Minnesota Department of Employee Relations
Minnesota Department of Finance
SEMA4 Database Security Audit

December 1998

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 296-1727.

Financial Audit Division
Office of the Legislative Auditor
State of Minnesota

98-63

Centennial Office Building, Saint Paul, MN 55155 • 612/296-1727

STATE OF MINNESOTA

OFFICE OF THE LEGISLATIVE AUDITOR

JAMES R. NOBLES, LEGISLATIVE AUDITOR

Senator Deanna Wiener, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Karen Carpenter, Commissioner
Department of Employee Relations

Mr. Wayne Simoneau, Commissioner
Department of Finance

We have audited selected areas relating to security of the Minnesota Statewide Employee Management System (SEMA4), as further explained in Chapter 1. Our audit focused on how the Departments of Employee Relations and Finance control access to the SEMA4 database. We emphasize that this has not been a complete audit of the SEMA4 system. The following Summary highlights the specific objectives of our audit and the conclusions that we reached. We discuss these issues more fully in the individual chapters of the report.

We conducted our audit in accordance with *Government Auditing Standards,* as issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. They also require that we design the audit to provide reasonable assurance that the Departments of Employee Relations and Finance complied with provisions of laws, regulations, contracts, and grants that are significant to the audit. Management of the Departments of Employee Relations and Finance are responsible for establishing and maintaining the internal control structure and for compliance with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of the Departments of Employee Relations and Finance. This restriction is not intended to limit the distribution of this report, which was released as a public document on December 11, 1998.

James R. Nobles
Legislative Auditor

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: July 31, 1998

Report Signed On: December 8, 1998

1ST FLOOR SOUTH, CENTENNIAL BUILDING • 658 CEDAR STREET • ST. PAUL, MN 55155
TELEPHONE 651/296-4708 • TDD RELAY 651/297-5353 • FAX 651/296-4712 • WEB SITE http://www.auditor.leg.state.mn.us

SUMMARY

State of Minnesota
Office of the Legislative Auditor
1st Floor Centennial Building
658 Cedar Street • St. Paul, MN 55155
(651)296-1727 • FAX (651)296-4712
TDD Relay: 1-800-627-3529
email: auditor@state.mn.us
URL: http://www.auditor.leg.state.mn.us

Minnesota Department of Employee Relations
Minnesota Department of Finance
SEMA4 Database Security Audit

Public Release Date: December 11, 1998 No. 98-63

Background

The Statewide Employee Management System (SEMA4) is an integrated human resource and payroll system that is used by most state agencies. SEMA4 data resides in a database at the central mainframe computer center managed by the Department of Administration's Intertechnologies Group (Intertech). Access to this data is provided by a software package called DB2. ACF2, SEMA4, and DB2 security software help prevent unauthorized access to sensitive payroll and personnel data. ACF2 authenticates the identity of users who try to access Intertech's central mainframe computer. Once authenticated, users also need a special security profile within SEMA4. These security profiles limit different types of users to the specific screens that they will need to fulfill their job responsibilities. Finally, DB2 prevents users from directly accessing the database without using the appropriate SEMA4 screens.

Audit Objectives and Conclusions

This audit focused on how the Departments of Employee Relations and Finance prevent unauthorized users from directly accessing DB2 and the underlying SEMA4 data tables. We refer to these types of connections as "backdoor" access methods because they provide users with an opportunity to circumvent important SEMA4 screen edits.

Our audit revealed that the Departments of Employee Relations and Finance do not have effective security administration procedures to protect the SEMA4 database. The departments do not have a detailed understanding of pertinent database security risks or formal procedures to control those risks. Instead, the departments place a great deal of reliance on security administration duties performed by employees in the Department of Administration's Intertechnologies Group (Intertech). We feel that this level of reliance may be unjustified because each agency's security administration roles and responsibilities have not been clearly defined.

We found significant weaknesses when reviewing detailed security data. Of greatest significance, some users may have more clearance than they need to fulfill their normal job duties. We also found that the data used by DB2 and ACF2 to control access to the SEMA4 database has not been properly maintained. Unauthorized changes to critical data could occur and remain undetected because the departments do not log the activities of all users with powerful backdoor security clearances. Finally, the departments' procedures for controlling user accounts and passwords are susceptible to abuse.

The Departments of Employee Relations and Finance agreed with the findings and recommendations in this report.

