VIRUS DETECTION USING CRYPTOGRAPHY ALGORITHM

DR. A.H. AL-HAMAMI * & VENUS W. SAMAWI **
** SADDAM UNIVERSITY , DEPARTMENT OF COMPUTER SCIENCE -BAGHDAD, IRAQ
* HEAD OF COMPUTER SCIENCE DEPARTMENT AL-RAFIDAIN UNIVERSITY COLLEGE BAGHDAD, IRAQ

VIRUS DETECTION USING CRYPTOGRAPHY ALGORITHM

*Dr. A.H. AL-HAMAMI * & VENUS W. SAMAWI ***

** SADDAM UNIVERSITY - DEPARTMENT OF COMPUTER SCIENCE- BAGHDAD, IRAQ*
** HEAD OF COMPUTER SCIENCE DEPARTMENT AL-RAFIDAIN UNIVERSITY COLLEGE BAGHDAD, IRAQ*

خلاصة البحث

ظهرت عدد من البحوث التي تتناول موضوع فايروسات الحاسبات وذلك لما تسببه من اضرار قد تؤدي الى تعطل الحاسوب او تدمير جزء هام من البيانات او البرامج المخزونة فيه. معظم الفايروسات مصممة لمهاجمة الحاسبات المايكروية وذلك لانتشارها الواسع، وبساطة نظام تشغيلها والذي ادى الى ضعف نظامها الامني مما يسهل مهاجمتها من قبل الفايروسات.

يعتبر التجفير او هي عملية تحويل النص الواضح الى نص غير واضح" احد الطرق المهمة لحماية البيانات (وخصوصا تلك التي تنتقل من خلال شبكات الحاسوب) من المتطفلين، كما تستخدم تقنيات التجفير للكشف عن التغيرات التي قد تحصل على الملفات بسبب المتطفلين او الفايروسات.

يهدف البحث الى التعريف بالفايروسات التي تصيب الحاسبات المايكروية، اذ تعرض كيفية عملها و الطرق المتبعة للوقاية منها او القضاء عليها. واخيرا يقدم البحث فكرة جديدة لتحسين وجود الفايروسات (Virus Detection) وذلك من خلال تضمين احد تقنيات التجفير في نظام التشغيل الخاص بالحاسبات المايكروية (وخصوصا المرتبطة بشبكات الحاسوب) وذلك لتحسين نظام حمايتها ومنع المتطفلين او الفايروسات من محاولة حشر ايعازات في ملفات النظام او المستفيد والتي قد تؤدي الى تدميرها او التاثير سلبا على النظام.

ABSTRACT

Many papers have been published about manipulating computer viruses; instructions that infect a computer system and after a period of incubation and reproduction, activate and demonstrate their presence.

Most viruses were designed to attack microcomputers, since microcomputers are widely used nowadays, and have simple operating systems which result in lack of quality of there security system.

Connecting computers with networks and using copies of programs from unreliable sources such as bullet in board systems, will increase the risk of viral contact and the spread of viruses.

Data encryption disguises data flowing through a network so that it is unintelligible to any one monitoring the data. Encryption techniques can also be used to detect file modification which may caused either by unauthorized users or by viruses.

This paper concern in viruses attacking users or system files (.exe and .com) in microcomputer systems, where viruses types, how they work, and anti-virus strategies are going to be discussed. Finally, a detection strategy depending on Encryption techniques built in the operating system is suggested to improve PCs security and preventing unauthorized users from inserting into programs commands that will cause system corruption.

1. INTRODUCTION: Computer Viruses

Computer viruses can be defined as an instruction (code) that infect a computer system, and after a period of reproduction, activate and demonstrate their presence. They have the ability to attach themselves (under certain circumstances) to computer systems, programs, and data, rapidly propagate through a system, then make some damages to the programs with which it comes in contact. These damages can occur at the time of infection or later, depending on the design of the virus and the characteristics of the infected program.

Computer virus not only has an appending characteristic that allows it to modify other programs, but in some cases the virus software may modify itself according to the characteristics of the program to which it is appended. An infect program can then evolve and become another virus and can spread the evolved virus to other system.

