5010
Dealing with Information Accessibililty and Security

Sara Lafrance, President
Century Analysis, Inc.
114 Center Ave., Pacheco, CA 94553
(510) 680-7800

Security control used to be relatively straightforward to implement. With limited-function workstations physically attached to a particular processor, end users could be relegated to specific applications, and, in most cases, prevented from accessing unauthorized data through application-based security alone.

Today this is no longer the case. Workstations are more powerful and are typically attached to a network (either direct or remotely,) on which various applications reside, making end users only a password away from a wide variety of information sources. And the advent of technologies like Internet only complicate the problem further.

Providing appropriate access to information while ensuring that it is protected from unauthorized intrusion is not an easy mandate. It requires more than the security methodologies utilized to date.

The issues that must be considered fall into three general categories: administrative issues ... including proper password procedures, day-to-day monitoring, periodic audits, back-up procedures and other such security processes; authorization issues ... including user IDs and identity verification; and application control issues ...including user-specific permissions and application access audit trails. (See Figure A)

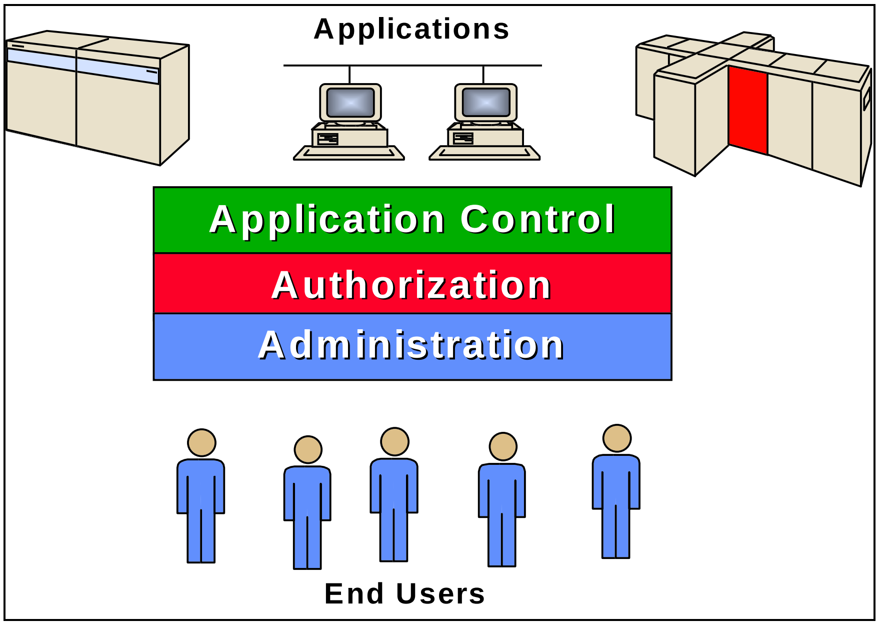

Figure A

Probably, the most difficult issue to address is that of authorization. A system can only be secure if it is known who is accessing it. Passwords act as the first line of defense. But equally important is ensuring the individual entering the password is actually who he or she claims to be.

One of the more recently developed technologies that addresses the authorization issue is that of "Single Logon," which takes the responsibility for managing security such that end users enter a single logon and password and are presented with a workplace that shows only the applications they are authorized to access. Individual sessions are controlled by a security broker each time a session is opened or closed, eliminating the need for end users to memorize individual passwords by application. All significant end user activity is also logged so as to allow for analysis. (See Figure B)

