NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

INTERNET SECURITY

E-mail and Web Site Security

Graduation Project
COM-400

Student: Alaa Qeshta (991479)

Supervisor: Professor.Dr
Fakhreddin MAMEDOV

Nicosia-2003

AKNWOLEDGEMENT

First of all, I would like to knowledge my profound indebtedness to my supervisor Prof. Dr. Fakhreddin Mamedov, under his guidance I have successfully overcome many difficulties require in this project, under his supervision, and discussion made through out the conduction of this project, and available comments on his study.

Through the years of education, my family has given me the fortitude to complete my graduate study with their endless encouragement and supports, special tanks would go for them.

Finally, I wish to express my gratitude and appreciations to every body who have contributed their efforts to make this project a successful one.

I specially, thank the committee members and my committee chairman Prof. Dr. Fakhreddin Mamedov

E-mail and Web Site Security

CHAPTER 6

Making Your Email Secure

CHAPTER 7

Using of Secure Email

ABSTRACT

In this project, you can see the contents about E-mail and web site security and the difference between the two kinds of security, how they work and how to make your E-mail secure from workers and hackers.

Also you can see some examples and their solution how it works and how to solve the problems.

There are some different types of secure e-mail and secure web site with some figures and how to work.

CHAPTER 1

"Automatic Repair" of Hacked Web Sites -an Information Security "Best Practice"

An Overview

Your web site is crucial to your business. What happens if it goes down? What happens when a hacker paints a political slogan on your home page, or steals your customer's credit card information? Will your firewall keep you safe? Will your intrusion detection tools catch everything?

No. Unfortunately, widely used "detect and prevent" methods don't always keep the bad guys out of a web site. You need an automatic way to fix your web site when the bad guys do get through.

"Automatic Repair" technology from Lockstep Systems automatically restores the correct content to your web site if a hacker has changes something. Our Web Again software is the first on the market to provide "Automatic Repair" for web site content. Now companies can confidently employ "Automatic Repair" as a "Best Practice."

1.1 Web Site Content Dependence and Risks

Reliable, always-available web sites are increasingly crucial to business and government enterprises. The integrity of content (e.g. web pages, images and scripts) comprising such web sites must be preserved to ensure availability and reliability.

Because of their dependence on their web sites, enterprises face considerable risks if web site content integrity is compromised or content is altered by unauthorized means:

- **Business Disruption**

Web site downtime due to corrupted content can be measured in terms of lost opportunity and the cost of alternative manual methods.

For example, a $100 million/year e-business could lose over $10,000 of revenue per hour of downtime if orders cannot be processed. Manual transactions, which may be necessary to replace the online order process while a web site is unavailable, are typically far more costly than on-line transactions.

- **Cost to Recover**

Recovery from content corruption can be costly if the recovery is based on reactive, manual methods. In a typical web site corruption incident, after a hack has been reported by a customer or employee, the web site is taken off line, a correct backup is located, and the web site is restored manually, usually in a panic mode. Money, time and frustration can be saved if the recovery is proactive and automatic, not reactive and manual.

- **Public Image**

A web site is a crucial element of an enterprise's public relations and customer interaction strategy. A home page defaced with pornography or political propaganda can be irritating or insulting to customers or constituents, thereby undermining confidence in the enterprise.

- **Transaction Theft**

While the majority of web site content corruption is the result of vandalism (Electronic graffiti), a recent survey stated that fully 13% of respondents whose web sites had been hacked had experienced the theft of transaction information as a direct result of the intrusion. i This can occur when a hacker changes a script or program on the web site to divert sensitive customer information (e.g. credit card number or confidential details) to illicit destinations.

- **Legal Liability**

If legally-binding documents (e.g. privacy policies, price lists, terms and conditions, financial results) are modified by a hacker and other web site visitors innocently rely on the altered content to make business decisions, the enterprise may incur unforeseen and potentially costly legal liability.

- **Hacking Threat**

Enterprises are increasingly subject to these risks because of the geometrically escalating threat of web site content corruption by hackers.

i. In an increasingly hostile global Internet environment, computer system intrusions are more than doubling each year.

ii because hackers are employing sophisticated automation tools and becoming much more focused in their attacks.

1.2 Introduction to FileMaker Pro Web Security

Pro software enables you to create powerful database solutions and publish them to your intranet or the Internet, so that users browse, search, and update the databases through a browser. When FileMaker Pro databases are used individually, shared on a peer-to-peer basis, or shared using FileMaker Server, FileMaker Pro security consists of passwords and access privileges. Passwords protect access to your databases, and the access privileges associated with those passwords determine your guests' ability to create, edit, delete, or export records, design layouts, and so forth. This is a security model that is both simple and powerful. Beçause sharing with FileMaker Pro guests or the Local and Remote Data Access Companions should only take place within the protected environment of a local area network, there is virtually no risk of an outside attack; data shared in these situations is very secure. When you share your FileMaker Pro databases over the Web or over an intranet, your networking environment is more complex, and your security needs are typically more complex as well. In those situations, you can use either access privileges or the FileMaker Pro Web Security Database with Custom Web Publishing to protect your databases.

Before you publish your databases on the Web, carefully consider your security needs, and follow the security procedures explained in this document. As the primary purpose of this document is to provide guidelines for FileMaker Pro web security, other aspects of web security are identified more generally. For more information about these topics, consult your network administrator, third-party documentation, or other network professional. The security concerns for your web-published databases can be divided into two broad categories: the need to protect your database files from outside attacks, and the need to protect your actual data from being improperly viewed, manipulated, or deleted.

1.3 Protecting your Databases from Outside Attacks Physical Security

First, consider the physical security of your host machine. The host computer should be a dedicated machine stored in a locked room, where it is secured to an immovable object such as a large desk, computer cabinet, or specialty anchoring hardware. The machine should be secured so that its hard drive cannot be removed.

Also consider the physical security of backup copies of files and databases that may be stored on portable media, such as tapes and diskettes. Finally, access to the host machine should be controlled, and only the minimum number of people necessary to deploy and maintain your databases should have access to it. You may not need this degree of security, but be aware that each step removed from the ideal represents an increase in the physical vulnerability of your host machine.

When assessing the physical security of your network, consider that the use of wireless networking devices, such as the Apple AirPort and other 802.11b networking cards and base stations, can pose some special security challenges. These devices can broadcast your network traffic beyond the walls of your building, so it is extremely important to encrypt your wireless networking signals. If you choose to use these devices as part of your network, always use the maximum level of signal encryption available.

1.4 Operating System Security

The security mechanisms of the operating system on the host computer need to be used to ensure that access to the directories holding the FileMaker Pro databases and related files are properly controlled. System user IDs, passwords and directory access privileges should be controlled so that only the people authorized to administer and maintain the FileMaker databases or the system as a whole will have access to the files. You should review settings for remote access, such as file sharing and FTP, to ensure that direct access to upload or download files from the host computer are restricted in a manner that prevents inappropriate access to your files.

1.5 Web Server Security and the Web Companion

The software you use to publish databases, images, and other content to the Web is called web server software. Web server software performs the critical task of processing and fulfilling requests for data. When someone enters a web address into their browser, they are requesting the web server software at that address to locate data or an image and download it to their machine, where it can be displayed in their browser. To protect the integrity of this process, your web server has its own security mechanism.

The FileMaker Pro Web Companion is a plug-in component of FileMaker Pro. The Web Companion functions as an HTTP server/web server/Common Gateway Interface (CGI) application, communicating with web browsers that request data from or submit data to a FileMaker Pro database. When you publish your data using FileMaker Pro Instant Web Publishing, the FileMaker Pro Web Companion functions as the web server, and security is provided by FileMaker Pro access privileges. As with FileMaker Pro desktop publishing, access via Instant Web Publishing is controlled by passwords. When you publish your data using FileMaker Pro Custom Web Publishing, you can use the FileMaker Pro Web Companion as your web server. If you are using FileMaker Pro Unlimited software and the FileMaker Web Server Connector, you can use third-party web server software, such as Microsoft Internet Information Server (IIS) or Apache Web Server.

If you are using the FileMaker Pro Web Companion as your web server, security is provided by either access privileges or the Web Security Databases. If you are using a third-party web server with Custom Web Publishing, your web server software may offer additional security features. Consult the documentation included with your web server software for more information.

1.6 FileMaker Pro Web Security Database

The FileMaker Pro Web Security Database is a set of three related databases that work together to protect databases published using Custom Web Publishing. The Web Security Database lets you provide user name and password protection to multiple FileMaker Pro databases. You can set specific user permissions and field restrictions for each database, and update or change those settings directly from your web browser.

The Web Security Database includes two types of files: databases for providing web security and HTML files for changing the web security settings remotely. When users attempt to access your protected database on the web, their web browser will display a user name and password dialog box, and they will be required to input both a user name and a password before proceeding.

This behavior is potentially more secure than that offered by access privilege protection, in which only a password is required (user name data is ignored by access privilege protection). With the Web Security Database, once a user name and password are established, that information is sent by the web browser with every request to the Web Companion. The Web Companion then checks those values against the settings configured in the Web Security Database and grants permissions or field restrictions based on the specified privileges. Remember, you can use access privileges or the Web Security Database when using Custom Web Publishing. Determine which security method delivers the specific features you need before you begin developing your custom web pages.

CHAPTER 2

How to Secure your Data in FileMaker Pro Web Publishing

You can publish FileMaker Pro databases to the Web or to an intranet by using either FileMaker Pro Instant Web Publishing or FileMaker Pro Custom Web Publishing.

2.1 Protecting Data for Instant Web Publishing

To secure your database for Instant Web Publishing, you must use FileMaker Pro access privileges to define one or more passwords for users who will be accessing your database over the Web/ intranet.

Important When you use access privileges as the only means of securing your database, any valid password is potentially available for use when guests access your database over the Web/intranet. The Web Companion permits you to enter any password defined in your database. If someone is aware of a valid password, they can enter that password through a browser's password dialog box. This includes master passwords, which provide access to the entire file. Even if you define unique passwords for web-only users, there is no way to disable your master password(s). Make sure that any master passwords you define are difficult to guess and are known only to those who need to use them. As FileMaker Pro access privileges are the only means of providing security through Instant Web Publishing, you should use Custom Web Publishing and the Web Security Database if you require a different level of security.

2.2 Defining Passwords

To define a web access password using FileMaker Pro access privileges:

1. Open your database file, then choose File menu > Access Privileges > Passwords.

If you see the Change Password command instead of the Access Privileges command, you have opened the file as a guest, or with a password that provides limited access. To create additional passwords, you must reopen the file as the host, with a master password.

2. In the Define Passwords dialog box, type a password in the Password box. If you want web users to have access to your database without being prompted for a password each time they access it, you can define a blank or empty password. This password can be given the same restrictions as any other password, for example, no modification or deletion privileges. When users access a database that contains a blank password from the Instant Web Publishing home page, they will not be prompted for a password and will automatically be assigned the blank password's privileges. This minimizes the ability to use master passwords. It also provides a way for all web users to access the database without being given passwords in advance. The disadvantage is that users who do need to log in with an alternate password will not be able to do so.

3. Select the privileges associated with this password.

4. Click Create.

If a master password with full access has not already been defined, you must define one before exiting this dialog box.

5. Click Done.

Note If the password limits browse privileges but does not limit the privilege to delete records, it is possible for users to delete records they cannot view. If FileMaker Pro detects this situation, it will display an alert when you create the password, but it will not prevent you from creating the password.

2.3 Specifying Access Privileges as the Security Method for Instant Web Publishing

After you have defined a web access password, verify that FileMaker Pro access privileges will be the security method used with Instant Web Publishing.

1. Choose Edit menu > Preferences > Application.

Mac OS X: Choose FileMaker Pro menu > Preferences > Application.

2. In the Application Preferences dialog box, click the Plug-Ins tab.

3. Select the Web Companion Plug-In from the list, then click Configure.

4. In the Web Companion Configuration dialog box, make sure that FileMaker Pro Access Privileges is selected.

5. You can also restrict database access to certain client IP addresses. When the Restrict access to IP address (es) box is checked, only those IP addresses specified (explicitly or through wildcards) in the accompanying text box will be granted web access. This restriction will apply to all databases. Access privileges will still be enforced for those IP addresses that are granted access.

6. Click OK.

7. Click OK in the Application Preferences dialog box.

2.4 Protecting Custom Web Publishing Solutions

There are two methods of protecting Custom Web Publishing solutions: FileMaker Pro access privileges or the Web Security Database.

