

Access Control Challenge for a Global Financial Institution

Josiah Lam, CISM, CISA, CISSP, ACCA, CPA

Vice President, JPMorgan Chase

Josiah.Lam@jpmorgan.com

October 05, 2004



Copyright © 2004 J.P. Morgan Chase & Co. All rights reserved.
May not be reproduced or distributed without written permission of J.P. Morgan Chase & Co.



Agenda



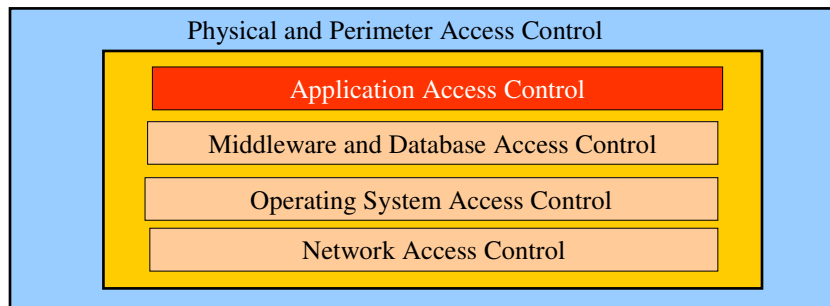
Page 2
Copyright © 2004 J.P. Morgan Chase & Co. All rights reserved.
May not be reproduced or distributed without written permission of J.P. Morgan Chase & Co.



Part I – Introduction & Concept



Access Control is Needed Everywhere



- Traditional view (only address certain specific vulnerabilities)
 - Attempts to integrate security at single layer
 - Access control by users or by objects
- Definition
 - Whether the requestor is allowed to perform a particular operation

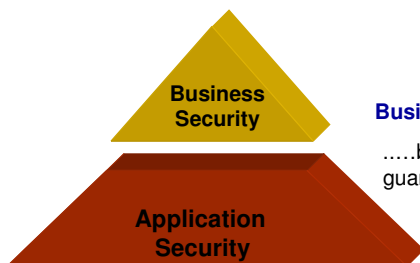
Application Security vs. Business Security

Application Security

- controls the access of information by **authorized** users only.
- e.g. Members of the finance division are allowed to query the accounting database.

Business Security

- addresses the use and **misuse** of information by authorized users
- e.g. Researcher can read a customer's data for the purpose of new product development if the Compliance Unit has explicitly consented to release these data.



Business Security requires effective application security
but effective **application security** does not guarantee effective business security

Chinese Wall -- Imaginary Wall of Separation

- Chinese Wall Policy refers to a system of information barriers designed to limit the flow of **inside information** from areas that routinely have access to such information ("insider areas") to those areas that trade in or sell securities or provide investment advice regarding securities ("public areas").
- The Chinese Wall Policy prohibits anyone in an insider area from communicating inside information, however obtained, to anyone in a public area, subject to limited exceptions approved by the relevant Compliance unit.

PUBLIC AREA

- Sales, Trading, Research
- Investment Management

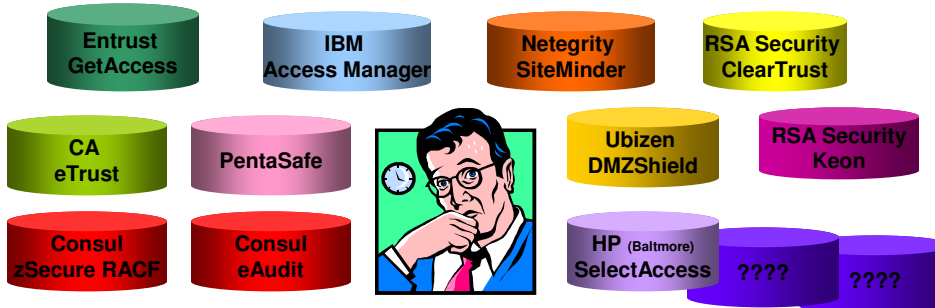
INSIDER

- Investment Banking
- Commercial Lending
- Restructuring
- Credit
- Mergers and Acquisitions

Part II – Challenges for Global FIs



Typical Access Control Environment

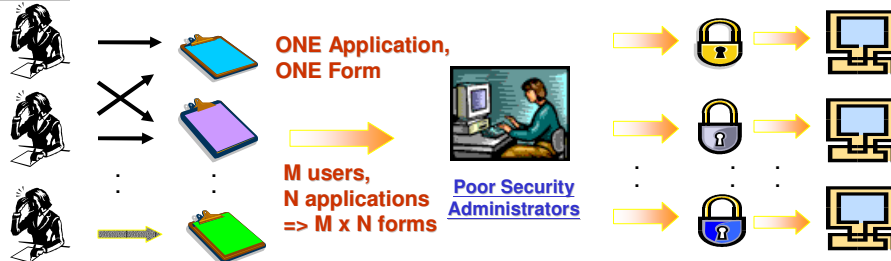


✦ Because of Merger & Acquisition and other historical reasons, Global FI developers have to deal with multiple access control vendors and products with overlapping functionality.