The activities of virus may be triggered when infected program is executed. During program execution, virus may check for specific conditions such as a particular time or date, a sequence of keystrokes or any event that is guaranteed to occur rarely. If the condition is not satisfied, the virus may replicate and remain dormant until the next time the infected program is executed.

Computer connectivity is a major reason that viruses have become a serious threat. Increasingly computer systems are able to connect with many other computer systems which expands the number of possible points of attack. Furthermore, viruses can be transmitted by people with legitimate access to computer systems. Connectivity allows many users to share data, programs, and computers; unfortunately it also allows vandals to attack these users with a virus program.

Viruses can also spread through groups of systems that can communicate with each other such as local area networks (LANs) and wide area networks (WANs).

Mainframes and minicomputers may be less vulnerable to viruses than microcomputers, because large computers have more complex operating systems with builtin security. In addition, the implementation of larger systems is more often unique, so that viruses that attack one system cannot successfully attack another.

The following sections concern in viruses attacking microcomputer systems, their types, work, and anti-virus strategies. A detection strategy depending on encryption techniques is suggested to improve PCs security and preventing unauthorized users from inserting into programs commands that will cause system corruption.

2. VIRUSES OVERVIEW

As mentioned above, viruses is a set of computer instructions which is nothing more than a few lines or number of letters that instruct a computer to change or destroy information and has the ability to propagate copies or versions of itself

into computer programs or data when it is executed within contaminated programs. These viruses are hidden inside a legitimate program (such as games or spreadsheets) that can infect a computer through a disk or even through a phone line.

All viruses work by finding files on their host computer which will be run at some point in the future. When these viruses activated, it may cause serious problems such as:

* altering files
* filling disk or memory with garbage information.
* change the file allocation table (FAT) in a PC so that files cannot be located.
* locking the keyboard
* Altering the boot sectors so computer will not run.
* Slow program execution time.
* Displaying inappropriate messages.
* Formatting the disk
* Changing programs or files.

2.1 TYPES OF VIRUSES:

Viruses work in three phases: infection, reproduction, and detonation. They exhibit a wide range of techniques and competence, and can be divided into five classes according to their effects:

2.1.1 Boot Sector Viruses (e.g New Zealand, Stoned,and Form)

It infects the Dos bootstrap sector or partition sector on a multiple partition hard disk by copying the original sector (old sector) to another position on the disk and mark it as bad sector in DOS FAT. When the computer is started up, the virus loads and runs, and then transfers control to the old boot sector. Boot sector viruses are slow to spread, files do not carry the boot sector therefore cannot spread the infection but they make few changes to their host and so are difficult to spot.

Infection often happens when an infected floppy disk is accidentally left in the drive of a computer which is subsequently reset. Although the message 'Non System disk or disk error' will be displayed and the PC will start up apparently normally when the disk is removed, the virus will have been made resident in memory and will infect the boot sector of the hard disk. All writable floppy disks inserted subsequently will become infected, whether they're supposed to be bootable or not.

2.1.2 File or Parasitic Viruses (e.g Jerusalem, Jushi)

File or parasitic viruses infect any executable file, and so spread much faster than boot sector viruses. They can find executable either by examining the disk or by monitoring common-DOS operations such as copying or program execution. On finding their target they copy themselves in.

The growth in program size might seem a guaranteed way of spotting infection, but some viruses hide themselves by modifying the directory

information about the file, so that the DIR command always shows the old size. Others work like boot sector viruses, creating some BAD sectors and using these to hold either themselves or the portion of the host program they've replaced.

2.1.3 Multi-partite Viruses (e.g Spanish Telecom):

This kind of viruses combines both Boot and File virus techniques to maximize its infectiousness. This type of viruses once it has become a boot sector virus, it will only spread via boot sector, and the same is true for files.

2.1.4 Two Uncommon Virus Types (e.g DIR II):

The last two varieties of virus are uncommon. One depends on the MS-DOS quirk whereby, if both FRED.EXE and FRED.COM are present in a directory, the COM program will be executed first. So a virus may create a COM file for every EXE it finds, and this will be run by DOS every time the user types the name of the original program. The final virus type directly modifies the directory entry of executable files. The directory entry contains the position on disk of the executable file, so the virus can intercept this position and make it point to the virus code. The virus copies the original position into an unused part of the directory entry, and uses this to run the original program once the virus itself has been activated.