Important When you publish databases using FileMaker Pro Custom Web Publishing, you make it possible for the Web Companion to use XML and/or CDML to execute commands in FileMaker Pro. The ability to use XML and/or CDML is intrinsic to Custom Web Publishing, and cannot be disabled; however, the execution of these commands can be limited or prohibited using the security methods.

2.5 Using the cdml_format_files Folder

FileMaker Pro 6 introduces a new feature to protect the source code and structure of your CDML format files: the cdml_format_files folder. Located at the root level of the FileMaker Pro folder, the cdml_format_files folder provides a way to protect your format files (files that are specified using the -format parameter) when publishing databases using Custom Web Publishing. Unlike the FileMaker Pro Web folder, the cdml_format_files folder cannot be accessed directly by the FileMaker Pro HTTP server. Instead, the Web Companion searches this folder for CDML format files during CGI requests.

The Web Companion will forward the results of a search or other action that references a CDML format file located in this folder, but it will deny any attempts to view the source code information of files located within it.

2.5.1 Protecting your CDML Format Files

The easiest way to protect one or more CDML files in an existing solution is to copy the entire directory into the cdml_format_files folder and then delete the CDML format files from their original locations within the Web folder. No modifications to the content of the solution are necessary. Copying the entire folder will leave duplicate copies of static content, such as image files and standard HTML pages, in the cdml_format_files folder. This will make it easier for you to maintain your solution, and your site will function normally, but you should be aware that the Web Companion will only access static content from within the Web folder. For Windows development, we recommend managing your CDML format files together with other related files in a development directory, either in a separate development folder that is not published to the web or in the appropriate sub-folder under the cdml_format_files folder. By using a development directory, you can edit your files and preserve the file references used in relative links typically managed by HTML authoring environments. You can then separately publish the public files into the appropriate sub-folder of the Web folder when ready for web users to see, and if needed publish the CDML format files into the appropriate sub-folder of the cdml_format_files folder.

For Mac OS development, you can manage your files in the same way using a development directory as described above. Another option is to manage the CDML files in the cdml_format folder, and use aliases within the cdml_format_files sub-folders to point back to the corresponding sub-folder in the Web folder. This will typically resolve any broken link/missing image problems when working in HTML authoring environments. For example, you can have an alias in the cdml_format_files copy of the site named 'images' which points back to the images folder in the Web folder, rather than copying the entire images sub-folder under the cdml_format_files folder.

Important For better security, we do not recommend placing aliases to locations outside of the Web folder within the cdml_format_files folder or Web folder.

2.5.2 cdml_format_files Folder Tips

• The cdml_format_files folder lies outside of the Web folder. Any HTTP request attempting to access it directly will result in a "file not found" error.

• The cdml_format_files folder is intended to be a repository for your CDML format files only. Image files, XSLT and/or CSS style sheets, or other types of files will not be recognized or served by the Web Companion if they are placed in this folder. For convenience, you may place duplicate copies of these files in the cdml_format_files folder, but these files can only be served by the Web Companion if they are also present in the Web folder.

• FileMaker, Inc. does not recommend storing databases in the Web folder (or sub-folders). Databases can be stored in any file folder on the system, including the cdml_format_files folder. However, their placement in the cdml_format_files folder serves no distinct purpose from other folders on the system, and consequently is not recommended.

• The cdml_format_files folder will not be accessed by the -dbopen action. Databases placed within the cdml_format_files folder can be used in a solution. But they must be launched by some means other than the -dbopen command. Optionally, you may decide to leave one or more databases within the Web folder in order to use the -dbopen command. Because this command is only available when remote administration is enabled, be aware that enabling remote administration also enables support for the HTTP PUT command, which can compromise security in the Web folder.

• The FMP-Include tag checks for the path to the cdml_format_files folder. No error is returned when this tag is used, since the FMP-Include tag is used to add content to a document being processed by the Web Companion. Using You do not need to change any code containing the FMP-Include tag, since the new behavior of the Web Companion causes it to automatically search for format files within the cdml_format_files folder. Protect files containing the FMP-Include tag by copying it to the cdml_format_files folder.

Note With remote administration enabled it is possible to use HTTP PUT to place a CDML format file within the Web folder. Such a file could include the FMP-Include tag which could specify a CDML format file that was in the cdml_format_files folder. You can prevent such an attack by only enabling remote administration when absolutely necessary.

Important Although the FileMaker Pro HTTP server cannot make HTTP requests within the cdml_format_files folder directly, this feature is intended to provide security for CDML format files only. This feature is not intended to protect data, provide any additional system integrity, or prevent an attack by other means.

CHAPTER 3

Using the Web Security Database

The FileMaker Pro Web Security Database is a set of three related databases working together to protect your databases published on an intranet or the Internet. Designed to work with your custom web pages, the Web Security Database lets you provide user name and password protection to multiple FileMaker Pro databases. You can optionally set specific user permissions and field restrictions for each database, and update or change those settings directly from your web browser. With a Web Security user name and a password, web users can do one or more of the following in your published database(s):

- Browse records
- Create records
- Edit records
- Delete records
- Perform scripts
- View all except certain restricted fields
- Search all except certain restricted fields
- Edit all except certain restricted fields
- Enter a special value in a restricted field and view, edit, or delete only those records that contain the exact matching value
- Modify or delete records containing exact matching values in the restricted field

Important The Web Security Database is not designed to work with FileMaker Pro Instant Web Publishing. The ExactSearch, ExactUpdate, and ExactDelete field restrictions do not function properly in Instant Web Publishing. [1]

3.1 How the Web Security Database Works

The Web Security Database includes two types of files: databases for providing web security and HTML files for changing the web security settings remotely. Web security is controlled by a main database named Web Security.fp5 and two related databases named Web Users_.fp5 and Web Fields_.fp5.

When users attempt to access your protected database on the Web, the web browser displays a user name and password dialog box. Once you establish a user name and password, they are sent by the web browser with every request to the web server. The FileMaker Pro Web Companion checks these values against the settings configured in the Web Security Database, and then determines if any user permissions or field restrictions exist for a specific action.

3.2 Installing the Web Security Database

When you install FileMaker Pro, the Web Security Database files are automatically installed in Web Security/Databases folder. If the folder isn't there, then you'll need to do a custom install.

Note Do not install the Web Security Database to the Web folder unless you intend to use Remote Administration.

3.3 Enabling the Web Security Database

The Web Security Database must be open before you can enable it in FileMaker Pro.

1. In FileMaker Pro, choose File menu > Open and open the Web Security.fp5 file. (FileMaker Pro/Web Security/Databases/Web Security.fp5) The related files, Web Users_.fp5 and Web Fields_.fp5, also appear in separate (usually minimized) windows (Windows) or in the Window menu (Mac OS).

2. Choose Edit menu > Preferences > Application. Mac OS X: Choose FileMaker Pro menu > Preferences > Application.

3. In the Application Preferences dialog box, click the Plug-Ins tab (or choose Plug-Ins from thepop-up menu).

4. Select the Web Companion checkbox to enable the Web Companion plug-in.

Note If Web Companion doesn't appear in the Application Preferences dialog box, you must install the Web Companion plug-in.

You only need to enable the Web Companion plug-in once for the FileMaker Pro application. To do so, you must have a connection to the Internet or an intranet.

5. With Web Companion selected, click Configure.

6. In the Web Companion Configuration dialog box, make sure that Enable Instant Web Publishing is not selected (the Web Security Database is not designed to work with FileMaker Pro Instant Web Publishing).

7. Select Web Security Database to enable it.

Note The Web Security Database option is not available (dimmed) when the Web Security.fp5 database is not open.

8. For Remote Administration, select disabled if you do not plan to do remote administration.

Note Because of the additional risks to database security, FileMaker, Inc. strongly recommends that you leave Remote Administration disabled unless you are certain that you need to use this feature.

9. For Remote Administration, select Requires password and enter a password in the box if you want to access the Web Security Database settings later from the Web. Requiring a password for remote administration ensures that unauthorized web users cannot gain access to the Web Security Database and other files located in the Web folder. It is not recommended that you do remote administration without a password.

10. Click OK to close the Web Companion Configuration dialog box.

11. Click OK to close the Application Preferences dialog box.

12. Choose File menu > Sharing and make sure that the database is shared via the Web Companion.

Important When you select the Web Security Database as your method of security, you must create a record in the Web Security Database for each database you intend to share over the web. With this security method, web users will only be able to access those databases that are configured in the Web Security Database.

3.4 Assigning Web Security to your Databases

To protect one or more databases with the Web Security Database, you create a record for each database. In each record, you set up user names, passwords, and permissions for each user, and field restrictions for each database.

1. In the Web Security.fp5 database, create a record for each database you want to protect by choosing Records menu > New Record.

2. In the Database Name field of each new record, type the name of the database you want to protect. Or, type All Databases in the Database Name field of one record if you want to make the same user permissions and field restrictions for all of your published databases.

3. If the database has a password set up with FileMaker Pro access privileges, and you want that password's restrictions to be added to those of the Web Security database, type that password in the Database Password field. In most cases, you should type the master password here.

Note Any access privilege restrictions placed on the Database Password in FileMaker Pro override the Web Security Database permissions. Web access privileges can never be greater than the privileges provided by the Database Password, regardless of the settings in the Web Security Database.

4. Type the first user name in the User Name field.

5. Type a password in the User Password field.

When creating a password, use only the characters A through Z, numerals, or a combination of the two. Do not include spaces in your password. This minimizes the possibility that you will choose characters that may be interpreted incorrectly over the Web.

Important Do not use leading or trailing spaces in user names or passwords for remote administration, access privileges, or the Web Security Database.

6. Select one or more of the following permissions for the user.

7. Repeat steps 4 through 6 to add permissions for other users.

Select this User Permission	To Allow the Specified Web User to do the Following
Browse	Browse records in the database, subject to any field restrictions set below
Create	Add records to the database, subject to any field restrictions set below
Edit	Modify records in the database, subject to any field restrictions set below
Delete	Remove records from the database, subject to any field restrictions set below
Scripts	Run scripts defined in the database

Browse records in the database, subject to any field restrictions set below Create Add records to the database, subject to any field restrictions set below Edit Modify records in the database, subject to any field restrictions set below Delete Remove records from the database, subject to any field restrictions set below Scripts Run scripts defined in the database. You can type All Users in the User Name field to create privileges that apply to any web user. These privileges override more restrictive privileges set for other users. Therefore, if you set All Users to be able to browse, create, and edit records, then any other user names you enter for this database can also browse, create, and edit records regardless of the user permissions you set for them. Leave the User Password field blank if you're setting privileges for All Users. (FileMaker Pro displays an alert if you attempt to enter a password for All Users.)

8. In the Field Name field, type the name of any field that you want to restrict for this database (be sure to type the defined field name, not the name of a field label) and select one or more of the following restrictions for the field.

When this Field Restriction is Selected Web Users can do the Following

DontShow	View all fields in a record except this field. If a field with this restriction appears in the web page, a blank value is returned as if the field were empty.
DontSearch	Specify search criteria in any field except this field. Web users cannot search for data in this field.
ReadOnly	View but not edit data in this field.
ExactSearch	Retrieve only those records containing exact matching values to the search criteria specified for this field. A record is not returned unless an exact match is made with the field's value in the database. If ExactSearch is assigned to a field, the "equals" operator must be used with that field when it is present in a search action. Also, if the ExactSearch restriction is set for any field, then the -findall and -findany actions cannot be used with that database.
ExactUpdate	Edit only those records containing a value that exactly matches the value specified by the user for this field in a search. Web users cannot edit this field itself.
ExactDelete	Delete only those records containing a value that exactly matches the value specified by the user for this field in a search. Web users cannot edit this field.

Doesn't Show View all fields in a record accept this field. If a field with this restriction appears in the web page, a blank value is returned as if the field were empty. Doesn't Search Specify search criteria in any field except this field? Web users cannot search for data in this field. Read Only View but not edit data in this field. Exact Search Retrieve only those records containing exact matching values to the search criteria specified for this field.

A record is not returned unless an exact match is made with the field's value in the database. If Exact Search is assigned to a field, the "equals" operator must be used with that field when it is present in a search action. Also, if the Exact Search restriction is set for any field, then the -findall and -findany actions cannot be used with that database.

ExactUpdate Edit only those records containing a value that exactly matches the value specified by the user for this field in a search. Web users cannot edit this field itself. ExactDelete Delete only those records containing a value that exactly matches the value specified by the user for this field in a search. Web users cannot edit this field.

