Title:
Hierarchical Role-based Access Control for Multi-user Collaborative CAx Environment

Authors:
Chia-Chi Teng, ccteng@byu.edu, Brigham Young University
Francis N. Mensah, fn.mensah@byu.edu, Brigham Young University
J Ekstrom, jekstrom@byu.edu, Brigham Young University
Richard Helps, richard_helps@byu.edu, Brigham Young University
Greg Jensen, cgjensen@byu.edu, Brigham Young University

Keywords:
Multi-user CAD, Collaborative Design, Access Control, Security

DOI: 10.14733/cadconfP.2015.202-206

Introduction:
While the engineering design and manufacturing are highly collaborative processes, main stream commercial CAD and other computer-aided tools still limited to user interface and user experience that are single user in nature. The collection of single user tools unnecessarily constraint the design and manufacturing processes with too much serialization or difficult integration when teams of engineers are involved in complex projects. The lack of concurrent and distributed CAx tools not only limits the productivity and efficiency of the engineers, but also create risk in quality management in today's increasingly complex systems, which in turn lengthens the product development life cycle and increases cost.

Researchers have proposed a variety of methods and tools to facilitate concurrent multi-user collaboration in CAD modeling [7], mostly notably the NX-Connect system built by the National Science Foundation (NSF) Center of e-Design at Brigham Young University which successfully integrated such capability in the one of the world leading commercial CAD application [3]. The NX-Connect system is designed to support engineering teams that are distributed in multiple geographical locations connected through public internet infrastructure [8]. Past experimental design projects involving engineering students from multiple universities across the country have demonstrated the feasibility of such collaborative design process and the potential productivity gain [9].

But for such tools to be introduced to the real-world commercial product design and development, they need to address and comply with a long list of security requirements that are essential in the complicated corporate organization and enterprise network environment. The primary research objective of this paper is to design a security abstract layer that can be integrated with multi-user collaborative computer-aided engineering tools that can properly authenticate users and authorize proper access rights to hierarchy of objects based on the users' roles and access privileges in the organization. In order to validate the concept and create a functional prototype, such a security framework was built, integrated and tested with the current NX-Connect system.

Background:
Much research activity have been dedicated in the past decade to methods and tools for collaborative engineering design [7], including the v-CAx project at the NSF Center of e-Design [2],[4-5]. However, few have focused on the security aspect of such applications, even though protection of information from malicious activities or unintentional errors is a crucial part of any engineering development system. A study by Zhang et al reviewed some of the security requirement in a collaborative system and how they might relate to the general information technology (IT) systems, including some discussion of access

control pertaining to CAD models [10]. Another project showed a prototype of product definition management system incorporating directory service, encryption and secure communication [6].

While the current state of multi-user CAD prototype such as NX-Connect is highly functional with most of the features needed to execute concurrent design of complex engineering models, it does not have any security measures that are mandatory to be deployed in commercial project where protection of intellectual property is essential. For example, the communication between clients and servers are not encrypted and all users have rights to access all objects in the assembly and parts. In order for this multi-user system to be successful in the real-world application, it must include security protocols such as secure transport and access control suited for the target organizations.

In computer science, an access control matrix is an abstract and formal security model of information protection in computer systems that characterizes the rights of users with respect to objects in the system. Role-based access control (RBAC) and mandatory access control (MAC) are two commonly used mechanisms in modern operating systems to manage user access to files, network ports or other objects [1]. Hierarchical role-based access control is a variant of RBAC that incorporates inheritance of attributes in a hierarchy of objects, which is also often used in complex systems. For the scenario of multi-user CAD design, a similar access control matrix can be defined based on the organizational need of the engineering team. Various access rights to certain hierarchy of objects in the assembly can be given to selective roles and privileges of users. We propose that a security framework that combines both RBAC and MAC which can be integrated with multi-user CAD or other computer-aided applications to satisfy the need of a real-world enterprise level concurrent collaborative tool.

Any large-scale engineering organization typically uses a directory service to manage hierarchies of users and resources. Most such services have standardized on an open and vendor-neutral industry standard called Lightweight Directory Access Protocol (LDAP). To effectively integrate a multi-user collaborative tool into the enterprise environment, it is imperative that one must incorporate an access control function that is compatible with an LDAP service such as the Microsoft Active Directory.

