

# Zero-cost measures for personal data security

Toni Stojanovski, and Ivana Atanasova

**Abstract**— This paper describes measures to improve the security of email communication and data storage at personal computers. Any information worker can adopt the proposed measures. However, to the top management level at any institution it is strongly suggested to adopt the proposed measures. Recommendations given in this document bear no financial cost. The only investment required is that the information workers read, understand and follow this document. The zero-cost goal was achieved without compromising the level of proposed security.

**Index Terms**—Data Security, Cryptography.

## I. INTRODUCTION

Unless you take protective measures, messages you send via email can be read by third parties. If you send information via email that might be valuable to a motivated third party (government, competitor, intruder, share broker etc.), then you can be assured that your emails **are** read by **other** parties and not only the intended recipients.

Similarly, unless you take other protective measures, the data that you keep on your computer's hard disk can be accessed, read, modified, or even deleted by a motivated intruder. The likelihood that such data is accessed by unauthorised parties is proportional to the value it can bring to those parties.

Therefore, if you regularly or occasionally or even rarely send or receive emails with confidential information, or if you keep valuable and confidential data on your computer's hard disk, then you must protect them from unauthorised access.

There are two major security issues:

- All email communication is in clear. It is not encrypted. If the email communication is intercepted, which is not a significant technological challenge, then the email messages and attachments can be read and even modified before they reach the intended recipient.
- Files with possibly confidential and valuable data are kept in clear form on local hard disks. Domain administrators have full permission to all folders and files on all computers in the domain. Though the domain administrators are trusted employees of many years, this is not a desirable situation from a security viewpoint. Furthermore, if a breach of security occurred, then the domain administrators would find it quite difficult to prove their innocence.

In this paper we propose, justify and describe following

T. Stojanovski is with the Faculty of Information Technology at EURM (phone: +389 2 320 2159; fax: +289 2 320 20 30; e-mail: toni.stojanovski@eurm.edu.mk).

I. Atanasova is with the Faculty of Information Technology at EURM (e-mail: ivana.atanasova@eurm.edu.mk).

security recommendations:

- Privacy, integrity and authenticity of email communication and storage of emails should be protected by means of digital certificates.
- Data on your computer's hard disk should be protected from unauthorised access. For this purpose we suggest that the Encrypting File System (EFS) is used. Protection via EFS is available on Windows 2000 or later versions of the Windows operating system. We also point to the files and folders which are common candidates for protection.
- Protect your MS Office documents with passwords. Require a password to open a MS Office document to prevent unauthorised users from opening a document at all. Password-protected documents are saved in encrypted form.
- Restrict access to files and folders on your computer's hard disk. Disallow access to folders which contain confidential data to all Windows account except your own account. Remove administrator access to your files.
- Protect valuable data on your USB drive by encrypting the folders or the whole USB drive. There are numerous freeware applications which are indented for USB drive data protection. In this paper, we presented how to encrypt your USB data with the application "USB Disk Pro Security".

## II. INSTALLATION OF A SERVER CERTIFICATE

You first need to install the digital certificate of the Certificate Authority that will issue your digital certificate and the digital certificates for the people you will exchange emails with. Once you install CA's digital certificate as a trusted certificate authority, you will be able to check the validity of all digital certificates issued by that CA. For example, you can check the authenticity of a digital signature and a digital certificate sent to you in an email.

For following reasons, we recommend that **Ascertia** certificate authority (<http://www.ascertia.com>) is used:

- **Ascertia vs. other CAs:** Ascertia offers free digital certificates which can be bound to person's email, name, surname and company. CACert and Thawte certificate authorities also offer free digital certificates, but they can be bound to person's email only. Other personal details such as name, surname and company can not be included in the digital certificate.
- **External vs. internal CA:** Windows 2000 Server and Windows 2003 server include Microsoft Certificate Server which can be used to issue digital certificates. Similarly, MS Exchange can be used to issue digital certificates and to also distribute the public keys from the digital certificates. However, maintaining an internal CA is not a simple task, requires specialised knowledge, and will increase the burden

on the internal IT team. Using an external CA does not introduce any security issues compared to the use of an internal CA.