Department of Employee Relations
Department of Finance
SEMA4 Database Security Audit

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA	Information Systems Audit Manager
Mark Mathison, CPA, CISA	Auditor-in-Charge
Keith Bispala	Auditor

Exit Conference

We discussed the issues in this report with the following staff of the Department of Employee Relations and the Department of Finance on November 20, 1998:

Department of Employee Relations:

Chris Goodwill	Administrative Services Division Manager
Steve Jorgenson	Information Systems Manager

Department of Finance:

Michael Ladd	Assistant Commissioner

Chapter 1. Introduction

The State Employee Management System (SEMA4) is an integrated human resource and payroll system that is used by most state agencies. SEMA4 contains detailed personnel records for over 60,000 state employees. The system annually processes over five million payroll and business expense transactions, totaling approximately $2.2 billion.

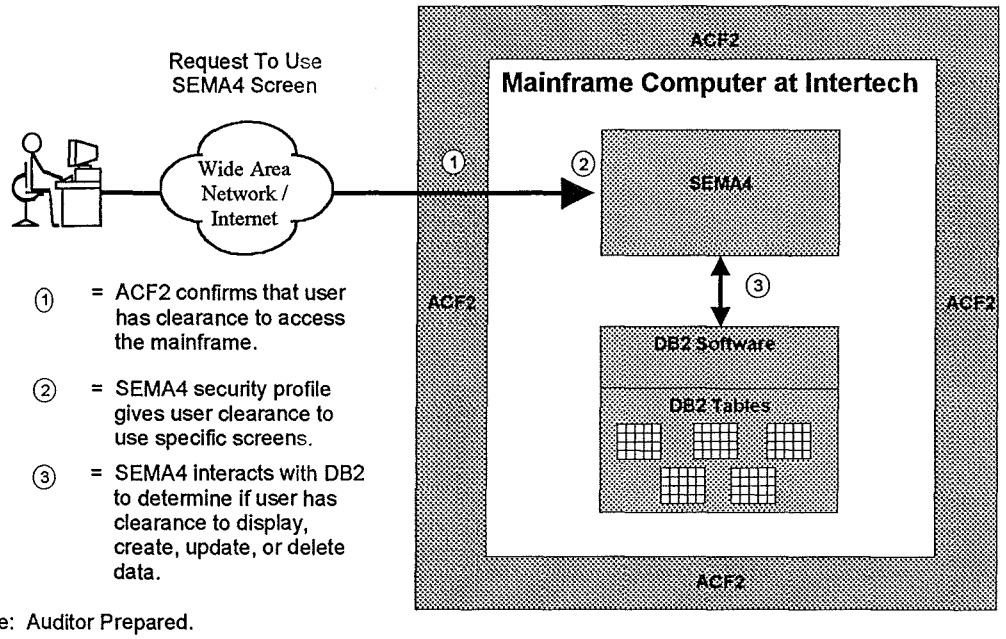
The system operates in a complex computing environment called "client server." The term client server refers to an environment where several different computers work together to accomplish a task. Typically, these computers communicate over a high-speed, wide area network or the Internet. With SEMA4, the personal computer (i.e. the client) of a state agency user completes a significant portion of the computer processing. The remaining processing occurs on a central mainframe computer. Communications between agency computers and the central mainframe occur over the State of Minnesota's wide area network.

Information systems professionals in the Department of Employee Relations and the Department of Finance are responsible for maintaining the SEMA4 software. They also establish procedures to prevent the unauthorized use, modification, or disclosure of SEMA4 data. To fulfill these responsibilities, the departments rely on assistance from the Department of Administration's Intertechnologies Group (Intertech). Intertech manages the state's central mainframe computing center and the wide area network.

All SEMA4 payroll and personnel data resides in a database at Intertech's central mainframe computer center. Access to this data is provided by a software package called DB2, developed by International Business Machines. DB2 is a relational database management system, meaning that data is stored in spreadsheet-like tables. At the time of our audit, the SEMA4 database had over 800 tables, some of which contained millions of rows of sensitive payroll and personnel data.

ACF2, SEMA4, and DB2 security software help prevent unauthorized access to sensitive payroll and personnel data. ACF2 authenticates the identity of users who try to access Intertech's central mainframe computer. Once authenticated, users also need a special security profile within SEMA4. These security profiles limit different types of users to the specific screens that they will need to fulfill their job responsibilities. Finally, DB2 prevents users from directly accessing the database without using the appropriate SEMA4 screens. Figure 1-1 illustrates how ACF2, SEMA4 security profiles, and DB2 work together to control access to payroll and personnel screens and data.

