

Diebold Security Analysis of ATM Operating and Application Systems Using the Center for Internet Security Scoring Tool

Section 1: Introduction

Document Purpose

The purpose of this document is to explain and compare the Diebold-supplied Microsoft® Windows® XP Professional SP1 1.1.0.7 hardened operating system to an accepted consensus baseline for a high security desktop computer using the Microsoft Windows XP Professional operating system. The baseline we have selected for this comparison is provided by the Center for Internet Security (CIS) and is identified as the CIS XP Pro Specialized Security / Limited Functionality template named CIS-WinXP-SpecSec-v1.3.inf.

Diebold Membership

Diebold is a member of the Center for Internet Security.

White Paper

This document serves as a white paper and was prepared by:

Joseph A. McGinley, CISSP, CISM, CCSE Manager, Self Service Applications and Network Security, Diebold Global Software Development

1.1 Definitions

This section provides definitions and additional information about the following topics discussed in the remainder of this document: the Center for Internet Security, the CIS Scoring Tool, the CIS-supplied security template, and the hardened operating system.

Center for Internet Security

The Center for Internet Security is a not-for-profit cooperative organization assisting network users and operators, and their insurers and auditors, to reduce the risk of significant disruptions of electronic commerce and business operations due to technical failures or deliberate attacks.

The mission of the Center for Internet Security is to help organizations around the world effectively manage the risks related to information security. CIS provides methods and tools to improve, measure, monitor, and compare the security status of Internet-connected systems and appliances. Refer to the following Website for additional information about the Center for Internet Security.

<http://cisecurity.org/>

CIS Scoring Tool

CIS licenses the use of a Scoring Tool that measures the security of a target computer's operating system against an established standard for security. The established standard is defined in a security template file. The CIS Scoring Tool compares the target system's configuration against the security standards set in the security template file and provides a security score by which the target system can be evaluated.

CONTENTS

Section 1: Introduction	1
1.1 Definitions	1
1.2 DieboldSecurityObjectives	2
1.3 DieboldHardeningProcess	2
1.4 DieboldSecurityTemplate –Diebold_SST	3
1.5 AnalyzingPreviouslyDeployedSystems	3
Section 2: Sample CIS Scoring Reports	3
2.1 CIS Scan of Laptop	4
2.2 CIS Scan of a Hardened ATM using the Diebold_SST.inf Template	4
2.3 CIS Scan of a Hardened ATM using the Consensus CIS Baseline Template	4
Section 3: Conclusion	6

Specialized Security – Limited Functionality Template

CIS provides this template, formerly known as the High Security template. Settings in this level are designed for XP Professional systems in which security and integrity are the highest priorities. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

Hardened Operating System

A hardened operating system is an operating system from which all nonessential services have been removed. The result is an operating system that is easier to lock down and manage than an operating system intended for general use.

1.2 Diebold Security Objectives

The objectives for securing the Diebold-supplied Microsoft Windows XP Professional operating system are as follows:

- To create a secure hardened operating system for use with Diebold ATM applications.
 - The target operating system is the Diebold-supplied, OEM-based, Microsoft Windows XP Professional operating system. A deny all approach will be followed to minimize vulnerabilities in the operating system.
 - The target security level is as specified in the CIS XP Pro Specialized Security / Limited Functionality template (CIS-WinXP-SpecSec-v1.3.inf) supplied by CIS.
- To provide an industry standard methodology, using recognized and accepted industry tools to implement Diebold's securing process.
- To provide a point of reference, a baseline, to measure improvements.

1.3 Diebold Hardening Process

This section provides an overview of the hardening process that Diebold performs on the operating system and ATM application software.

Operating System

The Diebold-supplied Microsoft Windows XP Professional operating system release has

been developed with a "Secured by Default" security approach, including the following precautions:

- All components and services identified as not necessary for the functioning of the ATM systems are removed.
- All TCP and UDP ports are closed by default in the delivered system.
- Additionally, the Sygate® firewall is installed and configured with a rule set which denies all access to and from the ATM. A rule must then be activated to allow communication to the host server. This rule should be limited to a specific IP address, port, and application.