You need to install Ascertia's root certificate as a trusted certificate authority.

### III. INSTALLATION OF A PERSONAL CERTIFICATE

Generating a personal digital certificate requires that an ActiveX control named "**CEnroll Class**" is installed on your computer. You need to make sure that the Security settings on your Internet Explorer satisfy the following requirements:

- Downloading and installation of Signed ActiveX controls is enabled
- Executing and scripting of ActiveX controls is enabled.

In order to satisfy the first two requirements, you can either change the settings of the zone Internet, or temporarily add web site [www.ascertia.com](http://www.ascertia.com) to zone **Trusted Sites** as follows.

Additionally, in order to be able to install your digital certificate it is required that you have enough permission on the system to install softwares and Controls. If your account does not have such permission, then you need to talk to your system administrator to install the ActiveX control "**CEnroll Class**" for you.

Next you need get your personal digital certificate from <http://www.ascertia.com>. Make sure the email address you write in the forms is the same email address for which you require the certificate. The issued personal digital certificate can be used to sign emails that you send from the specified email account only. We recommend that you choose the following settings for your digital certificate

- Certificate Type: Email Protection Certificate
- CSP: **Microsoft Strong Cryptographic Provider**
- Key usage: **Both**
- Key size: **1024**

By default, the security level for your DC is set to Medium. Later on you will see how to increase the protection of your digital certificate. Note that the private and public keys are generated on your computer using the ActiveX control "Microsoft Certificate Enrolment Control". Private key is not sent nor is known to Ascertia CA.

### IV. SEND DIGITALLY SIGNED AND ENCRYPTED EMAILS

You can use your Free Digital ID (Certificate) to securely send email using Outlook Express, Outlook 2000 and Outlook 2002.

#### A. Checks

First you need to perform the following steps to check that you email client MS Outlook is set up correctly. In MS Outlook, select the menu item **Tools** → **Options**. Select the tab **Security**. Make sure that the top three checkboxes are checked.

- Encrypt contents and attachments for outgoing messages
- Add digital signature to outgoing messages
- Send clear text signed message when sending signed messages




These settings ensure that by default your email communication will be digitally signed and encrypted. Later on, when using MS Outlook, you can choose not to sign or encrypt an individual message before it is sent.




Alternatively, if you rarely send protected emails, then you can leave the first and second check boxes unchecked. Then by default your emails will be sent not signed and not encrypted. Still, you can choose to encrypt or sign individual emails.

Click on the button "**Settings**". In the new window ensure that **SHA1** is the selected hash algorithm, **3DES** is the selected encryption algorithm, and **Send these certificates with signed messages** check box is checked. The last setting ensures that the public part of your digital certificate will be sent as an attachment to your messages, and then the recipient will be able to encrypt the messages sent to you. Click on the button **OK**.

#### B. Send digitally signed and encrypted emails


You can send email in the usual way. For example, you can select the following menu item **File** → **New** → **Mail Message**. Note that in the New Message window, the two

options   on the right hand side in the toolbar are selected.  means that the message will be digitally signed,

while  means that the message will be encrypted. If you don't need or don't want the message to be signed or encrypted, simply click on the item  or  in the toolbar and unselect it, respectively.

Clearly, email will be **signed** with **your** digital certificate, and encrypted with the recipient's digital certificate.



### V. RECEIVE DIGITALLY SIGNED AND ENCRYPTED EMAILS

In order to receive encrypted emails, you first need to send the public part of your digital certificate to your contacts. Please note that in the following new **Message** window, the toolbar item  is selected. This email will be digitally signed with your digital certificate, and will also contain the public part of your digital certificate as an attachment.

After receiving the above email, the recipient can start sending you encrypted emails.