3.5 Protecting Specific Records in a Database Using the Web Security Database

The Exact Search, Exact Update, and Exact Delete field restrictions provide record-level security for your databases on the Web. You can limit web user access to specific records in your databases by creating a special field value for those records that only authorized users know, and applying the Exact Search, Exact Update, or Exact Delete field restrictions to the field. Web users are required to enter the correct value in a search and only those records containing the value can be displayed, edited, or deleted. By adding the Don't Show field restriction to the field, unauthorized web users will not be able to see the value when the records are displayed.

Note When using the Exact Search restriction for any field, the -findall and -findany actions cannot be used with that database. The ExactSearch, ExactUpdate, and ExactDelete field restrictions can also be applied to related fields by adding the relationship name and a double colon to the field name. Web users must enter a non-blank value for the related field when searching the database. The value cannot contain any FileMaker Pro wildcard or range search characters (*, @, !, =, //, "..", or "...").

Note: To protect specific records in a database using the Web Security Database:

1. In FileMaker Pro, define a field in the database to contain the special field value.

YourSecretCode:

2. Enter the special field value for the field in each specific record you want to protect.

YourSecretCode: ch5rries

3. In a text editor or HTML authoring program, create an HTML text field in your search web page. Include the equal's operator in the search string, and use the same name as the *field you defined in the database.*

<P><FONT SIZE="+2"><B><TT>Enter your secret code here</TT></B></FONT>

<INPUT TYPE="hidden" NAME="-Op" VALUE="eq">

<INPUT TYPE="text" NAME="YourSecretCode" VALUE="" SIZE="35"></P>

4. In the Web Security.fp5 database, type the name of the field in the Field Name field, and select the DontShow and ExactSearch field restrictions.

If you're setting restrictions for a related field, type the relationship name, a double colon, and then the field name in the Field Name field.

relationship::YourSecretCode

Now, in order to retrieve the protected records, web users must type the special field value in the HTML text field on the search page.

Note All fields that you have set with the ExactSearch, ExactUpdate, or ExactDelete field restrictions must be present in the HTML form or script that specifies the search action. For example, if two fields are specified in the Web Security Database with these field restrictions, but only one of the fields is on the search page, then an error is generated when a web user attempts a search.

3.6 Changing Web Security Settings Remotely from the Web

Using the Web Security Database HTML files, you can make changes to the Web Security Database permissions and field restrictions remotely from your web browser. Changes made this way do not require restarting FileMaker Pro, disconnecting your web server, or disrupting your web server's performance. Consider using SSL to secure remote administration communications (which will contain database names, user IDs and passwords) in order to prevent other Internet users from obtaining this information.

To remotely change Web Security Database settings:

1. Move the Security folder and its contents from the Web Security folder (inside the FileMaker Pro folder) into the root level of the Web folder.

This enables the Web Companion to serve the Security HTML pages on the Web.

2. In the Remote administration area of the Web Companion Configuration dialog box, make sure that Requires password is selected and a password is entered in the box. (See "Enabling the Web Security Database" on page 30.)

Note Although remote administration can be enabled for use without a password, such use is absolutely not recommended.

3. In your web browser, type the IP or DNS address for the computer where the Web Security Database is open, and type /Security.

For example, type <your IP address>/Security where "<your IP address>" is the IP address of the host machine. This enables the Web Companion to display the default.htm file that's located inside the Security folder.

4. In the Database Name text box on the Web Companion Security Administration page, type the name for the web security record containing user permissions or field restrictions that you want to change and click OK. If a page contains a Reset button, you can click Reset to clear the form.

5. At the password prompt, type admin in the User Name field, type the password that you specified for Remote Administration in the Web Companion Configuration dialog box, and click OK. On the resulting web page, you see a summary of the user permissions and field restrictions for the specified database. You can remove the web security record of this database from the Web Security Database by clicking the Delete Database button on this page. If the password for the database was changed in FileMaker Pro, you can type the new password in the Database Password box and click Update Password to update the web security record.

Type "admin" in the User Name box

6. Click the underlined link to a user name that you want to change permissions for.

On the User Permissions page, you can remove the user name from the web security record byclicking the Delete User button.

7. Change the user password and permissions as desired and then click Update User.

The record for the specified database is updated in the Web Security Database.

8. Click the View <filename.fp5> Database link to return to the summary page.

9. To add a user, click the Add User link on the summary page for the specified database.

The Add User page appears. This enables you to create permissions for a new user in the database record.

10. On the Add User page, enter the desired user name, password, and permissions, and then click Add User.

11. Click the View <filename.fp5> Database link to return to the summary page.

12. Click a field's underlined link on the specified database's summary page to change the restrictions for the field in the specified database.

13. On the Field Restrictions page, change the field's restrictions as desired and then click Update Field.

14. Click the View <filename.fp5> Database link to return to the summary page.

15. To add a field, click the Add Field link on the summary page for the specified database. The Add Field page appears. This enables you to create restrictions for a new field in the database.

16. On the Add Field page, enter the desired field name and field restrictions, and then click Add Field.

17. Click View a Different Database to return to the Web Companion Security Administration page.

18. To add a database, click the Add Database link on the Web Companion Security Administration page. The Add Web Database page appears. This enables you to add a new database record to the Web Security Database.

19. In the New Database Name box, enter the name of the database you want to create a web security record for.

20. If the database has a password set up for FileMaker Pro access privileges whose permissions you wish to add to those of the Web Security Database, enter it in the New Database Password box.

21. Enter the first user name and the desired password and permissions. Then click Add Database. The summary page for the new database record appears. From this page, you can add more user names and permissions and set field restrictions for the new database.

3.7 Web Security Database Tips

Keep these points in mind when using the Web Security Database:

• In the Web Security Database, you can set user permissions for Browse, Create, Edit, Delete, and Scripts. The Web Security Database permissions for Create, Edit, and Delete do not restrict ScriptMaker scripts from performing these actions. Use access privileges to secure databases thathave ScriptMaker™ scripts. Scripts that include the New, Duplicate, Edit, Delete, or Export Records script steps should be protected by access privileges, although you can also use the WebSecurity Database to prevent all scripts from being executed on a user-by-user basis.

CHAPTER 4

Using SSL Protection with Custom Web Publishing

The Secure Sockets Layer (SSL) protocol is a standardized method for allowing encrypted and authenticated communication between web servers and web browsers. Encryption through SSL converts information being exchanged between web servers and web browsers into unintelligible information through the use of mathematical formulas known as ciphers. These ciphers are used to transform the information back into understandable data by the intended recipient through encryption keys. The actual instruments used to provide SSL protection are termed SSL certificates. SSL server certificates satisfy the need for confidentiality, integrity, and authentication. These certificates form the basis of an Internet trust infrastructure by allowing web sites to offer safe, secure information exchange to their customers. Server certificates are the first step to setting up an SSL environment, and are available from independent, third-party Certificate Authorities (CAs), such as VeriSign (www.verisign.com).CAs issue certificates to individuals, organizations, and web sites. To implement SSL you must request and then install a digital certificate on a web server. You can enable SSL capabilities after the certificate has been successfully installed.

SSL server certificates fulfill two necessary functions:

• SSL server authentication to allow web users to verify a web server's identity. Web browsers automatically check to see if a server's certificate and public ID are valid and have been issued by a certificate authority (CA).

• SSL encryption to allow a secure channel of communication that enables information sent between a web browser and a web server to be encrypted, preventing information from being intercepted over the Internet. SSL encryption also monitors the integrity of the data being sent over the Internet and determines whether it has been altered in any way during transit. This allows information to be sent securely and confidentially.

Note SSL protection is only available to users of Custom Web Publishing with FileMaker Pro Unlimited software, and only through the use of the FileMaker Web Server Connector (FMWSC) and third-party web server software, such as Microsoft Internet Information Server (IIS).

Example: Configuring SSL with Microsoft IIS

Part 1: Generating A Private Key Pair and Certificate Signing Request (CSR)

1. In Microsoft IIS, open Administrative Tools and then the Internet Services Manager. Right-click and select Properties for the web site you want.

2. Select the Directory Security tab in the Web Site Properties window. In the Secure communications section, click Server Certificate.

The IIS Certificate Wizard dialog box appears.

3. In the Server Certificate window, select Create a new certificate, then click Next.

4. In the Delayed or Immediate Request window, select Prepare the request now, but send it later, then click Next.

5. In the Name and Security Settings window, type a name for the new certificate.

The name should be easy for you to remember.

6. Choose the encryption strength for your server, then click Next.

Note Choose the highest encryption strength you are permitted. 128-bit SSL is the most powerful encryption compatible with both U.S. and worldwide versions of Microsoft Internet Explorer and Netscape browsers.

7. In the Organization Information window, select or type your organization's name and your organizational unit (your department). Click Next.

8. In the Your Site's Common Name window, enter the full domain name for your web site. For Internet sites use a valid DNS. You can also use a computer's NETBIOS name for intranet servers. Click Next.

9. In the Geographical Information window, select your country/region, you state/province, and your city/locality. Click Next.

10. In the Contact Information window, enter the name, phone number, and email address for the administrator requesting the certificate. Click Next.

11. In the Certificate Request File Name window, specify a location to save the certifica request. Depending on how you are requesting the certificate and which Certifica Authority you are using, you may need to copy and paste the certificate request into a we browser or send it via email. Click Next.

12. In the Request File Summary window, confirm that the information you have entered correct, then Click Next

The IIS Certificate Wizard should now confirm that you have successfully created certificate request. If you have not determined which certification authority you would lik to use, you can select a link from this window for a list of CAs that offer services f Microsoft products.

13. To close the IIS Certificate Wizard, click Finish.

Part 2: Entering your Certificate

1. After you have received your certificate from your Certification Authority (most like via email), copy the portion that begins with -----BEGIN CERTIFICATE----- to the portic that ends with -----END CERTIFICATE----- and paste it into Note Pad or a similar te editor.

2. Save the file as Certificate.CER

Note If you have used a different method for obtaining a certificate you may not need save the file. For example, if you have used a Certificate Server, the .CER file may hav been downloaded to a specified location. If you have received a .CER file, you can proce to the next line.

3. Open Administrative Tools and then the Internet Services Manager. Right-click ar select Properties for the web site for which you want to enable the certificate.

4. Select the Directory Security tab in the Web Site Properties window. In the Secu communications section, click Server Certificate.

5. In the IIS Certificate Wizard dialog box, click Next.

6. Select Process the pending request and install the certificate, then click Next.

7. Select the location of the .CER file, and then Click Next.

8. The IIS Certification Wizard displays the summary of the Certificate. Verify that the information is correct, then click Next.

9. Click Finish to complete the installation of your certificate.

Part 3: Enabling and Configuring SSL and other Certificate Features

1. In the Secure Communications section of the Directory Security tab for the web site, the Edit button should now be enabled. Click Edit.

2. Select Require secure channel (SSL).

3. Select Require 128-bit encryption, if applicable.

4. Click Apply, and then click OK to enable SSL and close the property window.

Note You can also specify how your site will handle client certificates, enable client certificate mapping, and enable the certificate trust list in this property window.

Part 4: Testing your new SSL Enabled Web Site

1. Attempt to access your site by typing http://localhost/Postinfo.html in the address bar of your web browser. You should receive an error message:

The page must be viewed over a secure channel

The page you are trying to view requires the use of "https" in the address.

HTTP 403.4 – Forbidden: SSL required Internet Information Services

Note The Postinfo.html page is a standard HTML page found in the root folder of the default web site.

2. Attempt to access the same web page by typing https://localhost/Postinfo.html in the address bar of your web browser. If you can view the Postinfo.html page you have successfully installed the certificate.

