VirusMD Personal Encrypter $^{(TM)}$

Encrypted Messenger $^{(TM)}$

User's Manual

by Cyrus Peikari, M.D.

CHAPTER 1

Introduction

Encrypted Messenger (TM)

The VirusMD Personal Encrypter (TM) is a revolutionary tool to protect your privacy. It contains the first Encrypted Messenger (TM) ever designed for mass use.

This utility also lets you rapidly encrypt files on your hard drive. In addition, VirusMD Personal Encrypter (TM) includes a quick text Encrypter (TM) for securing your email messages.

Why encryption?

When you use traditional messengers, your data is sent across the Internet as clear, plain text. That means that anyone along the way can read your messages without your permission.

Even when you think you have a direct computer-to-computer connection, your messages still pass through 15-50 "hops" before reaching their destination. At each one of these hops people can easily intercept and read your communication.

Keep your data private

Fortunately, by using the VirusMD Personal Encrypter (TM), you can prevent unauthorized users from reading your private conversations. The VirusMD Personal Encrypter (TM) scrambles your plain text communication. Your messages can not be unscrambled by anyone who does not have a special password that is known to you only.

CHAPTER 2

Overview of Features

- *Encrypted Messenger* (TM)*:* This is a fully functional, stand-alone Internet messenger. It is unique in that all messages are encrypted on-the-fly by the built-in encryption engine. This makes for a very powerful and easy way to keep your communication private.

  The program includes both a "server" (for hosting encrypted chat) and a "client" (for connecting to a server).

- *Fast Text Encrypter* (TM)*:* This feature is a very fast and easy to use text Encrypter (TM) amd decrypter. It is useful for encrypting email messages, or to combine with your existing messenger.

- *File Encrypter* (TM)*:* Quickly and easily encrypts files on your local hard drive. This feature works on any type of file, including executables; however, do not try to use it on zipped or compressed files.

CHAPTER 3 *Features*

Introduction

From the VirusMD Personal Encrypter (TM) program directory you can start either the "server", the "client", or the user's manual. For most uses you will want to start the "server." Use your mouse to select Start>Programs>VirusMD Personal Encrypter (TM)>server.

Main Screen

When you start the VirusMD Personal Encrypter (TM) "server", the main screen appears. On this screen is the red VirusMD target logo with the word "Menu" in the center. This is the control center from which you can launch any of the many features of the VirusMD Personal Encrypter (TM)'.

Fast Text Encrypter (TM)

This is a handy feature that lets you quickly encrypt short text messages. This is useful if you would like to encrypt an email message, for example. Or, you can encrypt a message to use with your existing messenger.

Simply select a password, then type or paste your text to be encrypted, then click "encrypt." You may encrypt the text as many times as you like, but just once is sufficient. Pressing "copy" will copy the encrypted message to the clipboard. A remote user will be able to later decrypt the message only if they have the VirusMD Personal Encrypter (TM) and then only if they know the specific password that you used for encryption.

File Encrypter (TM)

The VirusMD Personal Encrypter (TM) also includes the ability to encrypt files on your local hard drive. It is a quick and powerful way to protect your data. Simply select "file Encrypter (TM)" from the main menu.

This screen lets you browse to any file on your local hard drive. After you select a file, enter a password and click "encrypt." To decrypt a file, simply select the file and click "decrypt" while using the same password you used for encryption. Warning: If you forget your password, you will not be able to decrypt your files. Do not try to encrypt zipped or compressed files.

Encrypted Chat

This is the most powerful and innovative feature of the VirusMD Personal Encrypter (TM). By selecting "Encrypted chat" from the main menu, the "server" program of the Encrypted Messenger (TM) starts. When you are running this server, a remote user can connect to you by running the "client" program that comes included in the VirusMD Personal Encrypter (TM).

When you start the server, it will display your current "IP address". Your IP address is your unique number on the Internet, similar to a unique telephone number. It has the form of xxx.xx.xx.xx, where "x" is a numerical digit. If a remote user knows your IP address, she can connect to your computer, similar to a friend calling you on the telephone.

Your current IP address is displayed in the server program window. You will need to communicate this address to a remote user before each chat session. You can give your IP address to other users through telephone, through email or through other, less secure messengers.

By pressing the button labeled "Activate Chat", your server goes live. A remote user who has started the VirusMD Personal Encrypter $^{(TM)}$ "client" program can connect to your server by pressing "connect," and the chat begins. Type your text in the blank line at the bottom and click "send."

