UTORauth

Matthew Wilks
Russell Sutherland
University of Toronto
Computing and Networking Services

The Need for Centralization

- A member of UofT is likely to have a record in multiple databases around campus: ROSI, AMS, the Library, etc.
- Communication between these databases is hard because foreknowlege is necessary
- UTORauth created to address the need for intercommunication between systems on campus
- The UTID unites personal information such as surname, firstname, birthdate and SIN from the various systems

Definitions

- Identification
  - Who are you?
  - “I am Sam”
- Authentication
  - Proves you are who you say you are
  - --> “I am Sam”
  - <-- What is the full name of Dr. Seuss?
  - --> “Theodor Seuss Geisel”
- Authorization
  - What you can do:
  - “Sam is allowed to read the digital copy of Green Eggs and Ham”

The Identification System

- Ensures a common unique identifier for each UofT community member
- Collects basic identity data from authoritative sources
- Issues a unique UTID (**U**of**T ID**entifier)
- The UTID is unknown to the person, used only by computer systems
- Used by UTORauth as a basis to generate other identifiers:
  - UTORid
  - Barcode

The Authentication System

- Implementation is based on Kerberos
- Key Distribution Centers (KDC) will be available to all clients
- WWW browser based authentication will use PubCookie
- Kerberos credentials are based on:
  - a principal login ID
  - a corresponding passphrase
- The UTORid will be used as the principal login ID

The UTORid

- The chief UofT network identifier for access current and future network resources
- A UTORid is assigned to each incoming student
- Efforts are underway to make sure every new staff/faculty member receive this identifier
- Centralized authentication provides:
  - fluid interoperability between services
  - simplifies end-user experience by requiring only one identifier campus-wide

Authorization System: UTORable

- Provides a central directory of information for UofT staff/faculty/students
- Accessible to registered clients
- Level of access granted on the basis of the client services requirements
- Clients will:
  - Offer services to their end users
  - Set their own rules and policies
- Data available on a batch or interactive basis
  - Interactive -> LDAP
  - Batch -> FTP/SSH
- No end user can access UTORable directly

Some Examples

- The PAFs (**P**ublic **A**ccess **F**acilities)
- CCNet
- Locknetics Project

The PAFs – Interactive UTORable

- This project is used to control access to the various PAF workstations around campus
  - Who may access?
  - For how long?
- To collect accounting data for each session

PAF Chronological Info Trail

- UTORid/passphrase entered to workstation login screen
- Workstation authenticates via Kerberos
  - if this fails, the client will be denied access
- Workstation passes UTORid to PAF accounting server
- Accounting server queries UTORauth for the status of the UTORid
  - is_student -> access
  - is_faculty -> access
  - is_staff -> access
- Accounting server records user session data

CCNet – Batch process

- http://courses.ece.utoronto.ca/cgi-bin/display.cgi
- CCNet is an effort originating in the Engineering Department to ease the creation of course webpages
- CCNet receives a full listing of student's course registration information each morning from UTORauth
- This information can be used by professors to create student accounts for accessing grades, etc.

Locknetics – Selective Data

- Run by Phil Poulos to restrict access in the Bahen Centre
- Locknetics receives a batch every day containing all students registered in an Engineering or Computer Science course
- Students are required to swipe their TCard at the door
  - access granted -> if the student is in the list
  - access denied -> if the student isn't in the list