

Document Defense Tactics

Gini Courter and Annette Marquis, TRIAD Consulting

Session #400 Tuesday, July 19, 2005 1:00 pm to 3:00 pm

It's all about security these days. How do you make sure a final document doesn't get changed by someone else? How do you safeguard a document from someone not authorized to access it? How do you keep confidential material confidential? How can you be sure an email message is from who it says it is from? All of these questions are critical to today's electronic workplace. In this session, we'll explore various document defense tactics, including password-protecting documents, adding digital signatures, and choosing secure document formats. Learn how to protect yourself and your organization by keeping your documents secure from prying eyes and devious minds.

Why worry?

According to the 2004 CSI/FBI Computer Crime and Security Survey, "unauthorized use of computer systems is on the decline, as is the reported dollar amount of annual financial losses resulting from security breaches. In a shift from previous years, both virus attacks and denial of service outpaced the former top cost, theft of proprietary information."ⁱ

Although theft of proprietary information might be down, the numbers are still staggering – over 600,000 laptops were stolen in 2003 with an average loss per laptop of \$61,881. That includes the cost of the hardware and software but more importantly the loss of information on the laptop. Add to this, the risk of losing confidential information through snooping, hacking, and other means, it's never been more important for businesses and organizations to implement document protection policies and practices.

In the news

Two recent examples in the news show how easy it is to distribute insecure documents:

Hidden text shows SCO prepped lawsuit against BofAⁱⁱ

"A Word document in SCO's lawsuit against DaimlerChrysler originally identified Bank of America as the defendant. Hidden text indicates that SCO spent considerable time building a case against the bank. As some have learned the hard way, Word can also display the original version of a document and all subsequent changes."

Secrets leaked as software confounds the censorsⁱⁱⁱ

"Just a few clicks were enough to reveal names, training procedures, and other secrets the US military thought it had blacked out.

The leak resulted from a type of mistake that is becoming increasingly common as government agencies and corporations scrap paper for online distribution.

The US military command in Baghdad produced the report in Adobe Systems Inc.'s popular Portable Document Format and posted it Saturday. Its investigation cleared US soldiers of wrongdoing in the shooting of an Italian agent. The blacked-out portions included names of soldiers at Iraqi checkpoints, checkpoint procedures, and general security information.

John Landwehr, Adobe's director of security, examined the document and suggested censors "simply put black rectangles over the text and did not delete any of the text itself from the documents. They were trying to do redaction with something not designed to do redaction." By simply opening the document, hitting the "select text" button, copying and then pasting all the text into any word processor, readers could see what was buried beneath.

The military admits it goofed."

New regulatory requirements

In addition to increasing internal pressure to protect against these and other similar kinds of security mistakes, many companies are directly or indirectly affected by government mandates and regulations for providing consumer privacy. These include:

- Health Insurance Portability and Accountability Act (HIPAA)—Protection for health-related data
- Gramm-Leach-Bliley Act—Financial privacy
- European Union Directive on Privacy and Electronic Communications
- Privacy Acts of Japan and Australia
- California SB 1368—Privacy notification
- California AB 1950—Protection of customer data

And then there is SOX^{iv}

Sarbanes-Oxley is a US law passed in 2002 to strengthen corporate governance and restore investor confidence. The act was sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley.

- **Sarbanes-Oxley** law passed in response to a number of major corporate and accounting scandals involving prominent companies in the United States. These scandals resulted in a loss of public trust in accounting and reporting practices.
- Legislation is wide ranging and establishes new or enhanced standards for all US public company Boards, Management, and public accounting firms.
- **Sarbanes-Oxley** law contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties. It requires the Security and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

What does Sarbanes Oxley Address?

- Establishes new standards for Corporate Boards and Audit Committees
- Establishes new accountability standards and criminal penalties for Corporate Management
- Establishes new independence standards for External Auditors
- Establishes a Public Company Accounting Oversight Board (PCAOB) under the Security and Exchange Commission (SEC) to oversee public accounting firms and issue accounting standards

According to the 2004 CSI/FBI Computer Crime and Security Survey^v, the respondents in the financial, utility and telecommunications sectors believe the Sarbanes-Oxley Act is already having an impact on their organizations' information security. It's too soon to tell for other industries but the general feeling is that it will eventually impact information security in all major industries.

What does it mean to be secure?