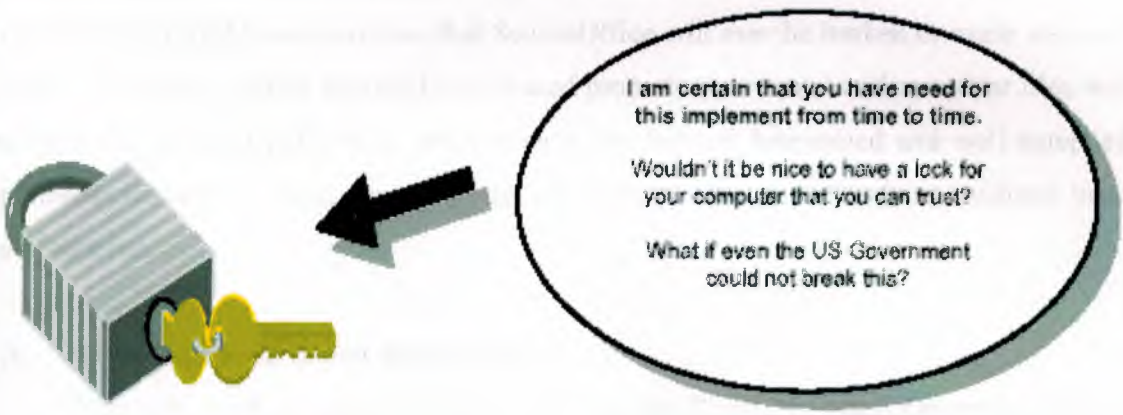
Note You may see a security alert stating that the certificate is not from a trusted root CA. Ignore this alert, and click Yes to continue to the web page.

CHAPTER 5

E-mail Security

An Overview

5.1 What is SecureOffice?



SecureOffice is an easy to use Cryptography Program that works with Microsoft Windows and Microsoft Office. SecureOffice will keep snoops, busy bodies, and the FBI Computer Crime Lab from reading your sensitive computer files and email. If you want to keep the documents on your computer private and prevent people from reading them, then you would use SecureOffice as a layer on top of your normal operations with such programs as Word, Excel, PowerPoint or a host of other programs that run under Microsoft Windows. SecureOffice works with your existing email system to prevent unauthorized access (anybody but the intended recipient) from reading your email. SecureOffice can also detect email tampering.

If you care to learn a little bit about the mathematics of Cryptography then I believe that I can prove to you that there is no Back Door to SecureOffice. I can prove to you that my algorithms, file formats, and cryptographic technique is what I claim they are. I encourage all of the hostile skepticism that humanity can manifest. The truth alone has never resulted in any human progress. It is only doubt that sets humanity free. I have tried, to the best of my ability, to make the subject of Cryptography, and the cryptographic methods I have used with SecureOffice as transparent to the user as possible. I have included CryptView with SecureOffice. CryptView is a separate computer program that will allow you to view the basic operation of SecureOffice and most of the file formats that SecureOffice generates. SecureOffice is the program where you are going to do 99% of the work. CryptView is the program I have written with the skeptic in mind.

You may decide that you never want to look at CryptView. If you hate math, and you want to keep your pornography collection on your lap top computer away from your parents, wife, girlfriend, boyfriend, or whatever, then you really don't have such a huge stake in the security of your documents. If you are a white collar criminal planning a major financial crime, and you think that you are clever enough to get away with it, then it is in your best interest to look at CryptView and approach SecureOffice with all the skepticism that you can muster. If you are smart enough to deal illegal drugs (a form of commerce that I approve of), or commit financial crimes (a form of commerce that I do not approve of), and you think that you are smart enough to escape the long arm of justice, then you had better be smart enough to understand the mathematics and file formats of SecureOffice. I do not ask for your trust. I demand your skepticism. I have also attempted to make SecureOffice easy and fun to use. If you do not care to become an expert in cryptography, that is OK as well.

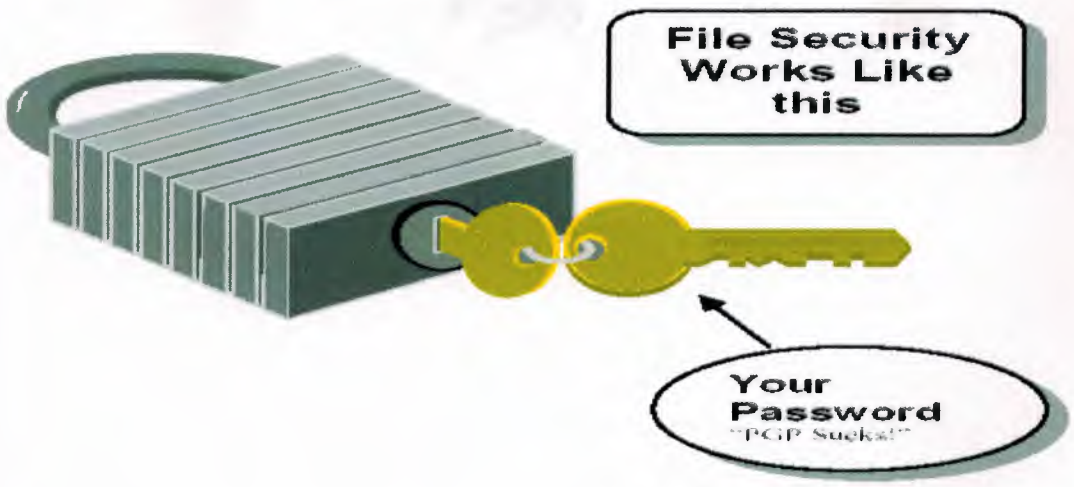
5.5 There are Three Things that are called Keys in SecureOffice

1. Symmetrical keys that are used to store and transmit document information. These Keys are computed from a password using a One Way Hash when you are storing information, and are selected randomly when you are transmitting information.

These keys are 168 bits long meaning that they can be any number between 0 and 374144419156711147060143317175368453031918731001856 these numbers are usually expressed as hexadecimal numbers. Computer programmers use hexadecimal (base 16) because it is very easy to convert to binary and it is much more compact than binary.

2. Public-Private key sets are small lists of very large numbers. One of the numbers in this list is the Private Key, and the rest of the list is the Public Key. You send the Public Key to another user and then when that user wants to send a secure document to you they make up a random 168 bit number and then encrypt it with your public key. They encrypt the rest of the document with the random 168 bit number as key and send the entire package to you. When you get the message you compute the random 168-bit number back using the Private Key and then decrypt the rest of the document.

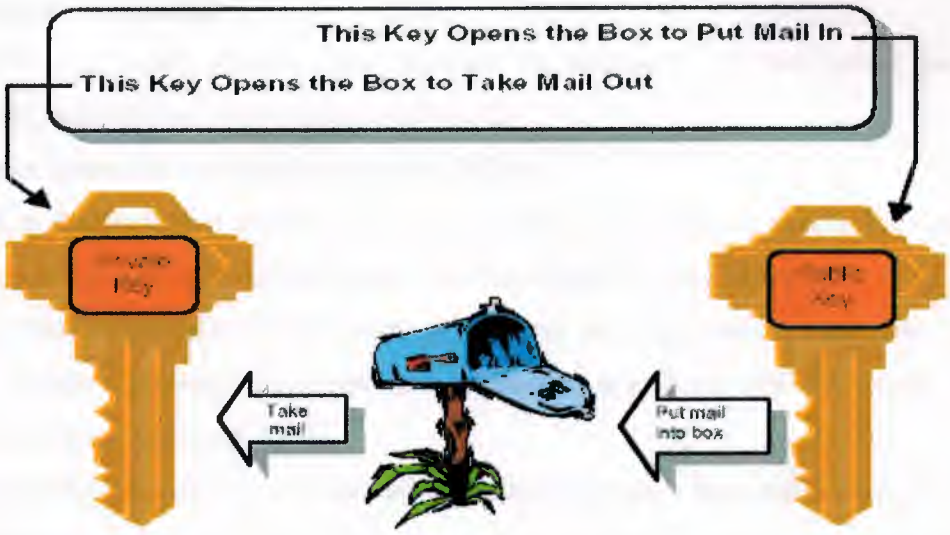
3. License Keys enable you to extend your version of SecureOffice. You have a license key in your license dialog that is always 64-bits or 8 hex characters long. You email this number to me and I compute another 64-bit number that will reset your expiration date on SecureOffice. File Security allows a user to store a document on a computer disk in such a way that another person cannot access the file without providing a password to the document. The password is provided when the document is created and must be invoked every time the document is opened. Passwords on documents can be changed. A password can be any length or composition. A strong password should contain a mixture of upper and lower case, numbers, spaces, and punctuation symbols. A password should be something that you have an easy time remembering.



Email Security (Public Key Cryptography)

A mailbox has two keys. Imagine that there is a **Public Key** one key that allows anybody to put mail into your box and you have a **Private Key** that allows you to open your mailbox and read your mail. You give the public key to another person so that you can get mail from them, and you keep the private key and use it to read your Email.

An Email Key is just a list of numbers that satisfy some mathematical relationships. Don't worry about the math you can view it, but you do not need to understand it to use the program.



5.6 Classification of E-mail Security

Objectives

This focuses on the functionality and requirements for email security controls. Email security mechanisms on information systems may have some or all of the objectives as follows:

a. To protect the confidentiality of identified information by preventing leakage of information to those without need-to-know.

b. To ensure an appropriate level of sender authentication and nonrepudiation.

c. To ensure an appropriate level of email integrity.

d. To protect the availability of the system by controlling access to critical system functions and preventing malicious code based denial of service attacks.

1. Email Terminology

Electronic mail (Email) has become an essential communication tool for government and business organizations worldwide.

Some of the common terms those are used as follows:

a. **HTML** is the Hypertext Markup Language. HTML is an evolving standard for creating web pages, and is also used for the transfer of some electronic mail messages.

b. **XML** is the 'Extended Markup Language', and an emerging standard for creating rich content, flexible electronic documents and application interfaces. XHTML is the bridge standard between HTML and XML.

c. A **mail server** is a software tool that receives email messages from either an email client, or another email server, and either routes the message to another server that is closer to the final recipient, or stores the message locally for collection by the final recipient.

d. A **mail client** is a software tool run by an end-user that is able to view email messages and associated attachments. Messages may be resented in raw text, or in some cases HTML or XML.

2. Mail Client Security

Some mail clients allow users to receive messages formatted in HTML, and will even run Java applets, VBScript, or Active-X controls. As such, your mail client may have similar client-side security risks as identified in Software or data files with embedded code (e.g. across) that are received as attachments in mail messages and are saved and executed or opened locally may contain malicious code that impacts negatively on the client system. Any executable code downloaded via email, the World Wide Web, news groups, gopher, or ftp, may contain malicious instructions designed to:

a. Introduce a virus into the organisation.

b. Conduct denial of service attacks.

c. Gain access to otherwise restricted information

Without appropriate controls on the receipt and execution of machine executable code, an organisation may be accepting significant risks to the stability and integrity of their internal network. Controls such as virus checking software may be appropriate for some organisations. More thorough controls may be to remove or quarantine executable content or attachments from email messages using a proxy or firewall solution.

3. Mail Server Security

Installation of mail server technology creates an access point into an agency's network that can potentially be misused by attackers. A poorly configured or maintained mail server is likely to introduce problems that allow unauthorised remote users to perform actions outside the scope of legitimate activity, impacting on the confidentiality, integrity or availability of the network, hosts and/or users. Examples of such actions include:

a. Flooding a server with large quantities of useless mail so that users find it difficult to access legitimate messages.

b. Retrieve information about the server computer that may allow a potential attacker to target the computer more effectively.

c. Exploit a bug in the mail server, which allows an attacker to execute commands that detrimentally change the system.

d. Exploit a bug in the mail server or other open resource to gain access to email messages before encryption is applied, or after decryption.

e. Use the mail server to distribute varies into the organisation.

f. Use the mail server as a spam relay to forward junk email to other organisations

A mail server is a conceptually simple piece of software, which accepts items of mail for delivery to a named recipient. An extremely simple email server can be implemented with a very small number of lines of code. More complex mail servers run into hundreds of thousands of lines of code. Complex server components are likely to contain errors, and some of these errors may potentially impact on the security of the server in question. Ensuring that the mail server has the latest recommended security patches will minimise the chances of a successful, well known attack. However, the primary factor in mail server security is the application of sound configuration control and management techniques.

Some simple operating system configuration mechanisms can be used to reduce the effectiveness of potential attacks against your server. Many of the controls are operating system specific, but can be broadly grouped into the following categories:

a. **Privilege reduction**. Running the mail server as a non-privileged user, this has limited access to system resources.

b. **File system limitation**. Ensuring that the user that run the mail server has limited access to the host file system. On Unix machines, this may imply that the server runs in a 'chroot' environment - with access only to the mail spool directory and appropriate configuration files at runtime. For Windows NT servers, this may imply restricting the user's group memberships to a very limited subset, and setting access controls to severely limit file system access for those groups.

c. **Limited interactive system access**. Removal of non-administrative users from the computer that runs the mail server further decreases the risk of any mail server level access controls being circumvented, and may reduce the requirement for strong global file system access controls or comprehensive auditing.

d. **Email filtering**. Using an automated or manual process to filter varies executables or other content from incoming or outgoing email messages. This may require the position of an external mail relay with this capability on the email path to/from the server.

e. **Regular system maintenance**. Many of the vulnerabilities associated with email programs have been related to the release/patch level of the mail server program and have been identified and fixed by subsequent releases.