To insure that a secure base is created, the CIS Scoring Tool from the Center for Internet Security is used together with the CIS-provided XP Pro Specialized Security / Limited Functionality template. The exact template used is the CIS-WinXP-SpecSec-v1.3.inf template. Settings at this level are designed for Windows XP Professional operating systems in which security and integrity are the highest priorities. The goal of the hardening effort is to come as close to this high security baseline as is possible and still have a functioning ATM. Each setting has been considered carefully and only applied after a thorough analysis and a level of understanding attained with regard to the potential impact of that setting or action in the Diebold ATM environment.

ATM Application Software

After the operating system is built and hardened to the level deemed necessary for a secure but functioning Diebold ATM, the Agilis® 91x for Opteva®, Version 1.3.0.0 application software is installed. At this time, the ATM is ready for scanning with the CIS Scoring Tool.

CIS Scoring Tool

The CIS Scoring Tool is used to evaluate the ATM against the baseline CIS-WinXP-SpecSec-v1.3.inf template. The score from this scan is 6.9 out of 10.0. This score is an indication of differences or mismatches within the operating system as compared to the baseline template. Although mismatches are the only criteria in the determination of the score, they do not necessarily indicate a lesser security setting. In many cases, the security setting for the ATM was in fact set higher than the CIS recommended setting.

To help clarify and provide greater perspective into the significance of CIS Scoring Tool, several sample scan reports are presented in Section 2.

1.4 Diebold Security Template – Diebold_SST

Diebold has created a security template file named Diebold_SST.inf specifically for use in hardening the Diebold-supplied Microsoft Windows XP Professional operating systems used in ATMs manufactured by Diebold. The template is divided into the following sections, each of which addresses a specific area of security:

- Account Policy: password requirement parameters
- Local Policies: audit policy, user rights, and other optional security settings
- Event Logs: log file sizes and retention methods/periods
- Restricted Groups: power users and administrators
- File System: critical system file and utility system permissions
- Registry: permissions on registry keys and optional values

This Diebold security template is the end result of extensive evaluation and testing of the recommended security settings as posted in the baseline CIS XP Pro Specialized Security/Limited Functionality template (CIS-WinXP-SpecSec-v1.3.inf) and then modified to produce a functioning ATM.

1.5 Analyzing Previously Deployed Systems

The CIS Scoring Tool has another useful but different function that can be utilized by Diebold field support representatives to analyze previously deployed systems. Suppose the CIS Scoring Tool is used with the Diebold_SST.inf template in an analysis against a system hardened to that template level. The resulting score logically should be 10.0 out of 10.0, with no mismatches listed.

So, if a field support representative runs the CIS Scoring tool against a deployed system and a score of less than 10.0 results, it is a good indication that the system security has been modified after release from the factory.

This modification may be by design, in which case the mismatch is explained. However, knowing the exact modifications could potentially assist in the investigation of system problems. If a parameter has changed and the behavior of the system is not as desired, it may be a good indication that the altered security parameter might have affected the system in an adverse way.

The CIS Scoring Tool could also be used to monitor a system and provide early feedback of system security changes. When used to monitor system security changes, the CIS Scoring Tool functions in a manner similar to an assignment tool and can be integrated into a company's change management process.

Refer to Section 2.2 for a sample scan report analyzing a previously deployed ATM.

Section 2: Sample CIS Scoring Reports

This section presents three sample CIS scoring reports. Report particulars are described the following paragraphs:

Diebold Laptop

A Diebold provided and supported laptop system with Microsoft Windows XP Professional is scanned against the CIS XP Pro Specialized Security/Limited Functionality template (CIS-WinXP-SpecSec-v1.3.inf). This sample report illustrates how system mismatches impact the reported score. Refer to Section 2.1 for this sample report.

Diebold Field Deployed ATM

A Diebold field deployed ATM system is scanned against a custom security template (Diebold_SST.inf). This custom template has been developed specifically for use in the hardening of the field deployed platform. This sample report illustrates another valuable use for the CIS Scoring Tool. Refer to Section 2.2 for this sample report.

Agilis 91x for Opteva, Version 1.3.0.x

An ATM running Agilis 91x for Opteva, Version 1.3.0.x with the hardened, Diebold-supplied Microsoft Windows® XP Professional operating system is scanned against the CIS XP Pro Specialized Security/Limited Functionality template (CIS-WinXP-SpecSec-v1.3.inf). Refer to Section 2.3 for this sample report. Detailed explanations of deviations between this Diebold hardened system and the CIS baseline are also provided in Section 2.3.