Figure 1-1
Controlling Access to SEMA4 Payroll and Personnel Screens and Data

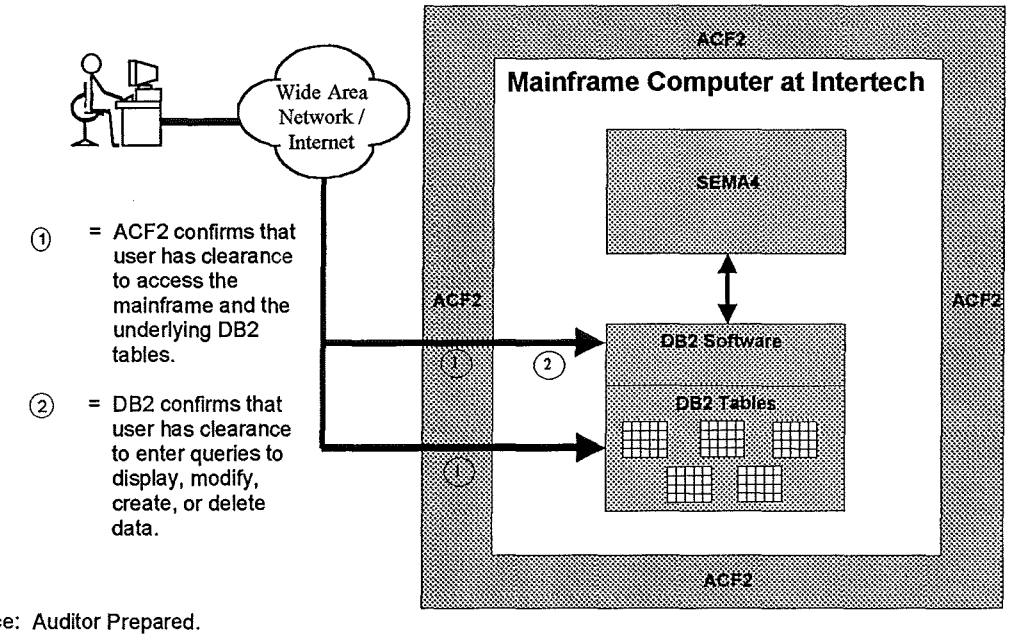


Source: Auditor Prepared.

Each SEMA4 screen contains numerous edit programs. These edit programs are extremely important because they protect the integrity of the data that flows into the database. Providing users with clearance to directly access the database without using the SEMA4 screens is very risky and could lead to the widespread destruction of data. However, it is important to recognize that some information systems professionals need this type of clearance to correct data errors and perform other database maintenance activities. Logging all work done by employees with these powerful "backdoor" security clearances is highly recommended.

Relational database management systems, like DB2, are particularly vulnerable to backdoor accesses. In fact, information systems professionals have at their disposal a variety of different mainframe-based software that can directly interact with the DB2 database management system. Software also exists that will let users connect to DB2 from personal computers that are attached to the Internet. Without proper security, unauthorized persons could use these software packages to connect to DB2 to display, create, modify, or even delete data. Therefore, it is very important for organizations to understand these risks and develop compensating security measures. As illustrated in Figure 1-2, organizations need strong controls to prevent unauthorized users from connecting to DB2. Organizations also need controls to prevent unauthorized users from directly accessing the data tables that underlie the DB2 database management system.

Figure 1-2
Preventing Unauthorized Users from Directly Accessing DB2 or its Underlying Data Tables



Source: Auditor Prepared.

During past audits, the Office of the Legislative Auditor has reviewed the administration of SEMA4 security profiles. We found that these security profiles limit the vast majority of employees to the payroll and personnel screens that they need to use to fulfill their job responsibilities. However, we did identify some users with excessive security clearances. The Departments of Employee Relations and Finance are now requiring agencies to justify the need for these powerful security clearances. The objective of this audit was to analyze how the Departments of Employee Relations and Finance control backdoor access to the DB2 database management system and its underlying data tables. Chapter 2 discusses the scope of our work and the conclusions that we reached.

Chapter 2. SEMA4 Database Security

Chapter Conclusions

The Departments of Employee Relations and Finance do not have effective security administration procedures to protect the SEMA4 database. Our audit revealed that the departments do not have a detailed understanding of pertinent database security risks or formal procedures to control those risks. Instead, the departments place a great deal of reliance on security administration duties performed by employees in the Department of Administration's Intertechnologies Group (Intertech). We feel that this level of reliance may be unjustified because each agency's security administration roles and responsibilities have not been clearly defined.

We found significant weaknesses when reviewing detailed security data. Of greatest significance, some users may have more clearance than they need to fulfill their normal job duties. We also found that the data used by DB2 and ACF2 to control access to the SEMA4 database has not been properly maintained. Unauthorized changes to critical data could occur and remain undetected because the departments do not log the activities of all users with powerful backdoor security clearances. Finally, the departments' procedures for controlling user accounts and passwords are susceptible to abuse.