Note that received encrypted email can not be viewed in the preview pane, as shown in the following picture.

You need to open the item in order to read its contents.

Following icons   indicate that the message is encrypted and digitally signed.

Even after you open the encrypted mail and view its content, the email stays on the MS Exchange server in encrypted form and thus protected from an unauthorised access. For example, even if your System Administrator can access the MS Exchange database or impersonate you when accessing MS Exchange., he/she can not read your emails.

## VI. DEFINE DIGITAL CERTIFICATE FOR YOUR CONTACTS

In order to send an encrypted email to a recipient, you need to have the public part of the recipient's digital certificate. If you try to send an encrypted email to a recipient whose digital certificate (the public part) you do not have, then you will be prompted with this warning.

You can either click on **Send Unencrypted** and send the message in clear text, or click on **Cancel** and don't send the message.

You have to take the following steps in order define digital certificates for your contacts and thus to become able to send them encrypted emails.

1. Your first need to receive a message signed by your contact. Note the following section from the message. It means that the message is digitally signed.

Signed By: toni\_stojanovski@hotmail.com

2. Right mouse click on the sender will open a pop-up window. Click on **Add to Outlook Contacts...**
3. If the sender's digital certificate is included in the message, then that digital certificate will be assigned to the sender's contact details. In the following window, click on the tab **Certificates**, and confirm that there is a digital certificate for the contact. Click on the button **Save and Close**.

## VII. HOW TO PROTECT YOUR DIGITAL CERTIFICATE

When you start using a digital certificate, you lose a bit of convenience:

- You can not view an encrypted email in the preview window.
- If you lose your digital certificate, then you can not access the emails that were sent to you in an encrypted form.
- You have to protect your digital certificate, as explained below.

But this loss of convenience is for a good reason, namely, an increase in security. You will use your digital certificate to protect your email communication, and to prove your identity. If your personal digital certificate gets stolen, then the thief can impersonate you and send emails and digitally sign them in your name. Your digital certificate represents your identity on all transactions where you use your private key. You should protect your private key in the same way you would protect other vital information that impacts your identity, such as the PIN number you use to access an automated teller machine.

If you lose the key to your house, then you can't open the door. You can call a locksmith, and he will break the lock, install a new lock and give you the new key. It is a bit different with the digital certificates: if you lose your digital certificate, then your encrypted emails can not be recovered and they are lost forever. There is no locksmith for digital certificates.

### A. Password protection [7]

Storing a certificate in a web browser program such as Internet Explorer is not a secure method of storage. Other users of your computer can potentially access your certificate

when you are away, and your certificate can be easily lost if something happens to your computer.

Certificate passwords protect your certificate while it is stored in your browser. When a password is enabled on a certificate, the browser requires you to enter the password every time you use your certificate. By default, in Internet Explorer browser, password protection is not enabled for stored certificates. You must manually enable certificate password protection.

At the end of the installation process for a personal digital certificate, your certificate is installed, but not yet password protected. To password protect your certificate perform the following steps:

1. In Internet Explorer, click on Tools, then Internet Options. The system displays the Internet Options screen.
2. Click the Content tab then click the Certificates button in the Certificates section of the screen. The system will display the Certificates screen.
3. Highlight the certificate you want to password protect by clicking it once, then click the Export button.
4. The system will display the Certificate Export Wizard window. Click Next.
5. Place the radio button in Yes, Export the Private Key then click Next.
6. Remove check marks from all check boxes and click Next.
7. Enter a certificate export password in both password fields, then click Next.
8. Click the Browse button. Navigate to your desktop then choose and enter a filename for the exported certificate, and then click Save.
9. Click Next then click Finish. You should receive a message stating, "The export was successful". Click OK. The system will re-display the Certificates screen.
10. Highlight the certificate you just exported and click Remove. The system will prompt you to confirm that you want to delete the certificates, click Yes. The system will delete the certificate and re-display the Certificates screen.
11. Click the Import button. The system will display the Certificate Import Wizard window. Click Next.
12. Click the Browse button, navigate to your desktop, select the certificate you just exported, click Open, then click Next.
13. Enter in the certificate export password you chose earlier, place check marks in **both** check boxes, then click Next.
14. Click the Next button twice, and then click the Finish button. The system will display the Importing a New Private Exchange Key window. Click Set Security Level. Select the High option and then click on the Next button.
15. The system will prompt you to enter the password information you will use to access your certificate.
16. In the Password for: box, type in a name that Internet Explorer will use when prompting for a password to use with your certificate. In the Password: and Confirm: boxes enter the password you will use to protect your certificate. Click on the Finish button.
17. Click on the OK Button. You should receive a message saying, "The import was successful".

