Tailored Trustworthy Spaces: The Right Security for the Job

What is a Tailored Trustworthy Space?

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor's office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Today's cyberspace recreates those environments, but security mechanisms and policies lack the flexibility to accommodate different behaviors

The vision is of a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

New Paradigm

- Users can select different environments for different activities (e.g., online banking, commerce, healthcare, personal communications) providing operating capabilities across many dimensions, including confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to create new environments with mutually agreed upon characteristics and lifetimes

Enabling Informed Trust Decisions

- Provide users with:
  - Context-specific trust services
  - Coherent policy implementation: an integrated set of security choices (or defaults) appropriate to the tasks at hand
  - User/provider/system visible rules and attributes
  - Means to negotiate boundaries and rules of the space

Key Concept

- TTS is about knowing how trustworthy your system is and understanding whether is it good enough for what you are trying to do.
- TTS is not about guaranteeing high trust

Challenge: Identifying dimensions of a tailored trustworthy space

- What is needed to safely support the activity we want to conduct?
  - Degree of identification / authentication
  - Information flow rules
  - Strength of separation mechanisms
  - Degree of monitoring / violation detection

Challenge: Policy Specification and Management

- How to we propose, decide upon, and instantiate our rules in the system?
  - Convenient specification of a tailored space
  - Convenient mechanisms to know it
  - Convenient mechanisms to change it

Challenge: Assuring Correct Operation

- How do we know our tailored solution is doing the job?
  - Validation of platform integrity
  - Challenge: Violation detection
  - Challenge: Verifiable separation of spaces
  - . . . and many more

What's New?

Nothing. Few of these individual problems or component technologies are novel

Everything. A structure that puts the pieces together to provide integrated, usable support for diverse trust environments would change the game.

Which technology areas matter?

- Identity management
- Component assurance
- Composition methods and logics
- Trust negotiation and management
- ...

What is the state of the art?

- Wide variance in the maturity of required technology
- Human dimension – how do we understand and establish trust levels – is least explored and most critical to success