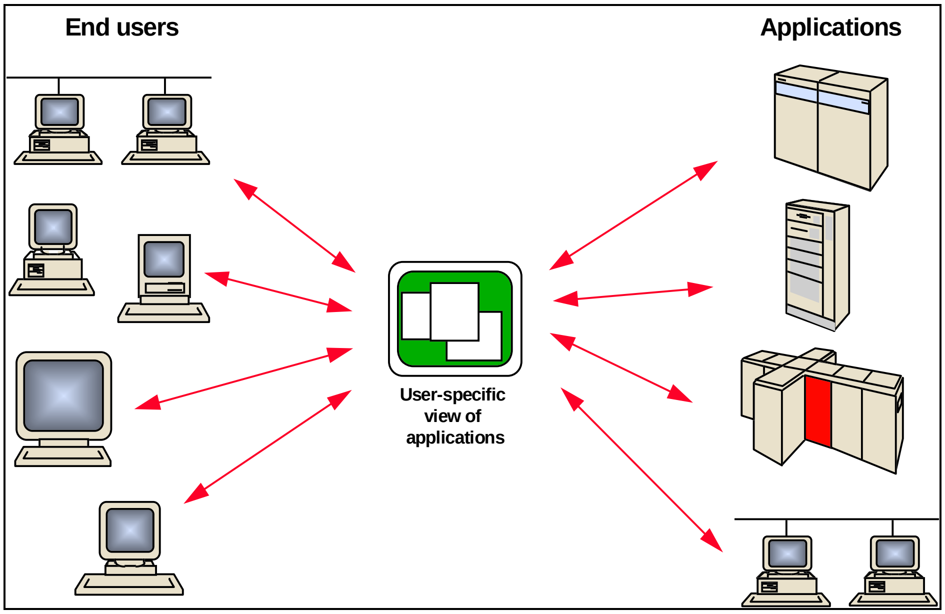

Figure B

Because end users have no knowledge of how to access applications directly, they cannot share with others, either intentionally or inadvertently by virtue of having written them down, password access. Given that it is not uncommon for end users in complex environments to actually have ten to thirty different passwords to various systems, Single Logon technology also resolves a procedural issue as well.

There are several commercial implementations of Single Logon technology, the most powerful of which include three components: access control, whereby the system takes responsibility for presenting only authorized applications to individual end users and managing passwords to the various applications, as well as automatically updating application passwords when they expire; authentication, which ensures that transactions are initiated only by authorized end users; and time-stamped encryption of all network traffic, which ensures that information is not intercepted or otherwise compromised. (See Figure C)

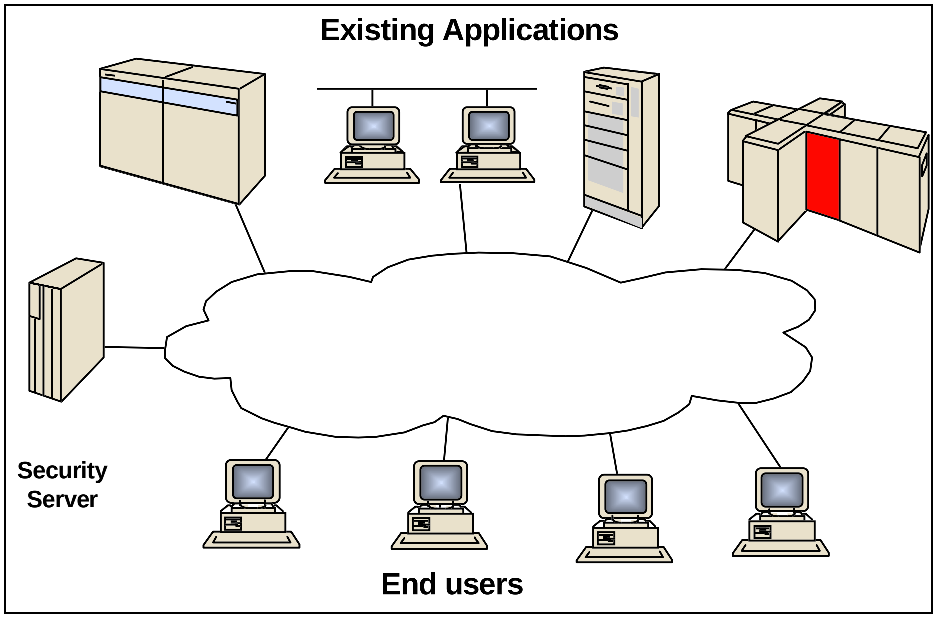

Figure C

Two industry standards have evolved that also should be considered when implementing a Single Logon solution -- DES for encryption (transforming data into a form unreadable by anyone without a secret decryption key) and Kerberos for authentication (a methodology for ensuring the identity of the sender and the integrity of the message).

An adjunct area of security control which is quickly gaining acceptance is Application Control, by which a new layer of security is introduced between the end users and the applications they use, transparently to the applications. Application Control limits end users' use of applications in such a way that only particular screens are visible, only user-specific records can be requested, and all uses of the applications can be recorded for audit purposes.

