust/assurance at lower layers effectively support higher assurance at the upper (application) layer?
- Is it possible to achieve higher trust/assurance at the upper layers than the lower layer baseline?
- What application scenarios are appropriate for evaluation of solution approaches?
- What can we learn from approaches that have been successful in the real world? Credit cards, Automatic Teller Machines, On-Line Banking?
- How do we develop a discipline of mission assurance as opposed to information assurance?
- ……..