Methods:

Figure 1 shows the architecture of the previous NX-Connect system where a simple username/password authentication is taken place against a local and isolated database. In addition, the data streams between clients and server are not encrypted. The system as it was could not be used in a complex commercial engineering development simply because the lack of security protocol.

We will continue using the NX-Connect system as an example to demonstrate our design and functionality. To accomplish the objective of proper access control for the hierarchies of assembly and parts in the collaborative model, new services in the network domain controllers need to be setup to interact with the existing NX-Connect clients and servers which also have to be modified with the addition of a security layer and access control attributes as described below.

Network Domain Services

This security framework is designed to leverage and integrate with domain services that typically already exist in the enterprise network environment.

- LDAP directory service. This server manages directories of resources and user information, including credential, roles and security privilege that are used for RBAC and MAC for objects in the CAD model. We use Microsoft Active Directory as the reference platform since it has the largest installed base and easy to use interface.
- Certificate service. A certificate service works in conjunction with the domain controllers to provide Public Key Infrastructure (PKI) for digital signatures or certificates to enable encrypted communication between clients and servers for improved security. This is particularly important when a complex project involves engineering teams in geographically dispersed locations which require data to transport through public network infrastructure.

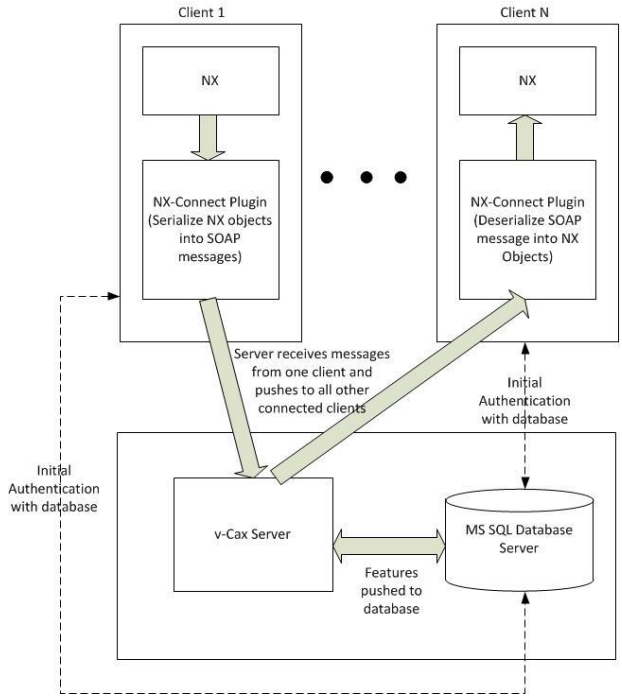

Fig. 1: Previous design of NX-Connect with simple database authentication and no encryption.

NX-Connect Clients
An additional security layer is added to the NX-Connect clients for the security requirement as follows:

- Domain Authentication. Instead of having a different set of login credential, the user now logs in with the same user credential for accessing other corporate network resources and authenticate through the domain directory services. This also enables the system to do RBAC and MAC on the data objects later on.
- Secured Transport Layer (TLS). After the user is authenticated, proper digital signature or certificates are given to the clients (and server) to encrypt their communication channel with TLS, an industry standard secure communication protocol.

NX-Connect Servers
The following modifications are made to the existing servers to complete the security functionalities:

- Database Server. The object class in the database is modified to include access control information including user roles and security privileges that are allow for various actions (create, view, modify or delete). The roles and privileges are security objects defined in the Active Directory server.
- NX-Connect Server. This is the mediator between the client applications and the database server where the model is stored. It now uses the domain authentication to coordinate the secure communication with the clients. In addition, it also work with the Active Directory server to enforce RBAC and MAC and authorize or deny user request to access data objects in the model. Only users with proper role and security privilege are granted access or action to the data object. Hierarchical inheritance of security attributes in the CAD model can also be enforced here.