- is there a single-source supplier to meet all requirements?
- How can we convert to few products?

Current Access Control Administration

USERS



Security Administrators spends **40%** effort on application administration:

(vs. 14% for NT/NDS admin,
7% for AS/400 admin.
5% for UNIX admin)

N Applications
=> N Access Control

FAQs in Global Financial Institution

- ❖ How to reduce the number of home-grown access control for business applications of different application architecture in heterogeneous operating environment?
- ❖ How to reduce the total cost of ownership ?
 - Day-to-day maintenance, deployment cost, operation support and administrative cost, license cost
- ❖ How to enforce an enterprise-wide security policy to have consistent control across the whole company?
- ❖ How to prevent Conflict of interest for Users with multiple roles in multiple applications across multiple line of businesses ?

General Challenge on Access Control

✦ Classification :

- How to classify the information, users and access purpose ?
- the nature of insider and public information is very dynamic and time-sensitive
- Data Classification criteria are complex and influenced by local legislation

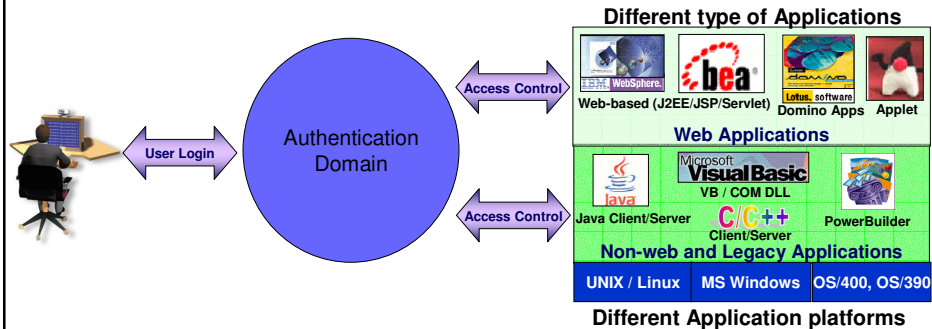
✦ Implementation:

- How to dynamically associate the proper access control ?
- How to effectively keep track of these accesses in thousands applications and reports any illegal access?
- How to effectively notify the customers for any data leakage?

Part III – Implementation Lessons Learnt



ONE Generic Access Control solution



- ✦ Fully integrate with different authentication mechanism
- ✦ External but plug-able to business applications
- ✦ One solution applicable for different application types in different platforms.

How to Stay In-line

- ✦ Application developers -- Defining authorization privileges
 - Resources to user groups/roles mapping and business rules
- ✦ User Managers – Defining user entitlement
 - User to user group and User application attributes
- ✦ Security Administrators -- Setting up the privileges
 - Set up application access control settings and user groupings
- ✦ Technology Audit
 - Review application access control and identify conflict of interests

Part IV – Recommendation and Summary



Start on the Right Track

- ✦ Developing a sound architecture
- ✦ Selecting vendors and partners
 - Promote encapsulation of vendor services
 - Focus on the application integration
 - Don't build your own stuffs, unless interim & absolutely necessary
- ✦ Deploying general purpose solution
 - Start with majority of application and ongoing to integrate additional applications in minority.
- ✦ Clear roadmap and migration plan
- ✦ Reputation and quality of services – critical to get ADs buy-in

Access Control Product Selection Criteria

- ✦ Can be scaled up from concept buy-in to pilot and finally phased deployment.
- ✦ Cannot block the application execution.
- ✦ Can adapt to different line of business requirements.
- ✦ Can manage hundred thousands users and resources.
- ✦ Can be implemented by a few security experts. (rare resources!)
- ✦ Can be deployed to different application architecture & platform.
- ✦ Access control activities must be auditable and traceable.
- ✦ Access control cannot be the single point of failure.

Questions and Answers