According to Adobe^{vi}, six criteria must be met in order to provide more effective protection for an electronic document throughout its lifecycle:

1. Confidentiality—Who should have access to the document?
2. Authorization—What permissions does the user have for working with the document?
3. Accountability—What has the recipient done with the document?
4. Integrity—How do you know if the document has been altered?
5. Authenticity—How do you know where the document came from?
6. Non-repudiation—Can the signatory deny signing the document?

To meet these six criteria, electronic document protection is obtained through the use of network passwords, file and document permissions, document passwords, and digital certificates.

Document Security in Microsoft Office

Microsoft Office 2003 offers four methods for securing documents:

- Password-protecting entire documents so they can't be changed
- Restricting permissions to specific parts of documents
- Using Information Rights Manager to restrict who can access documents and what they can do with them
- Adding digital signatures to documents to authenticate origination

Password-protecting Office documents

Whenever you need to create a password, create a strong password that combines upper- and lowercase letters, numbers, and symbols. An example of a strong password is: aheLp!2mE. A weak password is a simple word or phrase, such as: helpme. Do not use your dog, spouse, or children's name, your school, or any other identifiable word or phrase! Devise a strong password that you can remember so that you don't have to write it down. To secure a Microsoft Office document with a password:

1. Open the file.
2. On the **Tools** menu, click **Options**, and then click **Security**.
3. Do one of the following:

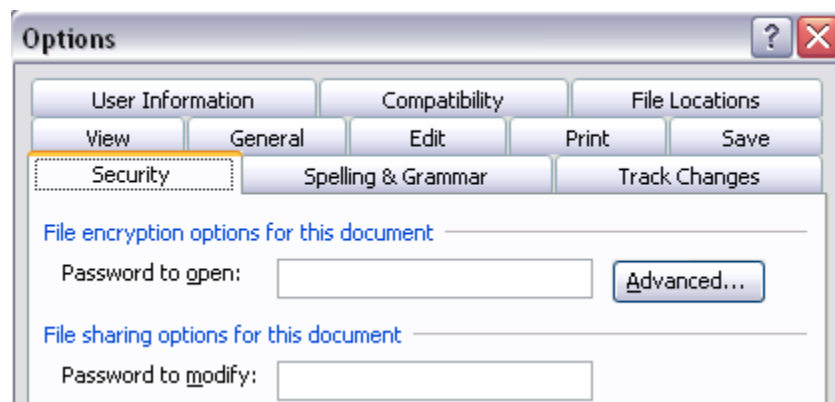
Create a password to open

1. In the **Password to open** box, type a password, and then click **OK**.
2. In the **Reenter password to open** box, type the password again, and then click **OK**.

Create a password to modify

1. In the **Password to modify** box, type a password, and then click **OK**.
2. In the **Reenter password to modify** box, type the password again, and then click **OK**.

Tip: To create a long password— up to 255 characters— click **Advanced**, and select an RC4 encryption type.



Restriction permissions to parts of Office documents

Protection in Word

Using the new document protection features in Word 2003, you can restrict others from changing formatting and from editing specific parts of a document. To apply document protection, follow these steps:

1. Click **Tools** > **Protect Document** from the Word menu.
2. To limit formatting, click the **Limit Formatting to a Selection of Styles** checkbox, and then click **Settings**.
 - a. In the Settings dialog box, select the styles you want to allow in the document.
 - b. For a recommend minimum number of styles, click **Recommended Minimum**.
 - c. Click **OK** to save your selection.
3. To apply editing restrictions,

- a. Click the Allow Only This Type of Editing in the Document checkbox.
 - b. Select which type of editing you want to allow from the drop-down list:
 - i. No changes (Read Only)
 - ii. Tracked Changes
 - iii. Fill-in Forms
 - iv. Comments
 - c. Set any exceptions by selecting parts of the document and then, choosing users who can freely edit them.
 - i. Hold CTRL while you select to select parts of the document.
 - ii. Click More Users on the Protect Document task pane.
 - iii. Enter the users' names, separated by semi-columns.
 - iv. Click OK.
4. When you are ready to enforce protection, click Yes, Start Enforcing Protection on the Protect Document task pane.

Protection in Excel

In Excel, you can protect all or part of a worksheet and entire workbooks. To protect parts of a worksheet, follow these steps:

1. Click Tools ➤ Protection.
2. Click Protect Sheet.
3. Enter a password, which you would enter to unprotect the sheet.
4. Select the actions you would like users to be able to take in the worksheet. Clear the checkboxes of actions you want to restrict.
5. Click OK.