Figure 2 illustrates the new architecture incorporating all the security features described above. The security functionalities listed above are implemented with Microsoft .NET Framework APIs for:

- Creating and managing custom security objects;

- Certificate and key management;
- Active Directory user authentication and authorization;
- Secure communication (TLS).

The new layer of security functions are compiled into a separate dynamic link library (DLL) which can be easily integrated with other similar computer-aided engineering tools.

Results:

A functional prototype was successfully built and validated with a simple simulated engineering organization which contains three levels/roles of engineers and two levels of security privileges. A small set of simple CAD assemblies each containing multiple parts and various access control settings were built with this new system to mimic real world applications. The system was tested with multiple users/clients with different roles and privilege concurrently connecting to the server through domain authentication while working on the same model. A set of scenarios were executed to validate the security and access control requirement.

Figure 3 shows an example of client views of a small assembly of engine parts from two users where user 1 has rights to view and modify the entire assembly and user 2 has rights to view only a subset of parts without being able to make changes.

Conclusion:

This paper proposed a compelling design to address the need of security protocols in the current state of the art multi-user concurrent collaborative engineering tools. Role-based and mandatory access control integrated with standard enterprise network service is a practical and effective approach that provides sufficient functionality for common security requirements. The resulting prototype may has certain limitations and requires more stringent testing, however, the new NX-Connect with built-in RBAC and MAC has shown that multi-user CAD system with sufficient security features can be a reality in real-world complex commercial engineering projects in not so distant future.

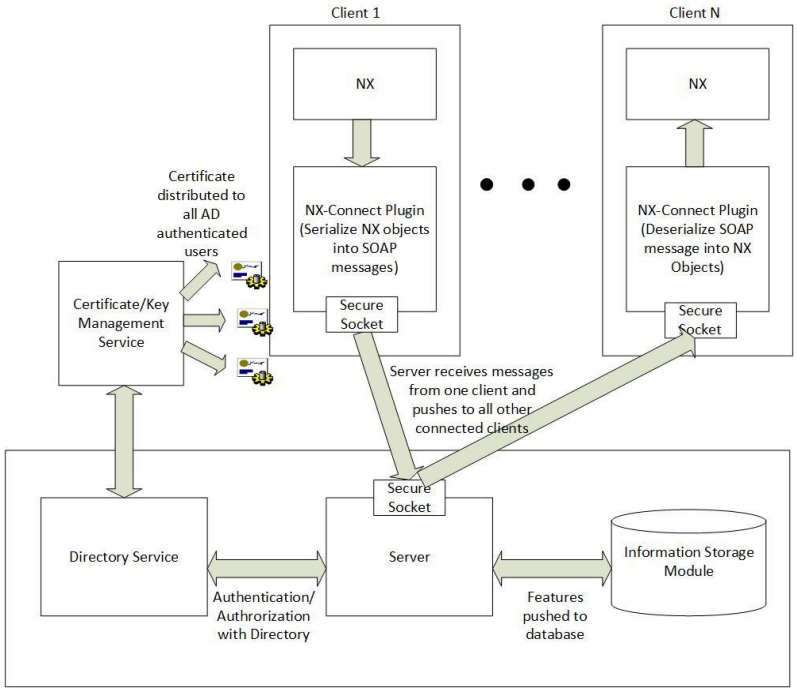

Fig. 2: Proposed new system with: (1) authentication with directory service, (2) encrypted data stream, (c) RBAC and MAC for objects in the model assembly.

