User Authentication and Authorization Summary

Champion: Colin Field

June 23, 2015

Overview of the Use Case

- **User Authentication** (e.g. username and password) is becoming increasingly difficult to manage both from a user perspective because of the requirement to have multiple usernames and passwords for a variety of systems and applications; and for administrators who must maintain these various systems and applications.
- **User Authorization** is the assignment of privileges allowing the user to perform certain functions (e.g. calculate dose, override an interlock, generate a CT scan). The assigned privileges depend upon the authenticated user and the system or application being accessed. The granularity of these functions is very poorly defined and is not standardized across systems.

An Example Problem

- A radiation therapist comes in to work and turns on the treatment workstation computer, username1/password1 is required.
- Another general purpose computer is turned on: username2/password2 is required.
- A treatment application (e.g. scheduling, charting, …) is started up, username3/password3 is required.
- The first patient is treated and an interrupt occurs, username4/password4 is required to clear the interlock.
- The user switches to the general purpose computer to read email: username5/password5 is required.
- During the day, the therapist moves to another treatment unit to cover coffee breaks and must clear another interlock; username6/password6 is required.

The Solution

The radiation therapist arrives at each workstation and either scans a fingerprint, iris, ID card, or provides a username/password and is identified by a user authentication / authorization servers. This system either grants or denies the ability to perform specific tasks on requested systems and applications depending upon the authenticated user. Backup (or distributed) authentication / authorization servers are required in case the primary server fails.

The Benefit

- All existing and new actors, transactions, profiles, and systems would authenticate / authorize with a common authentication / authorization server.

Issues for Discussion

- This Use Case spans all healthcare domains, and is NOT just relevant to the Radiation Oncology domain
- Potenially IHE-RO can emphasize the necessity of this Use Case with IHE-IT

References

- **Brief Template:** **http://wiki.ihe.net/index.php?title=IHERO_UseCase_User_Authentication**
- **Detailed Template:** **http://wiki.ihe.net/index.php?title=IHERO_Detailed_User_Authentication**
- **IHE-IT Infrastructure Profiles (Final Text)**
  - Enterprise User Athentication (EUA): enables single sign-on inside an enterprise by facilitating one name per user for participating devices and software
  - Cross-Enterprise User Assertion (XUA): communicates claims about the identity of an authenticated principal (user, application, system...) across enterprise boundaries - Federated Identity

Scoring Metric: Applicability / Reach

- **Applicable to all health care domains, and to all systems within the radiation oncology domain**

Scoring Metric: Safety

- **By eliminating ‘general’ logins, could facilitate improving process auditing and tracking of user actions**

Scoring Metric: Technical Ease of Implementation

- **Some standards (outside the DICOM domain) exist**

Scoring Metric: Industry Alignment

- ?