At first you may notice that the messages appear to be scrambled or garbled. This is just the VirusMD Personal Encrypter $^{(TM)}$ doing its job. Until you and the remote user have both entered the same password at the top of the program, neither of you will be able to read the other's text. This is how the VirusMD Personal Encrypter $^{(TM)}$ protects your communication from snooping or spying. The password should be secret, and it should be mutually agreed upon in advance.

If you prefer a different username than "Server" or "Client", simply enter your name into the appropriate box on the chat screen.

Help

From the main menu you can also browse to the VirusMD Corporation website (http://www.virusmd.com). There you may obtain technical support on the VirusMD Web Forum. Users who pay to register their software also receive limited time, free email support.

In addition, at the VirusMD.com website you can get personal help with computer viruses and trojan horses. You can also read up-to-the-minute virus alerts and security news from around the world. VirusMD.com is a warm, personal community where individuals, families and computer security industry experts come together to help each other learn to protect themselves.

CHAPTER 4 *Ethics*

Introduction

The VirusMD Corporation Institute for Information Ethics has been in the forefront of research to promote personal morality and responsibility on the Internet. One of the most controversial areas of ethics research is in the public use of encryption.

The controversy centers around an individual's right to privacy vs. the right of employers, government and law enforcement to monitor and to control the individual. VirusMD Corporation does not take either side in this controversy; rather, the goal of the Institute is to promote the highest standards of ethics on all sides.

Corporate ethics

At this time, employers have the legal right to monitor all of your activity in the work place. For example, your employer monitors every email that you send and receive, often filtering email "en masse" for keywords. Employers also eavesdrop on your personal telephone calls at work. In addition, network administrators can secretly log in to your computer over the network to monitor your activity. They can see what websites you are visiting. Also, by using what is called a "keystroke logger," they can even record your personal passwords from your on-line bank accounts accessed from a work computer.

It is not recommended to use the VirusMD Personal Encrypter (TM) at your work place. Your employer may prohibit the use of encryption, and it could cost you your job. The ethical solution for you is to never use the work place for personal activities. Unless it is an emergency, do not make personal telephone calls, send email, or recreationally surf the Internet at work. Your employer has paid for your time at work, and you have agreed to honor this commitment. Thus, if you act ethically, you will never need to use encryption, because all of your work activities will be permissible.

On the other hand, although the practice is currently legal, it is highly unethical for employers to use this power to monitor their employee's personal communication. Like the evil Nazi concentration camps in World War II, such an environment degrades the soul of the abusive employer, while dehumanizing the victimized employee. Moreover, there may be times when an employee needs to make an urgent bank account transaction, or they may need to discuss confidential medical matters with their doctor via telephone or via email. If an employer were to deliberately intercept such communication, they should be held accountable, both from a civil and a criminal perspective. Such cases might eventually lead to more personal freedom in the work place. Nevertheless, at this time it is recommended to use the VirusMD Personal Encrypter (TM) at home only.

Social ethics

VirusMD Corporation advises you to use the highest personal ethics at all times. The VirusMD Personal Encrypter (TM) will not prevent you from being caught if you attempt to commit electronic crime. There is no conceiveable encryption scheme that can ever hinder the intellect and resources of law enforcement agencies.

For example, law enforcement officers can purchase copies of the VirusMD Personal Encrypter (TM) for themselves. Then, with a court order, they can obtain your password from your house with the greatest of ease. One law enforcement technique is to enter your house after you leave and to plant video monitors in your computer room to record passwords. They can also secretly install either software or hardware keystroke loggers on your home computer to record your private passwords and conversations. Thus, there is no way to hide from determined law enforcement agents. Encryption will not protect you from justice. Your best recourse is to maintain high personal ethics and to obey the law at all times.

On the other hand, it is important for law enforcement agents to maintain a high standard of ethics as well. It is now possible for officials to mass-monitor private communication. However, the legality of doing so is currently under fierce debate. Consider the following example from a report by Kevin Poulsen which was published on October 4, 2000 (excerpt reprinted with permission from SecurityFocus):

> *The FBI's Carnivore surveillance tool monitors more than just email.*
>
> *Newly declassified documents obtained by Electronic Privacy Information Center (EPIC) under the Freedom of Information Act reveal that Carnivore can monitor all of a target user's Internet traffic, and, in conjunction with other FBI tools, can reconstruct web pages exactly as a surveillance target saw them while surfing the web.*
>
> *The capability is one of the new details to emerge from some six-hundred pages of heavily redacted documents given to the Washington-based nonprofit group this week, and reviewed by SecurityFocus Wednesday.*
>
> *The documents confirm that Carnivore grew from an earlier FBI project called Omnivore, but reveal for the first time that Omnivore itself replaced a still older tool. The name of that project was carefully blacked out of the documents, and remains classified "secret."*