2.1.5 Avoiding Detection (e.g Maltese Amoeba and Tequila)

As well as stealth, viruses use encryption and polymorphism to hinder detection. With encryption, most of a virus changes each time it infects a file. The program is scrambled according to a different code every time, reducing the chance of a scanner being able to match it to a signature. In encrypted viruses, though, the decrypting code (the part of the virus that unscrambles the main body of the infection) is not itself encrypted, and this can be used to identify the virus. Some viruses goes further, They consistently rewrite the decryption routine so that it's different each time even though it performs the same function. This is possible parity because a PC's processor has a number of program instructions that do the same thing as other instructions. A virus can mix and match these without changing the way it works while changing the signature each time.

2.2 VIRUS DETECTION

There are several software products that can be used to detect viruses. These products can be described as:

2.2.1 Virus Presence Detection

Products designed to detect the presence of viruses may do so by searching for suspicious code, suspicious text strings, or for specific file names to detect known viruses. These limited techniques may not provide adequate protection. There are two categories of such anti-viruses:

VIRUS MONITOR: Virus monitors are designed to remain active throughout the usual running of the computer. Commonly configured as TSRs (Terminate and stay resident programs which are loaded and continue running in the background

while the computer carries out other tasks), they scrutinise disk activity, file execution and copying, and report if they spot activity which they consider abnormal (e.g boot sectors EXE and COM files aren't usually modified, and if a monitor spots any attempt to write into one of these files it will halt operation and alert the user). This catches most viruses activity, but some of them can bypass the usual read and write mechanisms, and modify files in other ways. Hardware monitors is one solution at which virus detection included in PC chips.

SCANNERS: Scanners are designed to be run periodically. They search the disks or network devices attached to the computer and check each potentially infected file for viral code against a dictionary of *signature* patterns. If a program contains viral code, the scanner reports both the name of the file and the name of the virus, although it doesn't deal with them. This catches most common viruses, but not those which aren't in the directory. As a result, it is important to keep scanning software up-to-date with new dictionaries from software developer.

DISINFECTORS: Disinfectors need a precise identification of the virus found and are usually used in conjunction with scanner. Some viruses can easily removed from an infected program without any risk of affecting the body of the program code, other viruses may be more intricately with their host and are difficult to remove. Since all infected files are going to be executable files, therefore, as a standard policy there should be installation or backup version of them for safety purposes. Perhaps the safest way to disinfect a file is to delete it and install a new copy in its place. The same procedure can be used with boot sector or partition table.

2.2.2 The Detection of File Modification Caused by Viruses

Products designed to detect changes to a file caused by virus usually sum mathematical values of each byte in the file, such as:

INTEGRITY CHECKERS: Integrity checkers work in two passes: in the first pass, the integrity checkers go through the disk creating unique mathematically-derived signatures, called *Checksums*, for each file that might be infected. In second pass, the checkers recreate the checksums on subsequent runs, and match them against the old values to see whether the files have been changed in the meantime it's reported.

Integrity checkers do not care about the nature of the virus therefore don't need regular updating. Their main problems are that new or update software won't be covered unless a new set of checksums is created.

3. ENCRYPTION VERSES SECURITY

Encryption is the process of changing plain text so that it becomes unreadable. The resulting cipher text can not be read without the key used to encrypt it. Most enciphering methods also include something similar to a checksum, and error correction code.

There are two basic types of cryptographic systems used today, these are: *Private and Public key* systems. A private key encryption system requires that the

sending and receiving parties share a common key. This key must be kept secret (private) to insure the security of the encrypted information.

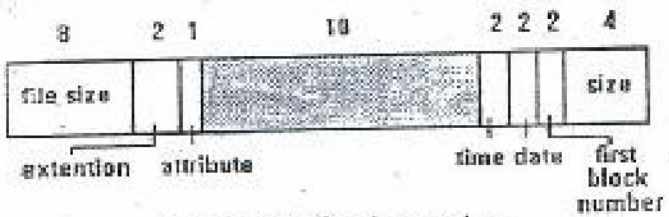
A public key cryptographic system involves pairs of keys, one for encrypting messages and another for decrypting them. The encrypting key is public, so that anyone wishing to send a message to a given user can use that encrypting key. Only the recipient, however, has the secret decryption key.