Your certificate is now password protected. Every time you use it, you will be prompted to enter the password you chose in step 16. You may safely delete the certificate file on your desktop or move it onto backup media for recovery purposes.

### B. Backup [7]

You should make a backup copy of your private key to protect yourself from loss through a hardware failure. If the hard drive on your computer failed and your private key were lost, you would no longer be able to decrypt information that was encrypted with your certificate.

It is especially important to create a backup copy of your certificate since you will use it to encrypt communications. Because your private key is stored separately from your certificate, is known only to you and is in your sole possession, it cannot be replaced if it becomes lost or damaged. Without the private key, it will be impossible to decrypt any messages that have been sent to you in an encrypted format. Therefore, you should create a copy of your certificate and private key. If you are using Netscape or Microsoft browser versions 4.X or later, your browser currently supports certificate export and import. This is also useful if you want to install your certificate on multiple computers.

Following are the steps to export your digital certificate to a file:

1. In Internet Explorer, go to the Tools->Internet Options menu.
2. Choose the Content tab.
3. Click on Certificates.
4. Highlight the certificate that you want to backup.
5. Click the Export button.
6. The Certificate Export Wizard will guide you through the rest of the process (steps 4 through 9 from the previous section).

Your digital certificate is now exported to a file and password protected. Store the file with the digital certificate to a physically secure place. The file will be encrypted using the specific password you supply. You must know this password in order to use the exported certificate. Should someone obtain your exported certificate file without your knowledge, the file is useless without the password. Remember this password. If you forget the password, no one can help you to recover the password and your digital certificate.

## VIII. KEEP YOUR DATA SAFE [3]

### A. Encrypt your data with Windows XP Professional

Anyone who accesses your computer is also able to access your files or folders. Windows XP Professional gives you the power to help keep your files and folders safe from unauthorized access by means of encryption.

You are a business executive and keep confidential data on your laptop or desktop computer. You take your laptop with you everywhere, or you leave your desktop at work after business hours. Maintaining the privacy of your business' confidential data is critical to the success of your business and your reputation. You already have a firewall and antivirus software installed on your computer, but these only protect

you from attacks on the Internet. What happens to your confidential files if your laptop is lost or stolen or your desktop is accessed while you are at home? Losing your computer doesn't have to mean losing your privacy. With Windows XP Professional, you can help protect private customer and financial information by using its Encrypting File System (EFS).

When you encrypt a file or folder, you are converting it to a format that can't be read by other people. A file encryption key is added to files or folders that you choose to encrypt. This key is needed to read the file. Windows XP Professional makes the encryption and decryption process easy—simply follow the steps below to encrypt your files or folders. When you are logged on to your computer, you'll be able to read them. Anyone who tries to use your computer without your logon will not be able to read them.

**Note:** Make sure you have your computer set up so that you have to log on to use it (when you start up, or when you have been away from the computer for a little while). If the computer is stolen when you're logged in, your encrypted files will be readable, and the encryption can be turned off. Lock the computer when you are away. Turn on the password protection for your screen saver.

