Security Risks For High-Volume Users

Roger Westman, CISSP
IIT Research Institute
Advance Technology Group
Lanham, Maryland 20706
+1-301-918-1199; +1-301-731-6378 (fax)
www.iitri.com
E-mail: rwestman@atg.iitri.com

THIC Meeting, DoubleTree Hotel at Tysons Corner
Fairfax VA 22043
23 April 1997

Agenda

- High-volume user characteristics
- Information system security definition
- Security risk concerns
- Threat types
- Summary

High-Volume User Characteristics

- **Corporate data warehouses featuring**
  - **Terabyte storage requirements**
  - **Corporate-wide resource**
- **Distributed data stores for local use**
  - **Gigabyte storage requirements**
  - **Replicate part of corporate data warehouse**
- **Data storage devices directly connected to network**

Information System Security Definition

- Management, operational, and technical controls required to achieve an acceptable degree of risk
- Measures and controls that protect data processed and the services provided by an information system against (accidental or intentional)
  - Unauthorized disclosure
  - Unauthorized modification
  - Unauthorized destruction
  - Unauthorized unavailability

Security Risk Concerns—Corporate Warehouse

- Centralizing data makes the impact of illicit entry, accidental loss, etc., more severe
- Data aggregation is a concern because a user's access to a large volume of data increases the probability that a user may be able to make inferences about actions/data that the user is not cleared for
- A large number of users with different sensitivity levels accessing a large amount of data increases the number of permutations that must be addressed by security software

Security Risk Concerns—Corporate Warehouse (Cont)

- Different data elements within a large volume of data may have different, conflicting security requirements
- The sensitivity level of the entire warehouse may be greater than the sensitivity level of the individual data elements because of data aggregation and centralization of data

Security Risk Concerns—Distributed Data Stores

- **Distributed data stores are starting to be stored on devices located outside of main computer centers**
  - **Devices could be misappropriated**
  - **Devices may be under end-user control**
- **Distributed data stores reply on local system protection capabilities**
  - **High-end data management and security functionality may not be available on all local systems**
- **Distributed stores may lose synchronization with other distributed stores**

Security Risk Concerns— Network Attached Device

- The network allows for an increased number of potential users
- Entry or modification of data may not be traceable to a specific user
- A directly connected storage device may only have limited security functionality
- The attached storage device may not be able to prioritize and schedule users because of network constraints
- Network communications bandwidth may not be dedicated to the data storage device

Security Risk Concerns—General

- **Specific data on a data storage device may not be easily sanitized**
- **Encrypting all data on a storage device may not be practical**
  - **Performance impact may result for read and write operations**
  - **Key management complexity may increase**
  - **Current encryption algorithms may not have an adequate life span (e.g., 30 years) because of increases in computing power**
- **An increase in amount of data increases the amount of noise that needs to be filtered in order to find specific information**

Threats

- **Accidental**
  - **Weather**
  - **Environmental**
  - **Hardware, software errors**
- **Intentional**
  - **Internal employee**
  - **Competitor**
  - **Foreign government**
  - **Hacker—noncriminal intent**
  - **Criminal (terrorist, financial)**

Summary

- Security concerns common to general information system processing are exacerbated by very large data volumes
- Each data management technique such as warehousing, distributed data stores, and network attached storage devices carry unique security risks
- The need to “recycle” storage media presents additional risks
- Storage management specialists need to be aware of security concerns and work in partnership with security specialists to find suitable solutions