Unlocking cells

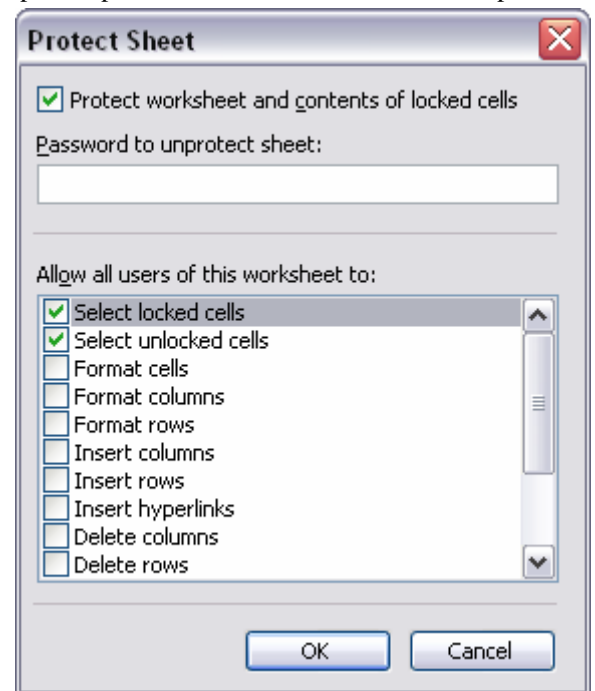
By default, all cells in a worksheet are locked, but until you activate worksheet protection, they are not restricted. To unlock cells you want users to be able to use,

1. Select the cells you want to unlock.
2. Click Format ➤ Cells.
3. Clear the Lock Cells checkbox on the Protection tab.
4. Repeat this process for additional cells you want to unlock.

Protecting Workbooks

To protect an entire workbook,

1. Click Tools ➤ Protection ➤ Protect Workbook.
2. Select Structure to protect the workbook so that worksheets in the workbook can't be moved, deleted, hidden, unhidden, or renamed, and new worksheets can't be inserted.
3. Select Window if you want to assure that Windows are the same size and position each time the workbook is opened.
4. Enter a password to prevent others from removing workbook protection.
5. Click OK.
6. When prompted, re-enter the password and then, click OK.



About Microsoft Information Rights Manager^{vii}

[The following description of the Microsoft Information Rights Manager is from Microsoft.com.]

Information Rights Management (IRM) in Microsoft Office 2003 is a new feature that allows individual authors to specify permission for who can access and use documents or e-mail messages, and helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people. Once permission for a document or message has been restricted with this technology, the access and usage restrictions are enforced no matter where the information is, since the permission to access an e-mail message or a document is stored in the file itself.

IRM in Office 2003 helps corporations and knowledge workers address two fundamental needs:

- **Restricted permission for sensitive information.** Most corporations today rely on firewalls, log-in security, and other network technologies to protect their sensitive intellectual property. The fundamental limitation of these technologies is that, once legitimate users have access to the information, they can share it with unauthorized people, potentially breaching security policies. IRM helps prevent the sensitive information itself from unauthorized access and reuse.
- **Information privacy, control, and integrity.** Information workers often deal with confidential or sensitive information, relying on the discretion of others to keep sensitive materials in-house. IRM eliminates the temptation to forward, copy, or print confidential information by disabling those functions in documents and messages with restricted permission.

IRM in Outlook 2003

IRM can be used in Outlook 2003 to help prevent messages from being forwarded, printed, or copied. Messages with restricted permission are automatically encrypted before they are sent. An Office 2003 document attached to a message with restricted permission is automatically restricted unless permission is already restricted for the attached document, in which case the attachment retains its existing permission.

IRM in Word 2003, Excel 2003, and PowerPoint 2003

Permission for Office 2003 documents can be restricted on a per-user or per-group basis (group-based permissions require Active Directory for group expansion). Each user or group can be given a set of permissions according to the access levels defined by document authors: Read, Change, or Full Control. Document authors have Full Control access. Just like document authors, those with Full Control access can select to restrict printing, set expiration dates, and even give permission to others or change permission for existing users. Once permission for a document has expired for authorized users, the document can only be opened by the document author or users with Full Control access to the document.

If a document with restricted permission is forwarded to an unauthorized person, a message appears with the document author's e-mail address so that the individual can request permission for the document. If the document author chooses not to include an e-mail address, unauthorized users simply get an error message.

Windows Rights Management client

To take advantage of this new technology, you must first install the Windows Rights Management client. You will need administrative rights to install this client on your computer and ensure it functions properly.