EFS uses an encryption attribute to designate files for EFS protection. When a file's encryption attribute is on, EFS stores the file as encrypted cipher text. When an authorized user opens an encrypted file in an application, EFS decrypts the file in the background and provides a plaintext copy to the application. The authorized user can view or modify the file, and EFS saves any changes transparently as cipher text. Other users are denied permission to view or modify EFS-encrypted files. EFS-protected files are bulk encrypted to provide confidentiality even from intruders who bypass EFS and attempt to read files by using low-level disk tools.

Upon encrypting data, the EFS service automatically creates user's EFS certificate that ties to a private and a public key of the user. Then EFS pseudo-randomly generates a file encryption key (FEK). The system uses FEK and the Data Extended Standard X (DESX) algorithm to create the encrypted file and write it to the hard disk. The system then encrypts FEK with your public key and stores it with the encrypted file. When you access the encrypted file, the system uses your private key to decrypt the FEK and then uses the FEK to decrypt the file. When you use EFS for the first time, the system automatically generates a public/private key pair if one doesn't already exist. If you're logged on to a domain, the public/private key pair resides on a domain controller (DC); otherwise, it resides on the local machine.

NTFS stores a list of encrypted FEKs with the encrypted file in special EFS attributes known as Data Decryption Fields (DDFs) and Data Recovery Fields (DRFs).

When EFS encrypts a file, it does the following:

1. Generates a bulk symmetric encryption key.
2. Encrypts files by using the bulk encryption key.
3. Encrypts the bulk encryption key using the EFS user's public key.
4. Stores the encrypted bulk key in a special field called the data decryption field (DDF), which is attached to the EFS file.

EFS can then use the user's private key to decrypt the bulk encryption key and decrypt the file as necessary. Because only the user has the private key, others cannot unlock the DDF.

EFS's key-storage mechanism is based on W2K's CryptoAPI architecture, which stores users' public and private keys separately from the randomly generated FEK. This setup lets users store their private keys on secure devices (e.g., NTFS volumes, smart cards).

You need to take the following steps in order to encrypt files or folders:

1. Click **Start**, point to **All Programs**, point to **Accessories**, and then click **Windows Explorer**.
2. Right-click the file or folder that you want to encrypt, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. Select the **Encrypt contents to secure data** check box.

When you add new files and subfolders to an encrypted folder, they will be automatically encrypted.

Here is a list of recommendations on using encrypted files:

- Names of files stored in an encrypted folder will appear in green type. You access these files in the same way that you access any unencrypted file.
- While you are editing a file in your encrypted folder, it becomes unencrypted. When you save the file in the folder again, it is re-encrypted.
- The encryption is based on your account for your computer. Should you want to change your password, you **must** change it through the Control Panel (Users, Change Password). Never reset your password using any other method or **you will no longer be able to access your encrypted files**.
- To share an encrypted file with someone, you can copy the file to a removable media device such as a CDRW (rewriteable CD), a USB flash drive, floppy disk, or a Zip disk. When you copy the file to the removable media, the file is automatically decrypted and stored. Since the file(s) on the removable media are no longer encrypted, you should take measures to protect them. Lock the media in a secure location after use or wipe the removable device's contents.

We recommend that you encrypt the **My Documents** folder and store all sensitive data inside that folder. If you store sensitive data in other folders, then you need to encrypt these folders too.

By default, **AutoRecover** option in MS Word is turned on. While you work on a document, MS Word saves the document every 10 minutes to the following folder: **C:\Documents and Settings\<UserName>\Application Data\Microsoft\Word\**. It is recommended that you encrypt this folder too.

When you receive an email attachment and open it inside the Message preview window, the attachment is saved to a temporary folder and then is open by the appropriate application. You need to encrypt this temporary folder too. By default, the path for the temporary folder is **C:\Documents and Settings\<UserName>\Local Settings\Temporary Internet Files**.