The state uses both ACF2 and DB2 security features to prevent unauthorized users from accessing the SEMA4 database. ACF2 prevents unauthorized users from accessing the mainframe computer. ACF2 also protects the data tables underlying the DB2 database management system. DB2 defines the specific users or groups of users that can interact with the database management system to access SEMA4 data or perform administrative activities.

Audit Objectives and Methodology

This audit focused on how the Departments of Employee Relations and Finance prevent unauthorized users from directly accessing DB2 and the underlying SEMA4 data tables. We refer to these types of connections as "backdoor" access methods because they provide users with an opportunity to circumvent important SEMA4 screen edits. Specifically, we designed our work to answer the following questions:

- Did the departments identify potential security risks to the SEMA4 data and design policies and procedures to mitigate those risks?

- Did the departments limit backdoor security clearances to only those employees who need such clearances to fulfill their job responsibilities?

To answer these questions, we interviewed information systems professionals from the Departments of Finance, Employee Relations, and Administration. We also analyzed both DB2 and ACF2 security documentation. Finally, we performed security tests using various DB2 utility programs.

Conclusions

The departments did not identify potential security risks to the SEMA4 data, nor did they design policies and procedures to mitigate those risks. The departments also did not limit backdoor security clearances to only those employees who need such clearances to fulfill their job responsibilities.

Finding 1 discusses our concerns with the overall design and management of the security infrastructure for the SEMA4 database. As discussed in Finding 2, we also found many users who appear to have more clearance than they need to complete their normal job duties. Finding 3 discusses weaknesses in the departments' security monitoring procedures. And lastly, Finding 4 discusses certain password management weaknesses that came to our attention.

1. The Departments of Employee Relations and Finance do not have effective security administration procedures to protect the SEMA4 database.

The departments have not performed a risk assessment to identify potential security exposures to the SEMA4 database. The departments also have not developed written security policies and procedures to mitigate those risks. When questioned, the departments could not tell us who has clearance to interact with DB2 to gain access to SEMA4 data. They also could not explain how existing security software controls those direct database connections. Instead, the departments referred many of our technical security questions to Intertech. Unfortunately, Intertech employees also could not answer many of these technical questions.

The Departments of Employee Relations and Finance maintain the SEMA4 software and data on behalf of all state agencies. We feel that part of this responsibility includes ensuring that an effective security infrastructure exists. Our audit revealed that the departments do not have a detailed understanding of pertinent database security risks or formal procedures to control those risks. We also found very little documentation to support or explain the current security infrastructure. We have reservations about the level of reliance that the departments currently place on Intertech to manage the database security infrastructure. In fact, we feel that this high level of reliance may be unjustified because specific security administration roles and responsibilities have never been defined.

It is difficult to develop and maintain an effective security infrastructure without policies, procedures, and documentation. These are the benchmarks that security officers use to judge the appropriateness of individual clearances. While reviewing ACF2 and DB2 data, we found

duplicate security clearances for some users. We also found some dormant security data, meaning that it no longer can grant or deny access to anyone. Finally, as discussed in Finding 2, we found many users who appear to have more clearance than necessary to complete their job duties.

Recommendations

- *The departments should perform a risk assessment to identify potential security exposures to the SEMA4 database.*
- *The departments should develop written policies and procedures to control backdoor security clearances.*
- *The departments should clarify and document Intertech's security administration roles and responsibilities.*
- *The departments should develop documentation to support the existing security infrastructure.*
- *The departments should review all security data on a continuous basis.*

2. Some users have inappropriate security clearances to the SEMA4 database.

We found 45 users who have clearance to interact with DB2 to modify SEMA4 payroll and personnel data. We reviewed these clearances and feel that many of the users may not need this high level of security clearance to fulfill their job responsibilities. For example, many of these users are computer programmers. Computer programmers typically only need to work with test data in a special test environment. We recognize that programmers sometimes need access to production data to perform maintenance functions. However, these occasions are rare and do not merit giving continuous and unfettered access. We also found a group of database administrators who may have more clearance than they need to fulfill their job duties.

Recommendation

- *The departments should review all security clearances that give users the ability to interact with DB2 to display, modify, create, or delete SEMA4 data.*

3. The departments do not monitor some high-risk security events.

The departments do not log or monitor the activities performed by some users with powerful backdoor security clearances. The departments currently log SEMA4 data changes made by 12 users with powerful backdoor security clearances. However, data changes made by 33 other users with similar security clearances are not logged or reviewed. We feel that unauthorized

changes could occur and remain undetected because the departments do not monitor these high-risk security events.