Rights Management Add-on for Internet Explorer

Because permissions are granted in an Office 2003 program, Office 2003 documents with restricted permission can only be opened by Office 2003. However, the [Rights Management Add-on for Internet Explorer](#) allows authorized people without Office 2003 to read content with restricted permission.

Additional server requirements for IRM

Microsoft Windows Server 2003 with Windows Rights Management Services is required to enable IRM in Office 2003. Microsoft also hosts a [free trial IRM service](#) for customers who do not have Windows Server 2003. This service will enable users to share documents and messages with restricted permission using Microsoft .NET Passport as the authentication mechanism, as opposed to Active Directory.

Other Office 2003 privacy options

To access additional privacy options in Office 2003, click Tools ➤ Options and review these options on the Security tab:

- **Remove personal information from this file on save.** Helps you to avoid unintentionally distributing hidden information, such as the document's author or the names associated with comments or tracked changes.
- **Warn before printing, saving, or sending a file that contains tracked changes or comments (Word only).** Prompts you to review tracked changes or comments before saving or distributing a document. Do this to minimize your risk of accidentally sharing private information.
- **Store random numbers to improve merge accuracy (Word only).** Instructs Word to use randomly generated numbers to help keep track of related documents for comparing and merging. Although these numbers are hidden, they could potentially be used to demonstrate that two documents are related. If you choose not to store these numbers, the results of merged documents will be less than optimal.
- **Make hidden markup visible when opening or saving (Word only).** Displays all comments, annotations, deletions, and other types of revisions. If you use the **Show** menu on the **Reviewing** toolbar to hide some or all of your revisions, and you select this option, your revisions will appear when you or another user opens the file. This option does not affect text formatted as hidden.

Adding digital signatures

Digital signatures are legally-binding electronic credentials. Before you can apply a digital signature to a document, you must obtain a digital certificate, an encrypted key that verifies that the originator of a document or message is who they say they are. You can obtain a digital certificate from a commercial certification authority, such as [VeriSign, Inc.](#) or [GeoTrust](#), or from your internal security administrator. This is not an immediate process – you have to complete a number of steps to verify your identity including submitting notarized documents – so plan ahead if you need a digital certificate.

After you have a verified digital certificate, you can apply your electronic signature to an Office document by following these simple steps:

1. On the Tools menu, click Options, and then click the Security tab.
2. Click Digital Signatures.
3. Click Add.
4. Select the certificate you want to add, and then click OK.

Protection on Adobe PDF documents

PDF (Portable Document Format) documents have a history of being considered more secure than word-processing documents because even without specific document protection, they cannot easily be changed. However, even for PDF documents to be truly secure, you must apply protection features, such as passwords and digital signatures.

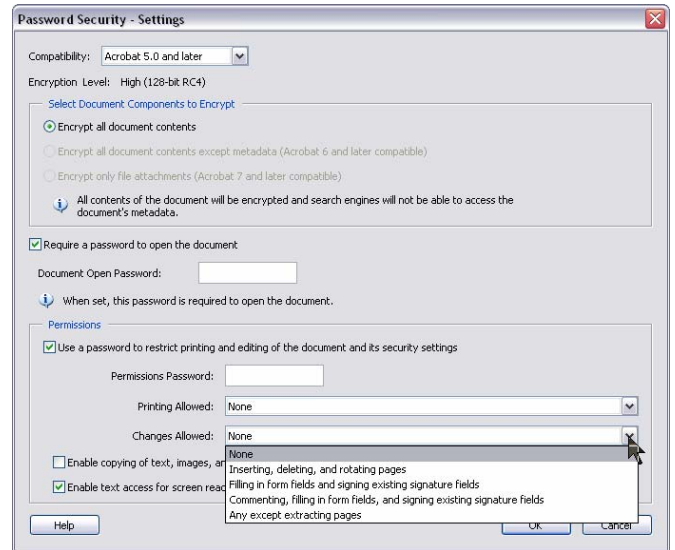
To apply passwords to an Adobe document, follow these steps:

1. Click File ➤ Document Properties and then, click the Security tab.
2. Select Password Security from the Security Method drop-down list.
3. Select the Require a Password to Open the Document checkbox.
4. Enter a password in the Document Open Password text box.
5. To restrict printing and making changes to the document, select the Use a Password to Restrict Printing and Editing of the Document and its Security Settings.
 - a. Enter a password in the Permissions Password text box.
 - b. Select None, Low Resolution, or High Resolution from the Printing Allowed drop-down list.