Encryption techniques used to keep secrecy of files or message exchanging through a network, they also can be used to detect file modification caused by intruders or by virus attacking.

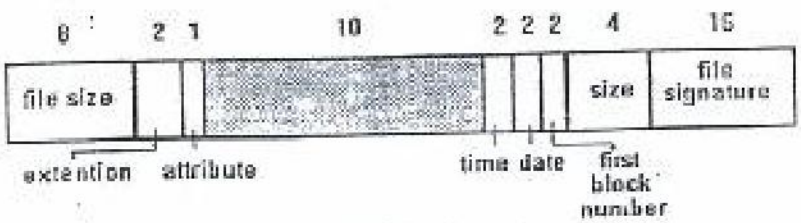
In the next section we are going to suggest a new way to detect viruses that infects execution files (EXE, COM files) depending on one of the encryption algorithms that could be built as a part of the operating system (DOS).

3.1 Encryption As a Virus Detection Tool

The most popular type of viruses are those who infect execution files (usually COM or EXE files). Once these viruses located a suitable file, they attach themselves to it in a place that guaranteed to be run before any legitimate program code. The most suitable part in the execution file that the virus ensure that it is going to be run is either the execution file header or the bytes next to the header. Therefore, if we put a file signature at the beginning of each file before changing it to execution file, this will help the operating system to check whether the current execution file is a legitimate file and is original (not modified). This can be done as follows:



a- current directory entry



b- suggested directory entry

Figure -1 Directory entry

1- We need to add new field to the FAT (File Allocation Table), this field contains the file signature (figure-1) which is needed to insure the file identity.

2- When generating execution file, the user should be asked to give the file signature which is kept in two places: first, at the beginning of execution file (after file heading), and second is at (signature field) in the FAT entry concerning the current execution file.

3- When the operation of generating an execution version of the file is finished, the resulted execution file should be encrypted (implicitly during the conversion operation) using public key algorithm.

4- Whenever this file needed to be executed, the operating system will load the file into memory, decrypt the file using its privet key, then get the file signature (from the area next to the file header), compare it with the file signature in the FAT. If the signatures matched then the file is legitimate (not modified) and can be executed safely. For further insurance, file checksum is implemented, if it matches the checksum list then the file is safe, or else the file will be moved to a special locked directory where the suspected files kept and reboot the system.

5- If the file signature discovered by the operating system and the file signature in the FAT are not identical, then the operating system will move the file from its position and keep it in a special locked directory (this directory contains all the suspicious files), and reboot the system again in order to remove the effect of the virus (if exist).

4. DISCUSSION & CONCLUSION:

Viruses come in many shapes and sizes, with widely differing patterns of behavior, infectiousness and severity. All have the ability to infect legitimate files and duplicate themselves from computer to computer through any medium that can transport those files (networks, floppy disks are all potential routes). There are different anti-viruses packages work by detecting the virus before activation and optionally removing the infection.

It was discovered that the cryptography algorithms can be used to detect the presence of viruses since any changes in an encrypted file will generate different file after decryption. Such algorithm is very useful in system protection but it will complicate the operating system and also may be costly from processing time and space point of view.

REFERENCES

1) Antivirus Software - Keeping up your Guard
By Robin Raskin with M.E. Kabay
PC Magazine, March-1993, p209-268

2) Antuvirus Software
By Ropert Goodwins & Faris Racuf
PC Magazine, May-1993, p176-p213

3) Computer Crime - Techniques Prevention
By Geoffrey H. Wold & Robert F. Shriver
Galgotia Publication pvt.Ltd., 1993

4) Cipher Systems - the protection of communications
By Henry Beker & Fred Piper
Northwood Publications, 1982

5) التجفير والترميز حماية ضد القرصنة والتطفل
د. علاء حسين محمد و مهدي صالح مهدي العزاوي
دائرة التدريب - مديرية التطوير الفني، الطبعة الاولى، كانون الثاني، 1989