We also could not find anyone who reviews DB2 security events on an ongoing basis. DB2 logs all unsuccessful attempts to access the system as well as other security-related events. However, we could not find anyone who reviews this information to determine if unauthorized users were attempting to compromise the system.

Recommendations

- *The departments should review all SEMA4 database changes made by individuals with powerful backdoor security clearances.*

- *The departments should establish procedures for reviewing DB2 security events on a continuing basis.*

4. The departments are not taking sufficient steps to protect the passwords of some user accounts.

One security administrator in the Department of Employee Relations knows the passwords for most SEMA4 users accounts. This information is stored in both an electronic file and on paper. We discussed the controls over both storage formats and found weaknesses. We feel that the departments need to take immediate action to improve controls over this sensitive security data. The departments also need to search for a new security solution that does not require one user to know other users' passwords.

Recommendations

- *The departments should search for an alternative security solution that protects the confidentiality of passwords.*

- *The departments should take additional steps to protect existing password data from unauthorized disclosure.*

Minnesota
Department of
Employee
Relations

Leadership and partnership in human resource management

Memo

DATE: November 30, 1998

TO: Christopher Buse, Information Systems Audit Manager,
Office of the Legislative Auditor

FROM: Karen Carpenter, Commissioner, Department of Employee Relations
Wayne Simoneau, Commissioner, Department of Finance

RE: Response to SEMA4 Database Security Audit draft report and exit conference

Thank you for providing the Office of the Legislative Auditor (OLA) findings and recommendations to the Departments of Employee Relations and Finance. We take our responsibilities for data security very seriously. We have made it a high priority to work to correct the weaknesses and gaps you identified in our security procedures. In the paragraphs below, we are providing our clarified understanding of some of the findings and our plans to address the recommendations.

We agree with you on our clarification at the exit conference for the scope of our security responsibility. It does not include providing security measures to prevent unauthorized users from accessing the InterTech mainframes. We agree that responsibility belongs to InterTech. We also agree that we need to be aware that there is a possibility of breach from the outside and we should identify ways to prevent and monitor the access of the SEMA4 database from such unauthorized users.

OLA Finding 1: The Departments of Employee Relations and Finance do not have effective security administration procedures to protect the SEMA4 database.
We agree that we lack sufficient written procedures and policies in the security of the SEMA4 database. The implementation contractor for SEMA4 developed the security methods and procedures. Details of this were passed on to state employees, mostly verbally. Staff from Finance and Employee Relations have worked with staff from InterTech to keep the system operational using this knowledge. We agree that further documentation of security policies and procedures will provide better management of security. We agree that no one person from the state fully understands all aspects of the security for SEMA4. We have already begun to implement some changes and plan to complete all of the recommendations for this finding by March 31, 1999.

200 Centennial Office Building • 658 Cedar St. • St. Paul, MN 55155-1603 • (612) 297-1184 • TTY (612) 282-2699

2. OLA Finding 2: Some users have inappropriate security clearances to the SEMA4 database.
We agree that permitting 45 users to modify the SEMA4 database using tools outside of SEMA4 is too many. We will complete the OLA recommendation by January 15, 1999 to review these security clearances. We have already begun to reduce the number of users.

3. OLA Finding 3: The departments do not monitor some high-risk security events.
We agree that we have a security exposure that is not being totally monitored. We have already begun substantially reducing the number of users who have this capability and to step up our procedures for reviewing DB2 security events on a regular basis. We will complete the OLA recommendations for this finding by February 15, 1999.

4. OLA Finding 4: The departments are not taking sufficient steps to protect the passwords of some user accounts.
Our exit conference clarified our mutual understanding of the limitations of the current version of SEMA4 based on PeopleSoft's security design. We have already taken steps to encrypt passwords within SEMA4. Further steps will be taken to address safekeeping of the electronic and paper password files. We will search for other solutions that give added protection to password confidentiality. We will complete the OLA recommendations for this finding by May 1, 1999.

In conclusion, we again wish to thank you for identifying these weaknesses and bringing them to our attention with your recommendations. While it appears that our exposure to harm was limited to a relatively small number of trusted employees, we do need to close those gaps. In the months ahead, we will work toward implementing your recommendations and will keep you apprised of our progress. Any questions or concerns you have in regards to this response should be directed to Chris Goodwill, Employee Relations, at 296-7956.

Copy:
Chris Goodwill, Senior Administrative Officer, Department of Employee Relations
Steve Jorgenson, Chief Information Officer, Department of Employee Relations
Michael Ladd, Chief Information Officer, Department of Finance