Standard Simple Mail Transfer Protocol (SMTP) mail servers do not require any form of authentication when sending mail. As such, unless digital signatures, encryption or similar technologies are implemented on top of SMTP, forging electronic mail is a very simple process. Unless the content is significantly out of character, a forged email that appears to originate from a trusted associate is almost indistinguishable from a legitimate message. Volumes of unsolicited email may intentionally or unintentionally comprise a denial of service attack against your mail server. Users may not be able to simply distinguish legitimate email messages from the mass of 'junk mail', and as such, productivity losses, or failure of critical hardware or software due to mail volume, may be experienced. Some unsolicited incoming electronic mail messages may actually contain information that is in violation of the organisational security policy, or perhaps compromise the organisation's legal obligations, such as pornography, inappropriate material. Password authentication for mail servers is susceptible to the same problems that plague normal operating system passwords, such as:

a. Network interception and replay.

b. Exhaustive password attempts.

c. Dictionary attack if the attacker has access to the mail server configuration files.

Additional security assets such as firewalls or screening routers, and content filtering systems may limit exposure to such attacks.

4. Mail Server Auditing

Audit logs produced by the mail server can be advantageous both from a security point of view, and for usage statistics. Managing audit logs is a non-trivial task that usually requires ongoing maintenance and monitoring:

a. File systems need to be watched to ensure that disk space does not fill, and therefore contribute to a denial of service situation.

b. Audit information needs to be protected by access controls so that it cannot be easily read or overwritten.

c. Audit information needs to be archived to offline storage, or removed from the file system when no longer required.

d. Audit analysis software needs to be acquired, installed, and run according to an agreed schedule.

e. The results of audit analysis need to be distributed to those who have a need to know, with the capability to recognise anomalous events. Anomalous events need to be followed up. The auditing of a mail server can result in significant benefits to the organisation, which may include:

a. Logs that can identify the source of some hacking attempts or denial of service attacks.

b. Logs that can pinpoint problems with your mail server configuration.

c. Usage statistics that can identify when an upgrade of network bandwidth is likely to be required.

A site that wishes to guard against denial of service attacks that attempt large volumes of connections to the mail server with the goal of filling the file system of the local machine may wish to consider locating the audit logging facility on a physical or logical disk device that is separate from the disk on which the primary operating system is located. If this is not possible, a form of automatic log rotation may be appropriate.

5. Data Integrity

Normal Internet SMTP mail does not offer integrity, authentication or nonrepudiation services. Some mail clients will respond to a 'return receipt' request, but this feature is optional for mail clients and implementation is not guaranteed. Most clients that allow return receipts will also ask the recipient for confirmation before sending a delivery receipt. The integrity of a mail message and its delivery can be enhanced by using digital signatures, encryption, hash exchanges, or a combination of these techniques. Encryption and digital signatures are discussed below. A hash exchange is a system whereby an original email mathematical signature is delivered to the recipient via another mail message or an alternative delivery mechanism. The mathematical signature of the received message is generated, and compared with that of the original message. If a match is obtained, the recipient can have more confidence that the message has not been modified in transit.

Sender integrity issues are also of concern. Standard SMTP mail servers do not require any form of authentication when sending mail. As such, users who either have access to the sender's mail client, or have knowledge of the SMTP protocol, can easily impersonate a legitimate user.

6. Data Confidentiality

Unless appropriate encryption technology is in use, information that is sent over a network can be intercepted and analyses at any point between the client computer and the remote recipient. Modern networks are structured in such a way that information usually passes through several network 'hops' to get from source to destination. In the following diagram, if a user on a machine on the right wishes to send an email to a user on a machine on the left, there are several places where the communication can be intercepted.

The communication between source and destination can be potentially intercepted by:

a. Any user who has physical access to the source or destination laptop or desktop computer. A user who has physical access to the source computer can consult the 'Sent' or 'Inbox' files maintained by most mail clients to examine incoming or outgoing mail.

b. Any user who has logical read-access to the mail spool owned by the sender or recipient. Some mail servers function as a mail holding area for a number of users. File system access controls should be configured to limit users to only those mail boxes for which they are authorised.

c. Any user on the source or destination local area network. A local area network usually operates in 'broadcast' mode. Each station 'shouts' over the network so that the destination host or any network devices that create a path to the network host, can 'hear' it.

d. The administrator of the source or destination router

The source router is responsible for creating a network path between the source machine and the destination machine, and as such carries the communication.

e. The administrators of any intermediate network devices such as routers or firewalls.

On an intranet, some level of trust can be safely assigned to the network devices on your network, and those staff that are performing administration tasks.

The Internet however, is a dynamic system that will re-route communications in response to degraded traffic flow or service interruption. The source machine has very little control over which path communications will flow, and as such, cannot guarantee the integrity of administrators at each network device along the path from source to destination. Encryption technology is one of the more effective mechanisms to provide data confidentiality between source and destination in an Internet or public wide area network environment. Whether or not encryption technology is employed between sender and receiver, messages are usually stored unencrypted in the Inbox of the recipient's computer, and in the Sent folder of the sender's computer. Physical security incidents such as theft of a laptop, or leaving a PC unattended in an insecure location, can therefore impact upon data confidentiality. The attacker may not be able to intercept the messages in transit, or may not be able to decrypt the messages, but accessing the mail at either the source or destination may be a viable alternative. An additional risk to data confidentiality known as 'cascading carbon copy' exists for electronic mail messages.

An original message distributed to one or more recipients often includes a wider recipient distribution in any replies due to the practice of 'info-ing' concerned parties. If the originator is not vigilant and aware of the full distribution, replying to the response may include a wider than intended distribution.

Pro-active scanning of an organisation's outgoing mail content may be required in situations where information leakage is a significant concern. Trade secrets, intelligence material, budget data, or similar information that has a high damage potential if released outside the organisation may require a lexical scan of outgoing electronic mail messages. This strategy also requires rigorous configuration of internal mail systems to ensure that message labeling is reliably implemented.

5.7 Encrypted Transactions and Public Key Infrastructure

To overcome the problems associated with lack of authentication of email, a digital signature can be attached to prove the identity of the source. Public Key certificates can also service other requirements including confidentiality and integrity. Keys and client certificates may be stored in a number of different configurations:

a. Within a user's home directory, relying on operating system access controls to determine access to the digital certificate, and providing a single-sign-on facility to a site's user base for access to the normal Page 11-8 operating system desktop and email signature and encryption.

b. Within a user's home directory, but protected using password-based authentication over and above the normal operating system access controls.

c. Within a directory server, and optionally protected using additional password authentication.

d. On magnetic media for ease of transport, and optionally protected by additional password-based authentication.

e. On a smart card, and optionally protected by additional password or biometric authentication.

Physical security issues aside, the items above are ranked approximately in order of security. More intrusion detection and access control management is required for each level in order to attain a similar level of assurance. For example, significant auditing and access control would be required to bring home-directory based certificate storage to the same assurance level as a smart card protected by biometrics.

5.7.1 Government Public Key Authority

In late 1997, the Government decided to take the lead in the development of a national framework for the authentication of users of electronic online services. The National Office for the Information Economy (NOIE) was charged with ensuring that a strategy be in place so that the Government can make optimal use of Public Key Technologies (PKT) for electronic transactions. The Government Public Key Authority (GPKA) has been established to manage the evaluation and accreditation for organisations and individuals who wish to participate in the delivery of public key technologies and associated evaluation services for government use. The GPKA will recognise two levels of Certification Authority accreditation: Entry Level Accreditation and Full Accreditation. Full accreditation involves satisfactory completion of the Entry Level requirements, and completion of the product evaluation.

5.7.2 Grades of Email Server and Client Security

The following email security grades have been included to assist in determining the level of effort that should be allocated to the task of securing mail clients and servers. They are not definitive, and when implementing security should therefore be used as a guide only. Implementation of email security will vary from organisation to organisation, depending on the outcomes of a risk assessment.

a. **Grade 0**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

b. **Grade 1**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and rotated nightly to assist with problem diagnosis and repair.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

c. **Grade 2**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and analysed for general intrusion attempts, or attempts to circumvent mail server controls. Audit logs are either rotated, or migrated to offline storage depending on results of risk assessment.

v. Mail proxy configured to virus check all incoming messages.

vi. Digital Signature and Encryption technology is available to users who wish to send mail messages with enhanced security - Public Key encryption based on x.509 certificates is used between sender and recipient to enhance data confidentiality.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

ii. Users' mail clients are configured to reject all Java and Active-X in attachments.

d. **Grade 3**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and analyses for general intrusion attempts, or attempts to circumvent mail server controls. Audit logs are either rotated, or migrated to offline storage depending on results of risk assessment.

v. Mail proxy configured to virus check all incoming messages.

vi. Digital Signature and Encryption technology is available to users who wish to send mail messages with enhanced security - Public Key encryption based on x.509 certificates is used between sender and recipient to enhance data confidentiality.

vii. Operating system accounts on the mail server are restricted to administrative users only.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

ii. Users' mail clients are configured to reject all Java and Active-X in attachments.

iii. Users' mail clients configured to reject all JavaScript and Cookies if determined appropriate by risk assessment.

iv. Application extensions to mail clients are evaluated by qualified system security staff if determined appropriate by risk assessment.

v. Laptop or other portable computing devices are purged of sensitive messages before leaving a secure area.

e. **Grade 4**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and analysed for general intrusion attempts, or attempts to circumvent mail server controls. Audit logs are either rotated, or migrated to offline storage depending on results of risk assessment.

v. Mail proxy configured to virus check all incoming messages.

vi. Mail proxy configured to scan outgoing message for sensitive information leakage.

vii. Digital Signature and Encryption technology is available to users who wish to send mail messages with enhanced security - Public Key encryption based on x.509 certificates is used between sender and recipient to enhance data confidentiality.

viii. Operating system accounts on the mail server are restricted to administrative users only.

ix. Mail servers forced by the operating system to use a virtual root - a subset of the computer's file system from which the mail server cannot escape.

x. Mail proxy configured to strip all attachments from incoming mail messages.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

ii. Users' mail clients are configured to reject all Java and Active-X in attachments.

iii. Users' mail clients configured to reject all JavaScript and Cookies if determined appropriate by risk assessment.

iv. Application extensions to mail clients are evaluated by qualified system security staff if determined appropriate by risk assessment.

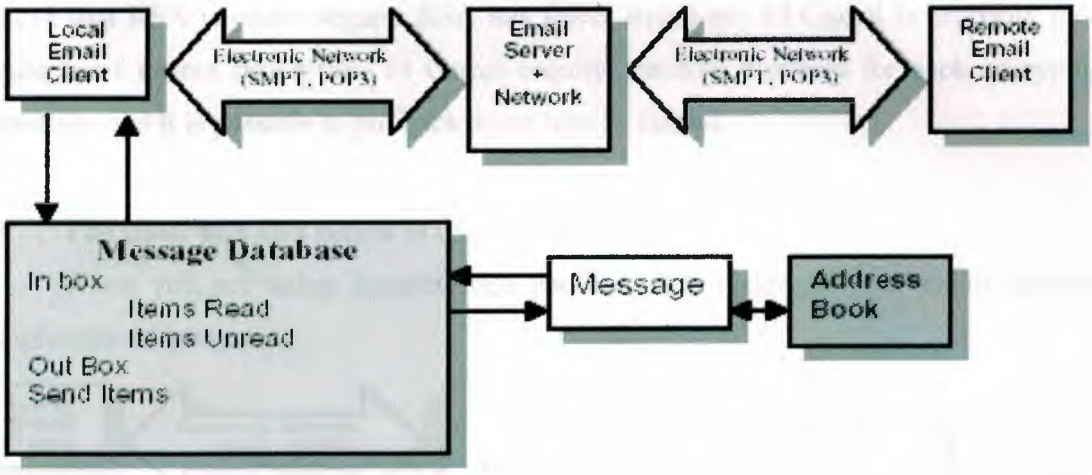
v. Laptop or other portable computing devices are purged of sensitive messages before leaving a secure area. [2]

CHAPTER 6

Making Your Email Secure

6.1 The Basic Bits and Pieces of Regular Email

Basic email works like this.