Because encryption is an attribute, you must have write permission to encrypt a file or folder. But even if you have

write permission, you cannot encrypt files or folders in the systemroot folder (for example, %systemroot%\Notepad.exe or %systemroot%\System32). You also cannot encrypt files or folders that have their system attribute set. If these types of files and folders could be encrypted, it might render the system useless. This is because many of these files are needed for the system to start up, and decryption keys are not available during the startup process to decrypt them. If you attempt to encrypt a file or folder in the systemroot folder or that has its system attributes set, the encryption attempt fails and an error message appears.

#### *B. Encryption File System file sharing*

In Windows XP, EFS supports file sharing of encrypted files among multiple users. With this support, you can give individual users permission to access an encrypted file. The ability to add additional users is restricted to individual files. You cannot encrypt a file for multiple users in Windows 2000. Support for multiple users on folders is not provided in either Microsoft Windows 2000 or Windows XP. Also, support for the use of groups on encrypted files is not provided by EFS.

After a file has been encrypted, file sharing is enabled through a new button in the user interface. A file must be encrypted first and then saved before additional users can be added. Users can be added either from the local computer or from the Active Directory directory service if the user has a valid certificate for EFS.

#### *C. Recovery Agents*

To prevent data loss, you should have a designated recovery agent. A recovery agent is an entity who has a backup copy of the encryption key and can decrypt files for you if you ever lose your encryption keys. The local Administrator account is automatically a recovery agent for the machine. If a user locks them out of an encrypted file, the Administrator can log in, take ownership of the file, grant them access to the file, and then remove the encryption bit or use the Cipher command to decrypt the file.

In Microsoft Windows 2000 EFS, the built-in Administrator account is used as the default recovery agent. In Windows XP Professional, the EFS recovery agent's recovery certificate is not set as the default. This configuration change prevents a malicious attempt at decrypting by using the Administrator account. In systems that are upgraded from Windows 2000, the Administrator account that is set as the default recovery agent is migrated and is used as the default EFS recovery agent.

#### *D. Protect your encrypted data*

Almost all of us have encountered a situation where it was necessary to fully reinstall Windows. This may have been due to the operating system's functioning being disrupted by software failure, a virus attack, or a mistake made by an inexperienced user, the system password for a user account was lost or a user profile was deleted. In this case, all encrypted data in the old configuration would most likely be lost.

Consider the following typical scenarios:

- **The system is not booting due a component having been replaced or failed or due to operating system failure.** For example, the motherboard is out of order, the boot sector is damaged, system files are corrupted, some “half-baked” updates or a different unstable piece of software was installed. In this case, the hard drive can be connected to a different computer and the data can be read off it, but if it is EFS encrypted, this would not work.
- The system administrator at the company or the user has reset the user password. In this case, access to EFS-encrypted data would also be lost.
- **The user profile was deleted.** In this case, the files (and the user keys) may still be on the disk, but the system cannot see them, even if the user is recreated with the same name, a different ID will be assigned to the account, which is used in the encryption process. In this situation, access to the data encrypted using EFS will also be lost.
- **The user is migrated to a different domain** (is authenticated through a different server). If the user encryption keys were stored on the server at the times of the migration (usually this is the case), then an unprofessional migration can result in the loss of access to the EFS-encrypted data.
- **System reinstallation.** In this case, access to EFS-encrypted data would naturally be lost. If a backup copy of the entire system disk is made at the time, or at least of the user profile (“Documents and Settings”), then access could be restored with the use of special software, but only if the keys are not damaged.

It should be said that there is a straightforward way to avoid this situation, if before using EFS the EFS Recovery Agent is set up, but this, just like the workings of EFS in general, are too complicated for the average user.

#### *E. Software solution for accessing your encrypted data*

The typical situation in which access to EFS-encrypted data is lost takes place when the connection between the operating system and the keys physically located on the disk is lost. In this case do not give up, there is a solution. There is high probability that access to the data can be restored. But if the keys had been deleted from the disk and no backup copy of the user profile or the user’s certificates had been made, then the data is indeed unrecoverable.