2.1 CIS Scan of Laptop

See Figure 2-1 for a sample report from a scan of a slightly hardened XP Pro laptop system:

As you can see from the results, the only positive scores received in this example were because the services pack level was at SP1. The remaining categories each received a score of zero even though there was some to significant agreement in the setting for the category. For example, the services provided a

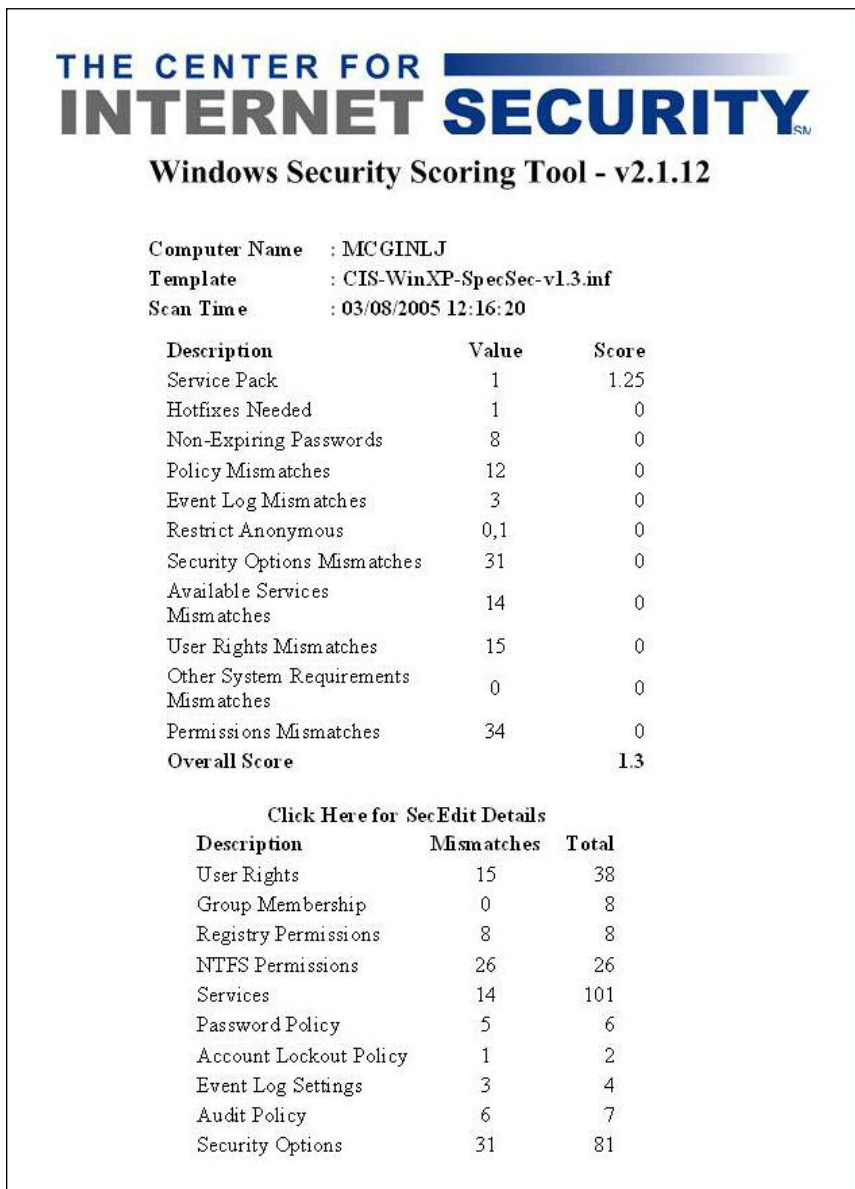


Figure 2-1

score of zero even though only 14 of the 101 identified services were not in agreement with the baseline template.

In this example, an audit of the laptop revealed a score of 1.3 out of 10.0. What is the significance of this score? In reality, only a

complete analysis can determine this. Again, this score is only an indication of mismatches between the laptop security settings and those suggested by the Center for Internet Security for a Specialized Security / Limited Functionality desktop Microsoft XP Pro operating system. A perfect score is 10.0 but, as explained above, slight deviations in each category reduce the overall score significantly.