- c. Select from the following Changes Allowed options:
 - i. Inserting, deleting and rotating pages
 - ii. Filling in form fields and signing existing signature fields
 - iii. Commenting, filling in form fields, and signing existing signature fields
 - iv. Any except extracting pages
6. Click OK to apply the security settings.

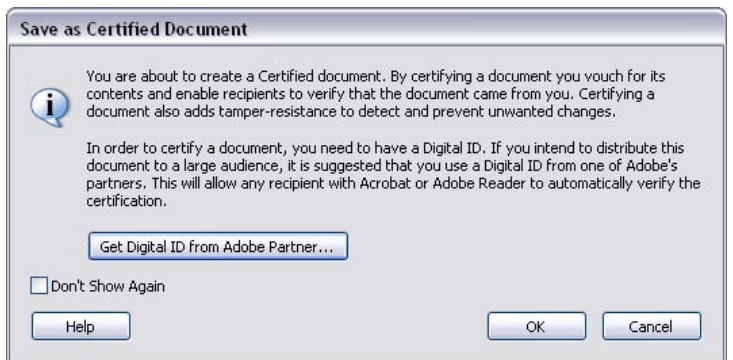
Digitally certifying a document

When you create a PDF document in Adobe Acrobat, you can apply a certifying signature to the document rather than a regular digital signature. If unauthorized changes are made to a certified document, the certifying signature is invalidated, relieving the original signer from responsibility. To certify a document,



1. Click the Sign button on the Adobe Acrobat toolbar and select Sign This Document.
2. Click Certify Document.
3. Assuming you already have a digital certificate, click OK.
4. Select the Allowed Actions:
 - a. Disallow any changes to this document.
 - b. Only allow form fill-in actions on this document.
 - c. Only allow commenting and form fill-in actions on this document.
5. Click OK.
6. Choose if you would like to display the digital certificate on the document or not. Click OK.
 - a. If you choose to display it, click OK again.
 - b. Drag an area on the document where you would like the certificate to display.
7. Select the digital ID you would like to use from the My Digital IDs list.
8. Click OK.
9. Select the Reason you are signing this document from the list of available choices.
10. Click Sign and Save As or Sign and Save to save the document.

Adobe saves the document and if you chose to display the signature, it applies a signature stamp like the one shown here, to the document.



Annette S.
Marquis

Digitally signed by Annette S.
Marquis
DN: cn=Annette S. Marquis
Date: 2005.05.19 19:07:40 -04'00'

The next generation of security

Over the next few years, digital signatures and other document protection tools will become much more commonplace. Fingerprint and other biometric security methods are already being used by 10% of companies. Although many of the methods of security discussed in this article will be replaced with tighter security measures in years to come, they provide a important level of security that should not be ignored. Anything and everything you can do to prevent unauthorized access to and/or revision of your organization's documents, is time and effort well spent in the long run.

ENDNOTES

- ⁱ Gordon, Lawrence A. et al. 2004 CSI/FBI Computer Crime and Security Survey. 2004 by Computer Security Institute. page 2. Available http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
- ⁱⁱ "Hidden text shows SCO prepped lawsuit against BofA", Published: March 4, 2004, 12:25 PM PST C/Net News.com. Available http://news.com.com/Hidden+text+shows+SCO+prepped+lawsuit+against+BofA/2100-7344_3-5170073.html?tag=nl
- ⁱⁱⁱ Kotidia, Munir. "U.S. military security defeated by copy and paste." C|Net May 4, 2005. Available http://news.com.com/U.S.+military+security+defeated+by+copy+and+paste/2100-1002_3-5694982.html
- ^{iv} "SixSigma Tutorial." <http://sixsigmatutorial.com/SOX/sarbanes-oxley.aspx?ref=aw>
- ^v Gordon, Lawrence A. et al. 2004 CSI/FBI Computer Crime and Security Survey. 2004 by Computer Security Institute. p.16. Available http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
- ^{vi} Adobe Technical White Paper. "A Primer on Electronic Document Security." p. 4. Available http://www.adobe.com/security/pdfs/acrobat_security_wp.pdf.
- ^{vii} Microsoft Corporation. "Introducing Information Rights Management." Available <http://office.microsoft.com/en-us/assistance/HA010397891033.aspx>.

For materials and links from this session, visit our web site
www.triadconsulting.com/events/iaap.htm



© 2005 TRIAD Consulting, LLC. All rights reserved.

www.triadconsulting.com

P.O. BOX 930 - TRAVERSE CITY, MI 49685 OFFICE: 231.268.3613 - FAX: 866.534.6010 info@triadconsulting.com