Practice shows that even the export/import of the profile or the certificates proves to be effective: the keys do reappear in the system, but access to the encrypted data is not restored.

If you find yourself in this situation and the EFS-encrypted data has become inaccessible despite the keys having been saved, then it is possible to use a specialized piece of software, which is highly likely to help restore access to the data.

Here we will try to describe the various possible actions that could be taken in this situation. You have a few options:

1. Boot using the working user account with administrator privileges, if it exists, and continue with the installation of the special decryption software.
2. Physically disconnect the hard drive and install it on a different workstation running decryption software.

3. Boot up using a different operating system, installed on the same machine, if it is installed, or install it specifically for this purpose.

Most importantly, you need to gain direct access to the disk. If following the first route, this is possible only for users with administrator permissions. This is why when the backup/working user account is insufficient you can try to expand the account permissions.

Once direct access to the disk has been obtained, it is possible to move on to the next step – directly decrypting and restoring the data. This can be done according to the following plan:

1. Search for and try to decrypt all keys on the hard drive of the problem computer.
2. Search for encrypted files on the hard drive and try to decrypt them.

One of the most effective tools, designed to decrypt EFS-protected data, is the Advanced EFS Data Recovery tool. EFS Data Recovery (AEFSDR) is a specialized software program for decrypting files, encrypted using EFS technology in Microsoft Windows 2000, Windows XP, Windows 2003 Server and the new Windows Vista environments.

#### *F. Encrypt your USB data*

Encrypting your data on your computer, you have protected it from being accessed from your computer from an intruder. However, when copying or moving it on USB drive or to another computer, the encryption attribute does not apply. Another way of protecting valuable data that you save on your USB drive is by encrypting the folders or the whole USB drive.

There are numerous freeware applications which are intended for USB drive data protection. Here we present how to encrypt your USB data with one of the many applications offered online.

The application used in this document is “USB disk Pro Security”. This application partitions the disk into two partitions, for which one of the partitions is 1.44MB, same size as a floppy drive; and depends on the flash memory; the rest of the capacity is allocated for normal use. The application has several useful features:

- Allows the user to set own password, and change it later on.
- Allows the user to enter “Password Hint”, in case password is forgotten.
- Automatically format the HDD part of the USB Disk Pro when enter wrong password 6 times.

When using USB Disk Pro with the security application program, only **one** USB Disk Pro is allowed at once. Do not plug in two or more usb disk pro at the same time.

After you set a password, when you remove the device from USB port and re-insert it again, the device will automatically be locked. If you try to access it, it will reply with some error message (depending on the operating system, the error message will be different).

Before you can access the HDD part of the USB Disk, you must “Unlock” first which requires you to enter the password.

You only have **six** chances to enter password correctly. If you enter wrong password six times, it will automatically **format** your HDD part of your USB Disk, and all data will be lost.

If you no longer want to use the password, you can disable the password, and remove the protection.

As a human being, we all forget things from time to time, so when you setup/change your password, you can also edit a "Password Hint" of your choice, in case you forget your password.

#### IX. PASSWORD-PROTECT MS OFFICE DOCUMENTS

Microsoft Office documents can be protected with passwords. For example, you can require a password to open a file to prevent unauthorized users from opening a document at all. Password-protected documents are saved in encrypted form.

When you create a "password to open" document, write the password down and keep it in a secure place, or simply remember it. If you lose the password, you cannot open or gain access to the password-protected file.

Passwords are case-sensitive and can contain any combination of letters, numerals, spaces, and symbols. Use strong passwords that combine upper- and lowercase letters, numbers, and symbols. Use a strong password that you can remember so that you don't have to write it down. Perform following steps to password-protect a MS Word 2007 document.

1. After opening the file, click on the menu **Office Button ->Prepare->Encrypt Document**.
2. In the **Encrypt Document** dialog, type a password, and then click **OK**.
3. In the **Confirm Password** dialog, type the password again, and then click **OK**.