For additional information on the benchmark, refer to the *Windows XP Professional Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings, Version 1.3, October 20, 2004*. This document is available at the CIS Web site (www.cisecurity.org).

2.2 CIS Scan of a Hardened ATM using the Diebold_SST.inf Template

See Figure 2-2 (next page) for a sample report that provides an analysis of the Diebold-supplied Microsoft Windows XP Professional operating system hardened with the Diebold_SST.inf template and analyzed against the Diebold_SST.inf template. See Section 1.4 for more information on the Diebold_SST.inf template.

As expected, the score is 10.0 out of 10.0 with absolutely no mismatches. If in the field in a post installation analysis the score is less than 10.0 out of 10.0, the exact area of change (a mismatch) will be clearly visible and could provide a first area for investigation in resolving a problem.

This scan can also be run periodically to provide assurance to the institution that security settings are as expected. See Section 1.5 for more information.

2.3 CIS Scan of a Hardened ATM using the Consensus CIS Baseline Template

See Figure 2-3 (next page) for a sample report that provides an analysis of an ATM running Agilis 91x for Opteva, Version 1.3.0.x with the hardened, Diebold-supplied Microsoft Windows® XP Professional operating system is scanned against the CIS XP Pro Specialized Security / Limited Functionality template (CIS-WinXP-SpecSec-v1.3.inf). Detailed explanations of deviations between this Diebold hardened system and the CIS baseline are provided.