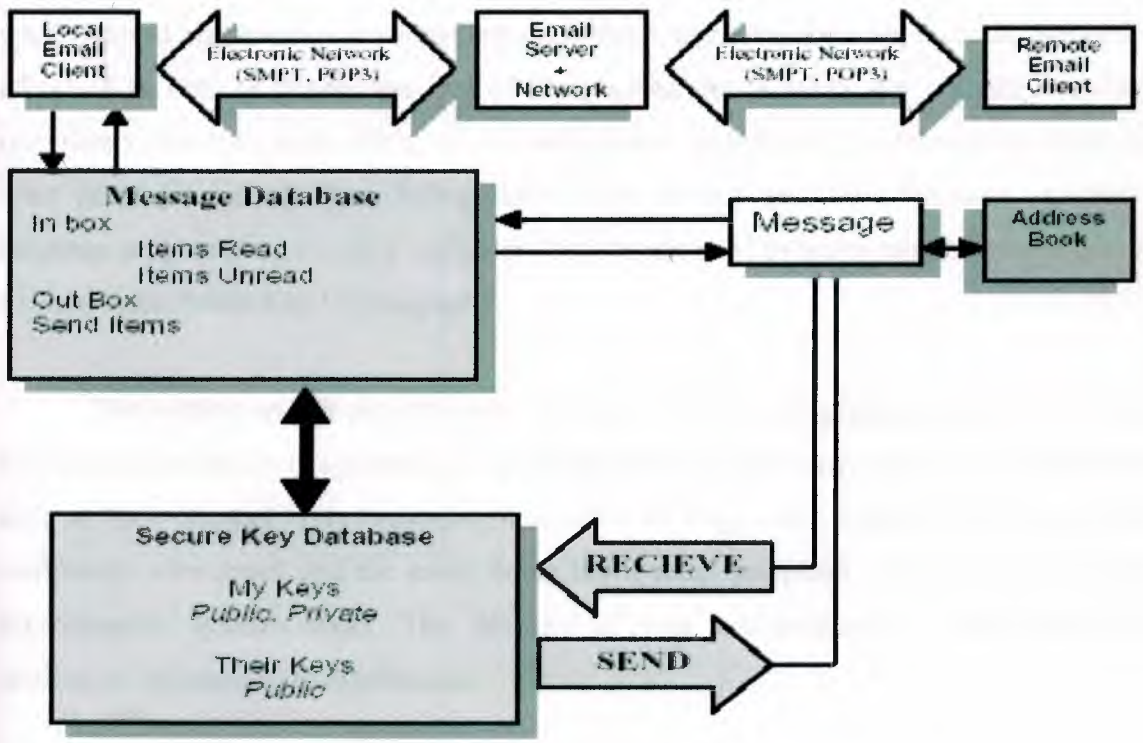
The email system is really a database system with two tables. One other table contains your "Address Book". This is a table of users that you communicate with frequently. The other table contains all of the email messages that you have sent and received. Each unit of transfer is mail message. There are two types of email messages: email that you have sent (or are intending to send) to another user, and email that you have received from other users. In addition to a program for managing your email you also use a program for writing and reading email messages. This program is your email editor and it comes with your email system. There is a program that sends your email to another user, the SMTP client program, and the Program that gets your email from the email server, the POP3 Client.

6.1.1 What exactly is an Email Key?

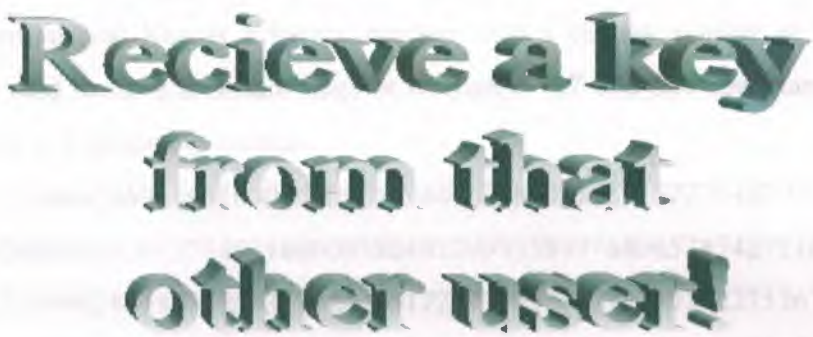
An Email Key is simply list of a few large numbers that satisfy a set of mathematical conditions. A single number in the list is the private key. The rest of the numbers are the public key. You transmit your public key to another user and then that user can use that key to send you a secret message. Since you have the private key you can read the message. Computing a private key from a public key is theoretically possible, but very difficult. It may take Billions of Years and Billions of Dollars to compute a private key from a public key. SecureOffice provides two different public key systems; El Gamal, and RSA. RSA is the default. They each have their relative advantages and disadvantages. I believe that RSA is more elegant. RSA has fewer equations. El Gamal is probably more secure but I cannot prove this. El Gamal requires random numbers for each encryption operations and it is possible to put back doors into El Gamal.

6.2 The Basic bits and pieces of encrypted email

When you are using SecureOffice another table inside of your email database complicates the picture.



Here there is a Secure Key Database. The Key Database contains two types of keys, your either make a key or you receive a key. You transmit your keys to other users. When another user has your key then that other user can transmit SecureOffice documents back to you and nobody, not even the sender will be able to open them. In order to send a SecureOffice document to another user you must first



6.2.1 The Basic Principles of Public Key Cryptography

Public Key Cryptography was invented by Whitfield Diffie at a mathematical conference at Stanford University sometime in the 1970's. Just because Public Key Cryptography was invented by mathematicians and is something that you need a pretty good grasp of mathematics to completely understand, that does not mean that you should be afraid of it. Lots of people use lots of complicated things every day without knowing completely how they work. Most people really do not understand how telephones work, or what keeps jet aircraft from falling down. You do not need to understand assembly language programming to use a computer. You do not need to understand Number Theory to understand Public Key Cryptography.

The section on file security went over symmetrical key cryptography. Public key cryptography works with symmetrical key cryptography to allow two users to communicate over an open channel Communication is secure even when the communication channel is completely wiretapped and the entity doing the wiretap completely understands how the cryptographic system works. The Security of your communication is the result of application of mathematical principles.

The math behind SecureOffice is straightforward and simple. You do not need to understand the mathematics of SecureOffice to use SecureOffice, many people are fearful of mathematics. I hope that SecureOffice makes more people interested in mathematics, but I doubt that the math problem that SecureOffice presents to humanity will ever be solved.

6.3 Public Private Keys vs. Symmetrical Keys

A symmetrical Key is a binary number with a certain number of bits. Decimal numbers are said to have a certain number of digits: 747 and 666 are examples of three digit numbers. The following number

393287487308948410696163101054205843944162281031483157276487020135227152231541442242990493436157749318000958249239993589976806528742721687968176832167513004310898248783355583274844961727773592657121553722752673523844525686803972258875545362415244188043175651445089840680352256863421989800411293580539582022704994479331336500075045211954249467628053584421375975138236475921079907572643504220275343336059851431278008707507403106601397021575734493577695769096294296266795095052346648447291145285993680177553877468518072561074604771943979752361191449699646592939970818839649108658179427676341776200863888886290195805486320931735294547912940095319700646199381692344055296452108421534395040250868560576391604244762386626964378502995688208066702529637966312302079799706812954251337137016681434390740538393347216094977090988731034395476677685028805127093134371398671997319042757814592545631 71 is an example of an 889 digit number. Numbers of this size are very typical when High Security is needed.

This number is the modulo of my Lucifer2 key and in order for an attacker to be able to read my email messages transmitted on this key they would need to factor this number into the two large prime numbers that are its factors. This is not an easy math problem to solve. A number can also be expressed as a binary number. Usually we express the binary value of a number and instead express it in base 16. The reason that we use base 16 is because it is more compact to write down and the number can be translated into binary very quickly.

When a number is expressed in hexadecimal format we use the numbers 0-9 to express numeric values 0 to 9 and the numbers a-f to express the numbers 10-15. Base sixteen is used because each hexadecimal digit is equal to four bits. It is sometimes customary to write hex numbers with the "0x" prefix in front of them in order to indicate the number base of 16.

Hex Number Table

Decimal (Base 10)	Hexadecimal (Base 16)	Binary (Base 2)
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	a	1010
11	b	1011
12	c	1100
13	d	1101
14	e	1110
15	f	1111

6.3.1 The SecureOffice has two public key systems

- Unlimited Key Length El Gamal
- Unlimited Key Length RSA

The methods are unlimited because SecureOffice imposes no maximum key size. Both of these systems require large prime numbers.

6.3.2 Setting up your Secure Key Database

Your keys are a pretty sensitive thing. You do not want anybody to be able to look at your keys. If your keys can be accessed then all of your incoming email can be accessed. In order to prevent anybody but an authorized person from reading your incoming email your keys are kept in a Secure Key Database File.

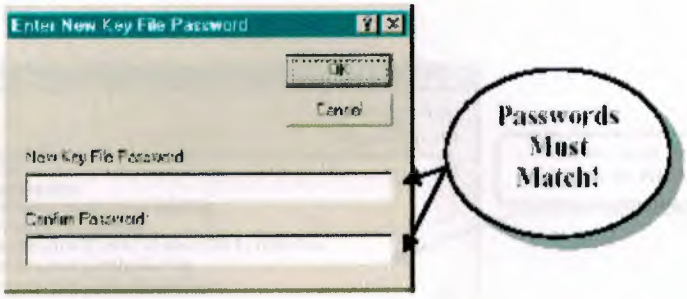
Your Secure Key database is encrypted in a very similar way to your document files. This file must be set up to store your keys. You can have more that one key database file. You must give it file a password before your can put any keys in it. Your outgoing email is encrypted with Public Keys and the Public keys don't absolutely need to be protected. When the password for the database is entered all of these keys are encrypted with the same system and the private keys. The first thing that you will need to do is to get your secure key database set up. This database uses the same triple DES encryption system that SecureOffice documents use. You must first specify the file that you are going to use for your keys. You can maintain any number of key files with SecureOffice. As long as your key file paths are unique you can manage them any way that you want. To create a new Secure Key Database go to the SecureOffice Menu and Select public Key and then Select Set Key File

Doing this will take you to the Set Key File Dialog.

You can set your key file to any valid path. For simplicity I recommend that you put all of your keys on the root of your C: director. This is simply a pointer to a key file. When SecureOffice begins an operation that requires access to a key file database then this file will be accessed. If the file is not there then the first time your access it to create a new key you must create a password for the key file.

You can use the Manage menu button to take to the Set Key New Key File Password.

This will take you to the Enter New Key File Password Dialog.



Your key file password must be typed twice, must match, and you must never forget your key file password. If you forget your key file password then the only thing you can do is to start a new one, or delete it. Your key file password contains keys. There are two types of SecureOffice Keys.

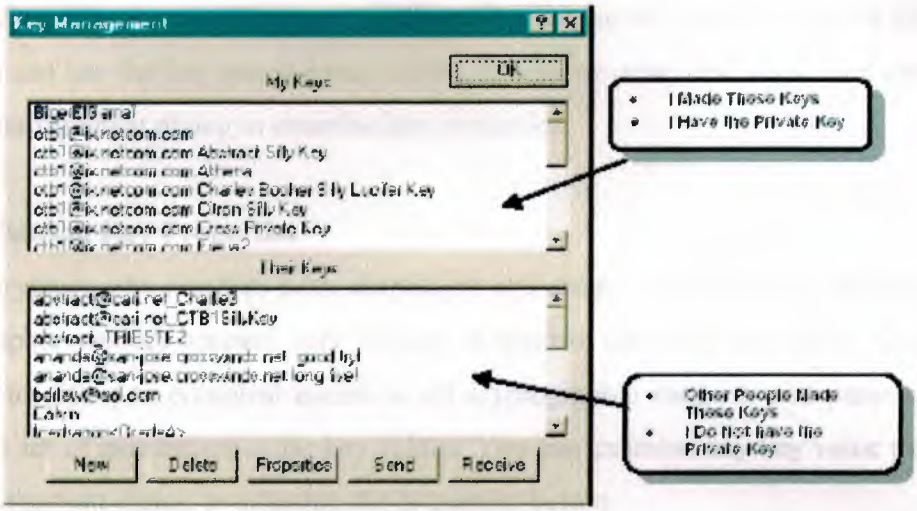
1. Keys that you have made yourself (You have the public and Private parts of the key)
2. Keys that other people have sent to you (You only have the Public Part of the key)

The Key Management dialog is a good place to manage your email keys.