MS Word 2007 uses AES 128 encryption algorithm.

#### X. RESTRICT ACCESS TO FILES AND FOLDERS

On Windows XP you can set file permissions to specify who can access which files and folders. Then only you and those you give permission to can touch your documents. And the permissions apply whether your computer is accessed across your network or by another user sitting at your keyboard logged into his or her account.

By default, only your user account and any user with a Computer Administrator account can access your files. To limit access to your files and folders, you need to remove administrator access.

By default, all Computer Administrator accounts have access to all files on your computer. You can never completely block this type of user, because administrators can take ownership of files and then grant them permission. However, you can remove this permission to make it more difficult for them. You can also restrict other users from accessing your files.

To remove Computer Administrator access to your files you need to perform following steps.

1. Start Windows Explorer. Select the folder or files you want to set permissions for, e.g. My Documents folder.
2. Right-click the selected folders and files, and then click **Properties**.
3. Click the **Security** tab. Click the button **Advanced**.
4. Clear the **Inherit from parent the permission entries that apply to child objects** check box.
5. In the **Security** dialog box, click **Copy**.

6. In the Permission entries list, click Administrators. Click on the button **Remove**. Repeat this for all other users or groups that must not have access to the folder or file. Note that Windows XP uses the SYSTEM account, so you shouldn't remove it.
7. Once all unauthorized users and groups are removed except for your account, click on the button **OK**.

Now only you can access the files in the **My Documents** folder.

#### XI. CONCLUSION

This paper recommends a number of steps to protect the privacy of you data when you send them or receive them via email, and when you store them on your computer or external media.

These measures bear no financial costs. The only requirement is that the end-users are properly trained and obliged to use them, which is not a simple task.

#### BIBLIOGRAPHY

- [1] <http://www.udel.edu/topics/encryption/windows.html>
- [2] <http://www.computerhope.com/issues/ch000705.htm>
- [3] <http://www.microsoft.com/windowsxp/using/security/learnmore/encryptdata.mspx>
- [4] [http://www.comodo.com/products/certificate\\_services/email\\_certificate.html](http://www.comodo.com/products/certificate_services/email_certificate.html)
- [5] <http://www.ascertia.com>
- [6] <http://www.verisign.com.au/repository/tutorial/digital/intro1.shtml>
- [7] <http://www.digisigtrust.com/support/instruction/cpi.html>
- [8] <http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/dataprot/w2kadm21.mspx>
- [9] <http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>
- [10] <http://www.microsoft.com/windowsxp/using/networking/security/permissions.mspx>

**Toni D. Stojanovski** was born on 22nd of February 1968 in Skopje. He received BSc in Electrical Engineering in 1990 and MSc in Electrical Engineering in 1995 from Sts Cyril and Methodius University, Skopje, Macedonia with major in Telecommunications. His doctoral research was done at the Centre for Advanced Technologies in Telecommunications, RMIT University, Melbourne, Australia from 1996 to 1998. In 1999 he received his PhD degree.

From 1998 to 2006 he worked in a number of Australian and international software development companies in Melbourne. After working for a year as an independent consultant, in 2007 he joined European University, which is the first private university in Macedonia, as an assistant professor. His areas of research include information security and software engineering.

Prof. Stojanovski is an IEEE Member, an initiator for the creation of Standardization Technical Committee on Information Technologies in Macedonia, and a member of the National Council for Information Society. He serves as a reviewer for IEEE Transactions on Circuits and Systems I.

**Ivana Atanasova** was born on 15th of March 1987 in Kavadarci. She received graduate degree in Software Engineering in 2008 from European University, Skopje, Macedonia.

From 2005 to 2008 she had several practical experiences in a number of software development companies in Kavadarci and Skopje, Macedonia. After getting her graduate degree in 2008 she joined European University as a teaching assistant.

Her areas of research include cryptography, database applications and pattern recognition.