As shown in Figure 2-3, the score is 6.9 out of

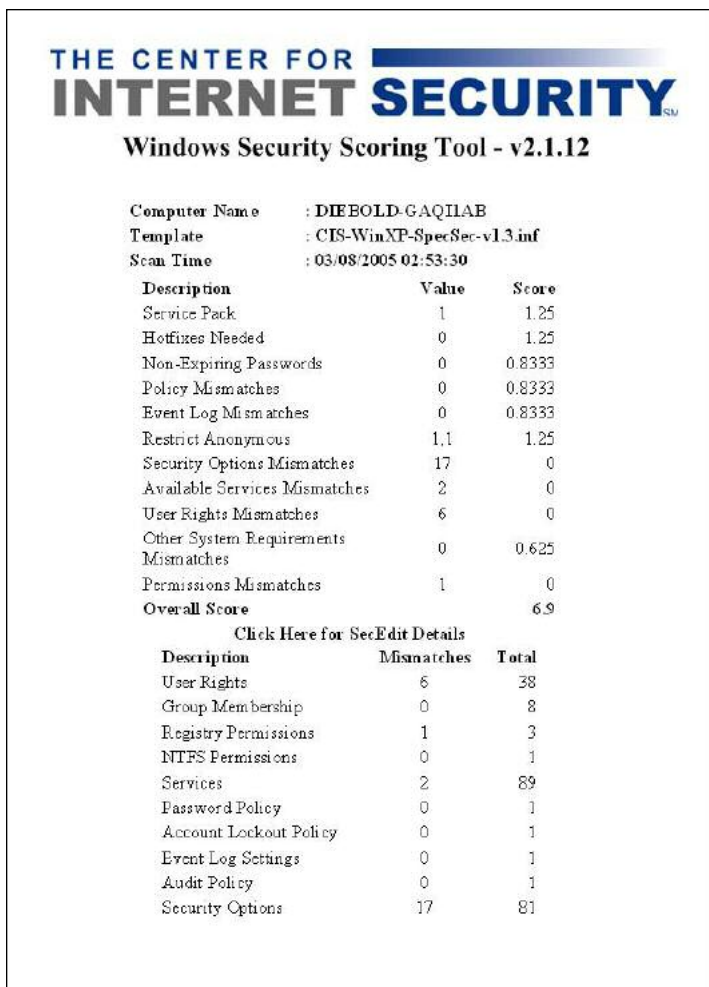


Figure 2-2 CIS Scan of a Hardened ATM using the Diebold_SST.inf Template

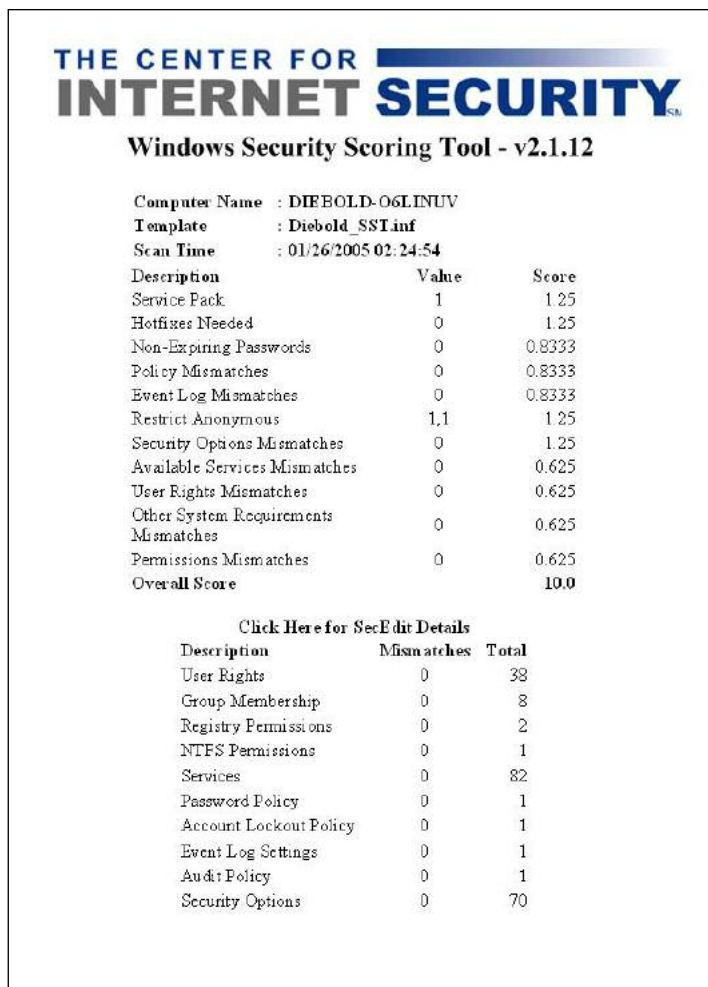


Figure 2-3 Diebold Hardened System against a Consensus CIS Baseline Template

10.0. A score of 10.0 out of 10.0 is not possible for a deployed and functional ATM. The full analysis shows that the areas described in the following paragraphs reduced the overall score, but not necessarily the security of the platform.

Security Options:

(17 mismatches out of 81 settings.)

The deviations are required for the unique ATM environment. The specific differences are as follows:

- 1. Accounts: Administrator account status**
In a deployed Diebold system, the "Administrator" user account is a decoy with no rights and no group association but a complex password.
- 2. Audit: Shut down system immediately if unable to log security audits.** If this set-

ting was enabled as recommended in the baseline on an ATM it could permit a DOS attack.

- 3. Devices: Restrict CD-ROM access to locally logged-on user only.** Although restricting this functionality is desirable, it is required for Microsoft installer to function. Diebold uses Microsoft installer to install software packages.
- 4. Devices: Unsigned driver installation behavior.** "Silently install" required for ATM silent driver installations.
- 5. Domain member: Maximum machine account password age.** Most ATMs are non-domain members.
- 6. Interactive logon: Message text for users attempting to log on.** Diebold_ATM user is an auto logon. No other user level interactive users.

7. **Interactive logon: Message title for users attempting to log on Warning!** Diebold_ATM user is an auto logon. No other user level interactive users.
8. **Interactive logon: Smart card removal behavior.** Smart cards are not currently implemented for maintenance access. User is auto logon.
9. **Microsoft network client: Digitally sign communications (always).** If Windows 2000 or greater domain, then the setting can be "always"; else, breaks communications in mixed environments with NT systems.
10. **Microsoft network server: Digitally sign communications (always).** If Windows 2000 or greater domain, then the setting can be "always"; else, breaks communications in mixed environments with NT systems.
11. **Microsoft network server: Disconnect clients when logon hours expire.** Only client is the Diebold_ATM application user, which MUST not be disconnected.
12. **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients.** Does not apply to an ATM.
13. **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers.** Does not apply to an ATM.
14. **Network security: Force logoff when logon hours expire.** Under investigation. However, no remote users are currently allowed or configured.
15. **Network security: LDAP client signing requirements.** LDAP not enabled.
16. **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.** Microsoft bug – broken in XP Pro SP1. Will not allow Internet Windows Activation or Window Updates.
17. **Network Access: Named pipes that can be accessed anonymously.** Named Pipes are communications channels between two processes.