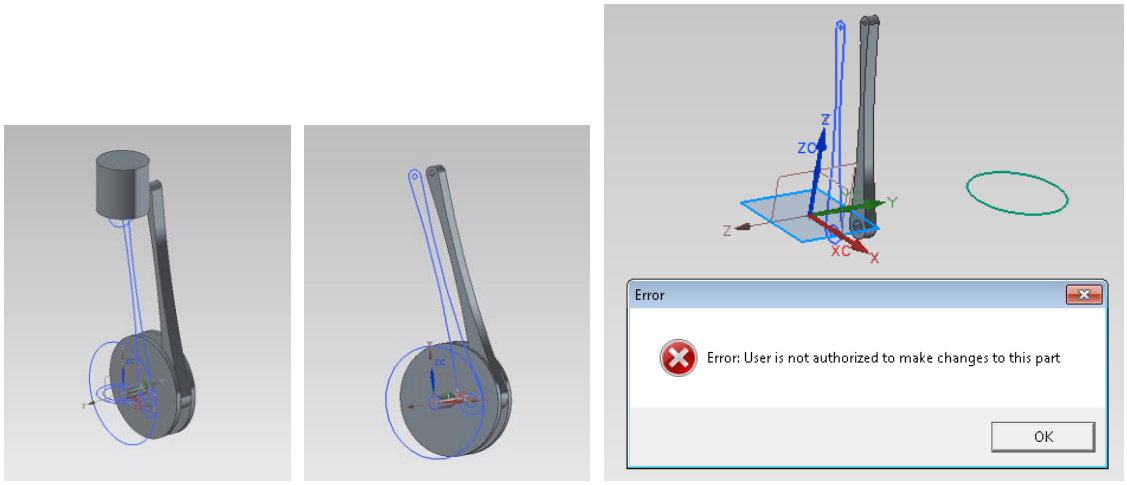

Fig. 3: From left to right, NX client view for user 1, NX client view for user 2, and authorization error resulted from user 2 trying to modify a part without proper access rights.

References:

[1] Kim, S.; Kim, D.-K.; Lu, L.; Park, S.; Kim, S.: A Feature-Based Modeling Approach for Building Hybrid Access Control Systems, Fifth International Conference on Secure Software Integration and Reliability Improvement, 2011, 88–97. http://dx.doi.org/10.1109/SSIRI.2011.16

[2] Moncur, R; Jensen, C. G.; Teng, C.-C.; Red, E.: Data Consistency and Conflict Avoidance in a Multi-User CAx Environment, Computer-Aided Design & Applications, 10(5), 2013, 727–44. http://dx.doi.org/10.3722/cadaps.2013.727-744

[3] Red, E.; Jensen, C. G.; Ryskamp, J.; Mix, K.: NXConnect: Multi-User CAx on a Commercial Engineering Software Application, PACE Glob Annu Forum, 2010, 1–9.

[4] Red, E.; Holyoak, V.; Jensen, C. G.; Marshall, F.; Ryskamp, J.; Xu, Yue.: v-CAx: A Research Agenda for Collaborative Computer-Aided Applications, Computer-Aided Design & Applications, 7(3), 2010, 387-404. http://dx.doi.org/10.3722/cadaps.2010.387-404

[5] Red, E.; French, D.; Jensen, C. G.; Walker, S. S.; Madsen, P.:. 2013. Emerging Design Methods and Tools in Collaborative Product Development, Journal of Computing and Information Science in Engineering, 13(3), 2013.. http://dx.doi.org/10.1115/1.4023917

[6] Rouibah, K.; Ould-Ali, S.: Dynamic Data Sharing and Security in a Collaborative Product Definition Management System, Robotics and Computer-Integrated Manufacturing, 23(2), 2007, 217–33. http://dx.doi.org/10.1016/j.rcim.2006.02.011

[7] Shen, W.; Hao, Q.; Li, W.: Computer Supported Collaborative Design: Retrospective and Perspective, Computers in Industry, 59(9), 2008, 855–62. http://dx.doi.org/10.1016/j.compind.2008.07.001

[8] Winn, J.; Bright, T.; Jensen, C. G.; Teng, C.-C.: Using game server technology on fully distributed architectures for collaborative multi-user CAx applications, CoDesign, International Journal of CoCreate in Design and the Arts, 9(3), 2012, 178-189. http://dx.doi.org/10.1080/15710882.2013.824482

[9] Zender, F.; Schrage, D.; Richey, M.; Black, A.; Sullivan, J.; Gorrell, S.; Jensen, C. G.: Wing design as a symphony of geographically dispersed, multi-disciplinary, undergraduate students, 54th AIAA/ASME/ASCE/AHS/ASC Struct. Dyn. Mater. Conf., 2013.

[10] Zhang, D. Y.; Wang, L.; Zeng, Y.: Secure Collaborative Product Development : A Literature Review, International Conference on Product Life Cycle Management, 2008, 331–40.