> *...The FBI can configure the tool to store all traffic to or from a particular Internet IP address, while monitoring DHCP and RADIUS protocols to track a particular user.*
>
> *In "pen mode," in which it implements a limited type of surveillance not requiring a wiretap warrant, Carnivore can capture all packet header information for a targeted user, or zero in email addresses or FTP login data.*
>
> *Web Surveillance Version 2.0 will include the ability to display captured Internet traffic directly from Carnivore. For now, the tool only stores data as raw packets, and another application called "Packeteer" is later used to process those packets. A third program called "CoolMiner" uses Packeteer's output to display and organize the intercepted data.*
>
> *Collectively, the three applications, Carnivore, Packeteer and CoolMiner, are referred to by the FBI lab as the "DragonWare suite."*
>
> *The documents show that in tests, CoolMiner was able to reconstruct HTTP traffic captured by Carnivore into coherent web pages, a capability that would allow FBI agents to see the pages exactly as the user saw them while surfing the web.*

Although at this time monitoring tools, including Carnivore, are being used legally, they raise important ethical issues for those who wield this awesome power. Law enforcement officials with such unregulated and unchecked omnipotence will be sorely tempted to overstep the bounds of moderation and to violate individual civil rights. Officials must actively resist this temptation in themselves.

The consequences of absolute, unregulated control of information can be devastating to society. To understand this, all users are urged to obtain and to read a copy of George Orwell's classic novel "1984." This book demonstrates that society degenerates when technology is used to usurp personal privacy without the controlling hand of ethics. Moreover, countless other examples from history show us the baneful effect of a government without ethics and respect for individual rights. Thus, it is important that the highest morality govern mass processing of information.

CHAPTER 5 *Trouble-shooting*

Q: How do I let other users know my password and IP address?

A: The password must be communicated to other users in advance.

Then, when you start the VirusMD Personal Encrypter (TM) "server," your current IP address will be displayed. You may send your current IP address to other users via telephone, email or other, less secure messengers. Then the remote user can enter your IP address in his "client" to connect to your server.

Q: When I start the VirusMD Personal Encrypter (TM) "client" it lists the IP address as "localhost." How do I connect to a remote server?

A: You must know the IP address of the remote server. Then, simply replace "localhost" with the correct IP address of the remote server and press "connect".

Q: When I start the VirusMD Personal Encrypter (TM) "server", it says my IP address is "192.168.1.1" or some other number that doesn't work. How do I find my real IP address?

A: If you have both a dial-up and a network/LAN card (NIC) installed, your IP address may not be displayed correctly.

To determine your true IP address, open an MS-DOS prompt and type "winipcfg" (If you are using Windows 2000, open a command prompt and type "ipconfig" instead). This will show your true IP address, which you can then use in your VirusMD Personal Encrypter (TM) server.

Q: Will VirusMD Personal Encrypter (TM) work through a firewall?

A: This depends on what firewall software and/or hardware you are using. Visit http://www.virusmd.com for further help.

Q: When I use the client to connect to a remote server, it says “connection forcefully rejected.”

A: In this case, the remote user has not activated the server. Wait until the remote user has pressed “activate chat” on the server, and then try to connect.

Q: Why is there not a central server showing which of my colleagues are online, along with their IP addresses, so that I may connect more easily?

A: Unlike less secure popular messengers, VirusMD Personal Encrypter (TM) does not store your personal information or track your movements on a central server. This is for security reasons, to protect your privacy. Similarly, your conversations are not stored on your local hard drive where unauthorized users could retrieve them later.

CHAPTER 6 *Future Releases*

Future releases of the VirusMD Personal Encrypter (TM) will include encrypted Internet Telephony (encrypted voice over IP), encrypted file transfer, and improved encrypted email features. At this time, VirusMD Corporation is planning to port the utility to a lower-level language to make it more robust and to enhance its catholicism.

Your feedback and suggestions are invaluable. Please send any comments to:

contact@virusmd.com

CHAPTER 7

About VirusMD Corporation

VirusMD has been at the forefront of computer virus and internet security research since 1998. VirusMD security products and software are unique in that they are easy for the novice user to learn and to use.

In addition to thier ease of use, VirusMD software products often introduce new technologies that have never before been seen in the world. This is achieved by using a proprietary research and development method that is impossible to duplicate.

Updated October, 2000