6.3.3 Key Database File Format

Your key file is encrypted on a string by string basis. The Key Database is a string archive were the format is specified by 0:keystring or 1:af1c0de40a98 The first digit indicates the Encryption State of the remaining string. If the digit is '0' then the string is not encrypted. This can happen when a public key is accepted into a key database before the user has entered in the password for that key database. Usually all keys in the database are encrypted. Any unencrypted keys will be encrypted once the password for the key file is entered into SecureOffice. Private keys are never allowed to be in a not encrypted state. The first line of the Key Database is the validation string, which are 16 hex digits long. The SecureOffice key database file can be given any name and placed on any write-able media that the file system can access. The system uses the same Triple DES encryption system that normal document file uses. The same 16 bit validation hash is also encrypted. Blocks are filled in with zeros. I have not as yet written a file format viewer for this file. I may decide to create such a program if there is enough user interest.

6.4 The Key Management Dialog



This is where most key management operations can be controlled. There are two types of keys:

- Keys you made (You have the Public and Private Part).
- Keys other People have made (You only have the Private Part of the Key).

The Basic Key Operations are

1. Making a new Key
2. Deleting an existing Key
3. Examine Key Properties
4. Send A Key
5. Receiving a Key.

6.5 Save to File

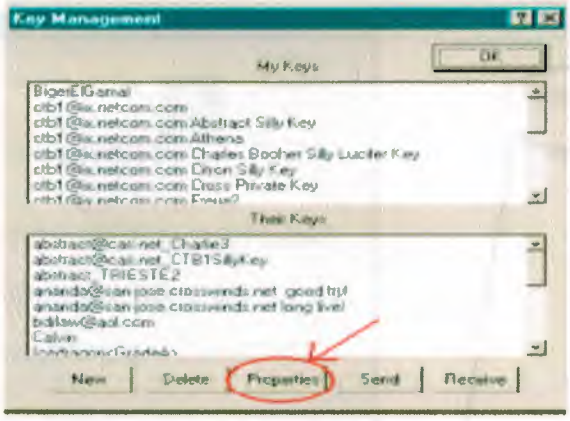
This will save the selected public key into a binary file that you can select by either typing the file name into the file text field, or by using the Browse button. This is in every way identical to using Send Mail, but the MAPI email part of the operation is dropped and the user must send the file via email attachment or some other transport system.

6.6 Key Management

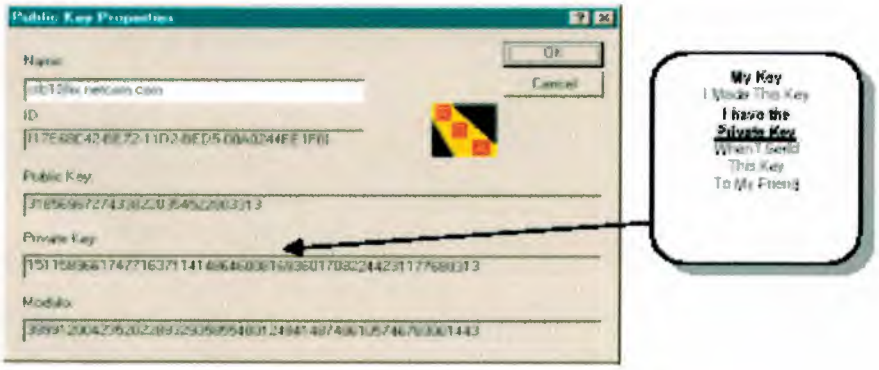
When you start communicating with lots of users in SecureOffice you will have lots of keys. Sometimes users will loose their key files so you will want to remove their public keys you can use the key management dialog to remove unwanted keys. You can also use the key management dialog to examine key properties.

6.7 Viewing Key Properties

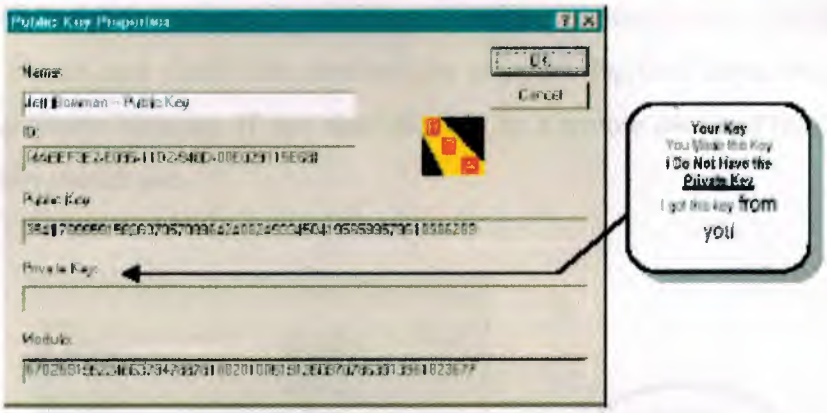
Cryptography requires both skepticism and trust. You should be skeptical of any cryptographic product because only through skepticism can trust be created. SecureOffice attempts to give you complete access to all cryptographic methods and parameters. One important set of parameters is the key values. You can examine any key value through the Key management dialog by pressing the properties button.



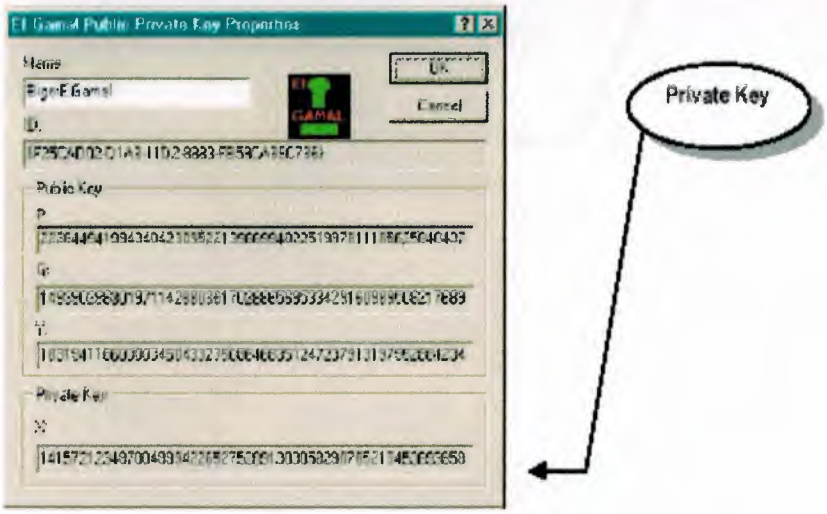
If you select one of your own RSA keys the dialog that would be presented would look something like this.



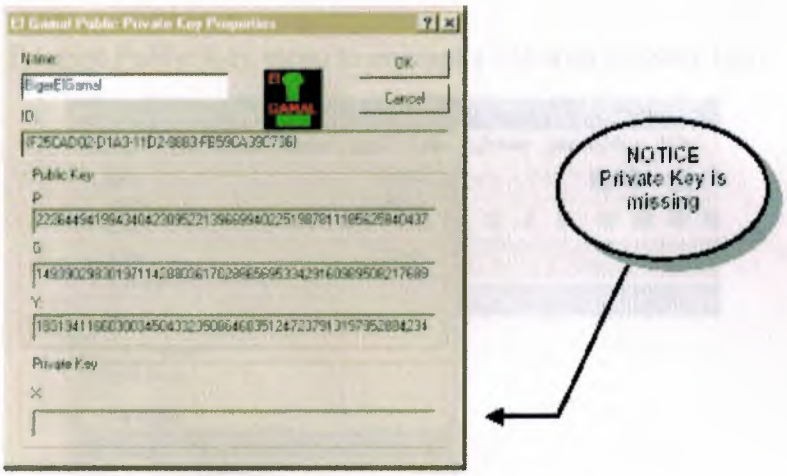
If you selected an RSA key that somebody else had sent to you and examined that key then it would not have the private key and the dialog would look something like this.



There is also a key properties dialog for El Gamal keys.



You can use these files in conjunction with the CryptView program to verify all cryptographic algorithms and file formats that SecureOffice uses. The reason that I show you these numbers is so that if you are somewhat mathematically included you can examine my results and check the numbers for yourself. Each of these numbers can be traced in a particular message. If you send this key to a remote user and they looked at it, this is what they would see.

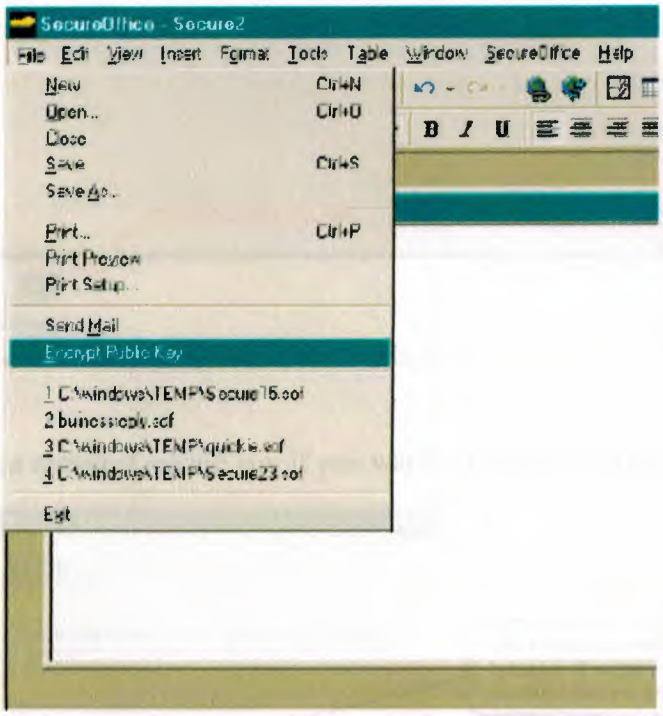


CHAPTER 7

Using of Secure Email

7.1 Sending Secure Email with older email systems

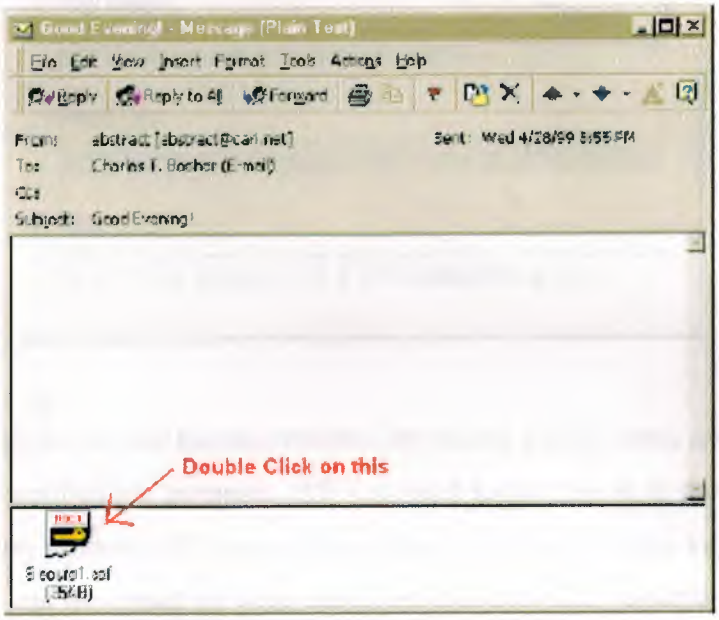
Use the file -> Encrypt Public Key menu to encrypt a file with a public key.



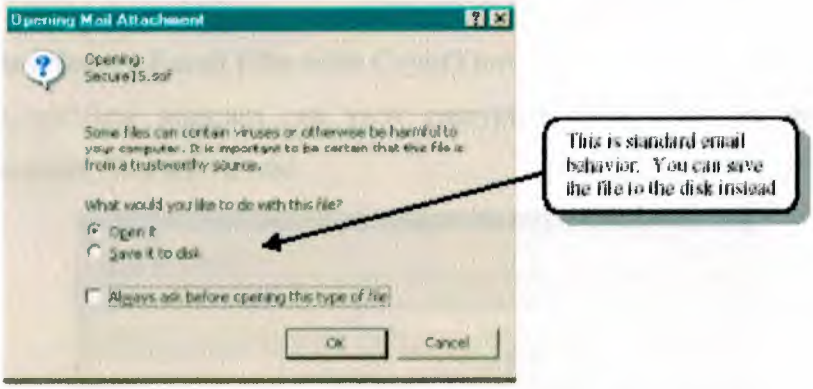
This operation is identical to the send mail operation except that you will be given a file dialog for saving the file. You can then transport this public key file to your remote use by attaching it to an outgoing email message as a binary attachment, or though some other transport systems such as a floppy though the mail system.