Services:

(2 mismatches out of 89)

1. IIS Admin
2. World Wide Web Publishing

NOTE: IIS Admin and World Wide Web Publishing are installed as parts of IIS. In a Diebold system, IIS is locked down to loop-back only. IIS is required for configuration of the Agilis 91x software.

There are many additional services not scored by the CIS Scoring Tool that have been removed or disabled in the Diebold platform. So again, Diebold presents a more secure ATM specific computing platform.

User Rights:

(6 mismatches out of 38)

These mismatches occur because of the default IIS users IUSR_MachineName and IWAM_MachineName installed by IIS and required for Agilis configuration.

On the positive side, IUSR_MachineName and IWAM_MachineName users are configured with IIS application generated 14 character complex non-expiring passwords. IIS is further locked down with component removals and communication only on loopback.

In new releases of the Agilis product, IIS is an optional component. In those releases, IIS is only required if the customer plans to serve ASP web pages locally for consumer screens. In the past, IIS was required for MMC snap-ins used in the configuration of the ATM application. This software has been replaced by .NET GUI applications. IIS will be removed completely as a required component for Diebold developed applications.

Permissions (NTFS File and Registry):

One mismatch, however this is very misleading. Actually, there are thousands of files and registries locked down that are too numerous to list.

Diebold restricted access to many files for the Diebold_ATM user and, therefore, experienced mismatches in most areas. Again, these mismatches do not lessen the security of the system, but actually enhance it. The score only identifies mismatches and is not meant to indicate the security posture of a specific system. The score indicates compliance with a consensus template for a generic Windows XP Professional-based desktop system.

Section 3: Conclusion

Having a benchmark score against an accepted and recognized baseline enables customers to assess the Diebold solution and make informed decisions on this or other examined platforms. However, an understanding of the score and identification of deviations and reasons for deviations is critical. Hopefully, this paper has provided insight into the usage and meaning of the CIS Scoring Tool scores and Diebold's actual score.

As shown in Section 2.3, the Diebold-supplied Microsoft Windows XP Professional SP1 1.1.0.7 hardened operating system measures up to the consensus standards as established by the CIS membership. The Center for Internet Security is in the process of modifying their CIS scan scoring tool. The modifications will, hopefully, use weighted values in each category. This will greatly enhance the Diebold score and give a more accurate rating on the level of security compared to the consensus baseline.

Document History

Document No.	Date	Remarks
TP-821129-001A	3/2005	Original edition
TP-821129-001B	4/2005	Change disclaimer page and Section 3

Copyright protection is claimed for each revision listed in the document history, as of the date indicated.

Any trademarks, service marks, product names or company names not owned by Diebold, Incorporated or its subsidiaries (collectively "Diebold") that appear in this document are used for informational purposes only and Diebold claims no rights thereto, nor does such use indicate any affiliation with or any endorsement of Diebold or Diebold products by the owners thereof.

The information contained in this document is subject to change without notice. When using the document for system implementation, please call your authorized sales or service representative for any applicable changes.

This document and the information contained herein are provided AS IS AND WITHOUT WARRANTY. In no event shall the copyright owner or its suppliers be liable for any special, indirect, or consequential damages of any nature resulting from the use of information in this manual.

This document may be reproduced by electronic, mechanical, or photocopying means, provided the document is reproduced in its entirety, with all copyright and other proprietary notices intact.

Your use of this document and/or any of the information contained herein constitutes your agreement to all of the terms stated on this page.

Diebold, Incorporated
Post Office Box 3077
Dept. 9-B-16
North Canton, Ohio
44720-8077

800.999.3600 USA
330.490.4000 International
e-mail:
productinfo@diebold.com
www.diebold.com



We won't rest.