In its simplest form, Application Control technology can transparently monitor existing end user interactions with applications and reuse information found in those screens to feed other applications. In a more advanced form, Application Control technology can be used to add screen fields to existing end user screens. In its most advanced form, Application Control technology can be used to build simplified consolidated views for personnel that need access to a number of information sources or for allowing business associates to gain computer access to various information sources. (See Figure D)

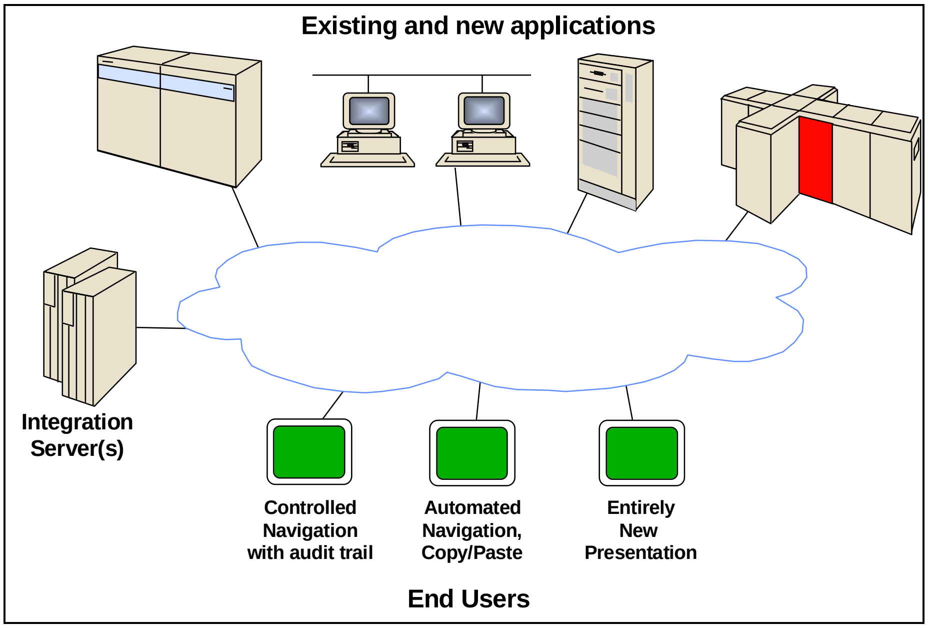
Existing and new applications
Integration Server(s)
Controlled Navigation with audit trail
Automated Navigation, Copy/Paste
Entirely New Presentation
End Users

Figure D

Despite the complex environments under which enterprises today operate, proper security is achievable. The combination of comprehensive administrative procedures, a strong Single Logon solution, and application control can provide a secure distributed computing environment without sacrificing end user productivity requirements. (See Figure E)

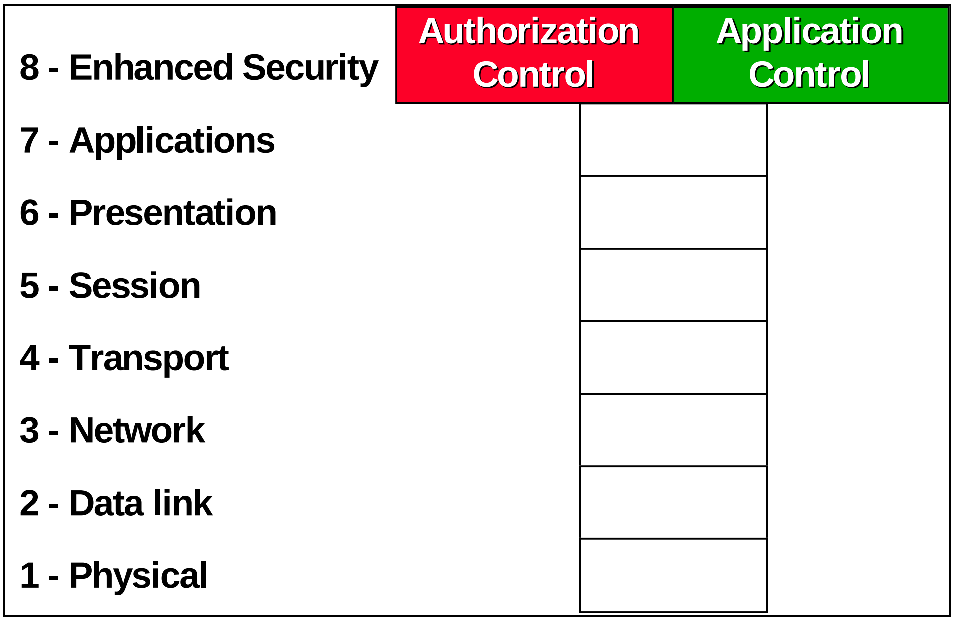

Figure E