7.2 Reading your encrypted email

When you get an encrypted email with will be received as a normal email message. If you were using Microsoft Outlook 98 as your email system then a SecureOffice message would look something like this.

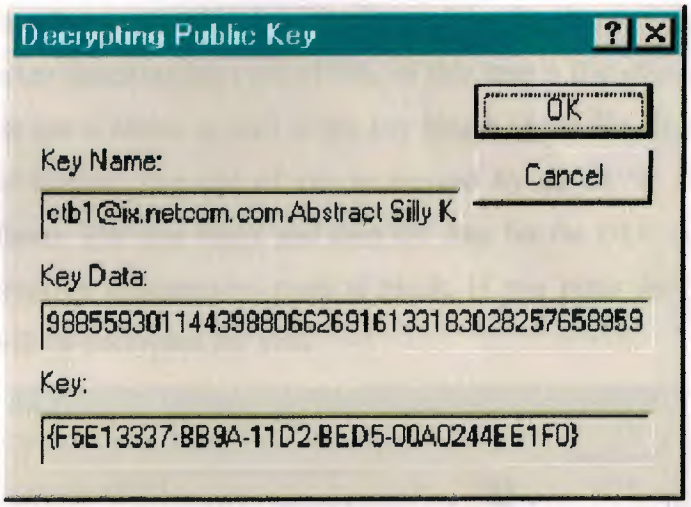


You would then get a message asking you if you wanted to open the file.



Select open it and then you will see the decryption dialog. Depending on whether or not you have provided a key file password during your current session of SecureOffice you may be asked for a key file password.

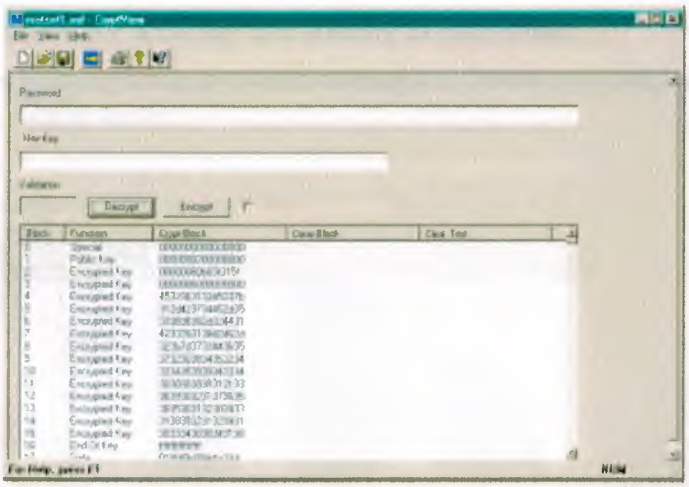
The public key decryption dialog looks like this.



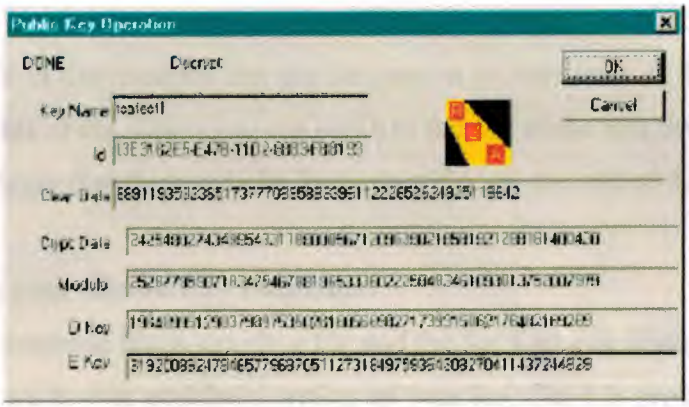
This dialog will show you the human readable key name, the key data, and the key id. This data is show for verification purposes. All you need to do here is to press the OK button and the decryption process will begin. Depending on the size of the key that your email sender has used and the speed of your computer this can take variable amounts of time. Once your message is decrypted it will be automatically opened with the appropriate OLE server application.

7.2.1 Viewing Secure Email Files with CryptView

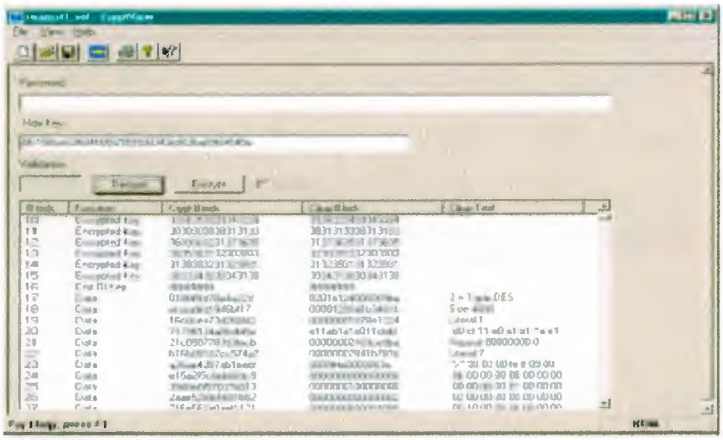
The CryptView program can view encrypted email files the same way that encrypted document files are viewed.



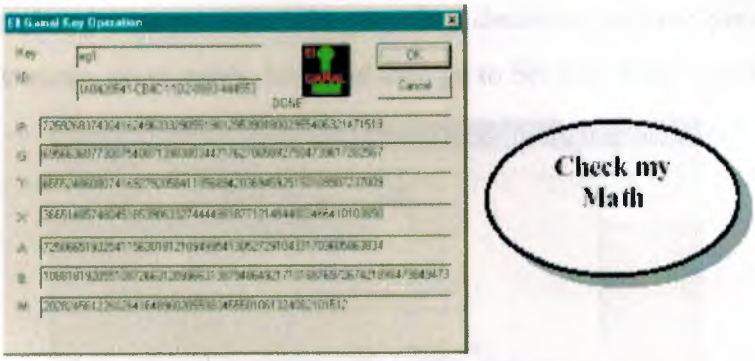
You can see each of the blocks in the file and verify those blocks using a binary file editor of your choice. There is a marker block in the front of the file that makes the file a "Special File", the next marker specifies the type of file, in this case a file encrypted with a public key. An anti tamper has is added as well as the key length of the file. The key is placed into the file in decimal format. The end of key is marked by an all '1' block and then the document data follows. The size block and then the data for the OLE server object follow the document encryption compression method block. If you press the decrypt button the symmetrical key will be decrypted for you.



This will show you all the numbers that you would need to check the math behind SecureOffice. The decryption process can take variable amounts of time depending on the size of the key that you are using and the speed of your computer. Once your key is computed you can press the OK button and it will be converted into a hexadecimal format and placed into the key line of the CryptView program. The file will be decrypted block by block and you can check for accuracy and honesty of decryption.



CryptView provides the same services for El Gamal as for RSA.



This shows you all of the numbers that the decryption process uses. If the numbers do not fit into the text fields of the dialog you can scroll to the end of the text field. In this example the B number is bigger that the text field. You can still view the rest of this number.

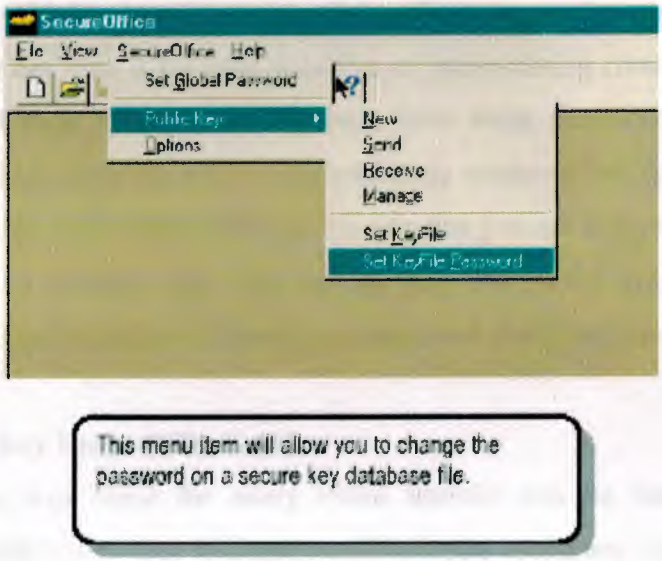
7.3 Managing your Secure Key Databases

Your Key database file is simply a file and the Set Key File Dialog simply points to a location. If you are having problems setting up your key file it is probably because your key database is set to an invalid folder. I recommend that you give your key databases simple names and put them on C:

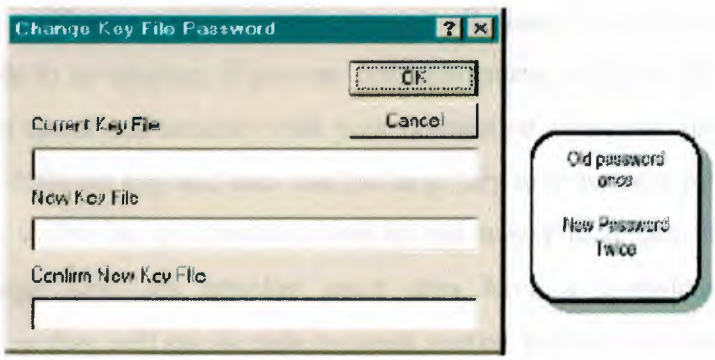
(Hint) You can make copies of your key database and move it around on floppies. Since it is a secure format you can also email it to yourself. If you forget your key file database password then you should just delete it, or use the Set Key File dialog to start a new one.

7.3.1 Changing Key Database Passwords

You can change the password on your key database anytime you wish. Use the SecureOffice file menu, go to public key, and then go to Set Key File Password.



This will take you to a dialog that will allow you to change your key file password.



In order to change a key file password you must enter the CURRENTLY EXISTING key you must enter the new password twice. If the current password does not match, or the new passwords do not match then the operation will fail. If you have forgotten you key file password then you should either delete your key file (See Set Key File Dialog), or start a new key file.

7.4 Sending Encrypted email to yourself

This sounds a little bit silly, but you should be skeptical of any cryptographic system you might consider using. Performing this exercise will allow you to see how SecureOffice works, if the algorithms are valid, and you can make your own decision on whether or not you can trust it for your sensitive or incriminating communications. Set up two key files, call them C:\test1 and C:\test2. Give them passwords and then got to C:\test1an make a key. Send the key to yourself using whatever key transport mechanism you care to use. When you receive your key, be sure that you are using C:\test2 as your key file. Send yourself a message after you get the key and switch your key file back to C:\test1. You can examine the key files and messages and check out how the system works.

7.5 Advanced Key Usage (Silly Keys)

Using large key sized for every email transfer can be time consuming and cumbersome. Wouldn't it be nice if a user could have the speed and convenience of small keys with all of the security of large keys? One method of accomplishing this is to use "Silly" keys. Silly keys are small 200 bit keys that have been transmitted on a secure channel. "Silly keys" are not really public keys at all since the public part of the key is never made visible to an attacker. If you are communicating with Gun dealers on a remote site and you want speed and security with your connection then start your session using a very large 2000 –5000 bit key and then use the large key to transmit a small key. Since the small key is not visible to an attacker there is not way that it can be broken without breaking the large key. An attacker must also have a complete history of the communications, or they will not be able to break routine traffic even when (if) they break the large key.

7.6 Public Key Ciphers

Public Key Ciphers allow two users to communicate over an open line. A little voice inside my head told me to implement two different systems just in case some idiot in a suit thinks he can claim ownership of Mathematics. I am planning a acquiring a Federal Patent for the mathematical operation of addition.

CONCLUSION

In this project I understood many things about the Internet security, web site security and their components like E-mail security, web site security.

It is seams to be a good work for computer engineering to do this kind of project to show other department how they can work for saving their time and money by making all computer component and their use are fully secure from hackers.

Under my supervisor suggestion and his guidance, I made this project as successfully one, and his help for all the time in the lecture and office.

Finally ,I would like to say what I gain from all my theoretical courses for transferring this know ledge to practical, and to help myself and my family .

REFERENCES

[1] www.filemaker.com

[2] http://gd.tuwien.ac.at/privacy/SecureOffice/soviewmanual.pdf

[3] http://www.dsd.gov.au/infosec/acsi33/HB11p.pdf