# INFORMATION WARFARE:

# Where are the Threats?

by

**Dr. H.B. Wolfe**

**"Emerge from the void, strike vulnerable points, shun places that are defended, attack in unexpected quarters."** - Sun Tzu 5th Century BC - *The Art of War*

## New Virus Opportunities - Macro Viruses

The computer virus phenomenon has not disappeared. It may not be gathering the media hype of years past but it is still a very real threat to computing. In addition, new types of viruses have appeared and the advent of Windows '95 has provided a new challenge to virus writers.

By now most of us are familiar with the original two types of infection formerly encountered. The boot sector and applications sector viruses have not gone away. The method of their general operation remains the same. However, these basic techniques have been improved with the introduction of companion, multi-partite, poly-morphic, and stealth viruses (for both boot sector and applications) to name a few.

The new approaches have come in the form of macro viruses. These have the unique ability to spread attached to **DOCUMENT** files. This is a major departure from the good old viruses we have come to expect and loathe. We have discussed in the past how such a virus might work but up until that last few months they were only found in the laboratory and not in the "wild".

Enter the Word "*Concept*" virus. While the *DMV* was developed earlier, the *Concept* is the first to be found traveling in cyberspace. Although it does have a payload, that payload is never executed. The Word macro viruses make use of the fact that Microsoft Word uses templates to set up documents. These templates can contain executable instructions - macros. The most common one that we usually see is identified as **NORMAL.DOT-** Word's global document template. This sets up your page margins and type fonts, etc. Some macro viruses modify this specific Word template in such a way as to be able to execute their code. That code is added to every new document file created thereafter with the **Save As** command.

One of the important features of this generic type of virus is the fact that it can travel between different environments. The Word macro virus can infect across platforms (no other virus family has that capacity - so far). What that means is that it can work in the Windows environment in versions 3.x, '95, and NT as well as in Word 6.x for Macintosh. This constitutes a major milestone in the development cycle of virus technology.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

In the short term, you can protect your system from most macro viruses **(but NOT all)** by creating a new macro called **AutoExec**. The commands necessary are as follows:

```
Sub MAIN
    DisableAutoMacros
    MsgBox "AutoMacros are now turned off.", "Virus protection", 64
End Sub
```

The newer versions of anti-virus products will scan for these types of viruses as well.

**New Operating Systems - New Virus Challenges**

Microsoft, in its infinite wisdom, has introduced a new operating system - Windows '95. This offers new challenges to the budding virus writer. Those challenges have not gone unnoticed. The first recorded Windows '95 operating system specific virus is called the *Boza.A* also know n as *Bizatch*. This was first discovered in January and is of Australian origin. This first version was written just to demonstrate that Windows '95 was vulnerable and is actually designed to do no harm. However, it has a bug that in some cases will cause infected **.EXE** files to increase in size by several megabytes. This is just the beginning of a whole new family of viruses.

The *Boza.A* infects Windows Portable Executable **.EXE** files. One to three files are infected each time that the *Boza.A* is executed. It was created by VLAD - a virus writers group originating in Australia. This group also have made available much in the way of virus source code on the Internet. Once again, most of the newer versions of anti-virus products will scan for this virus and repair files infected by it.

It is worth mentioning that there are several Word Trojans that are currently circulating. These do not replicate themselves, however, if you should be unfortunate enough to open a document that has one of these attached, it will immediately begin deleting data.

**Guarding Against Viruses - The Best Defenses**

The best defenses against viruses still apply. A good scanner should always be used on new files and now not just executables only but also document files capable of carrying macro code with them. John McAfee's **SCAN** or Frid Skulason's **F-PROT** can easily be downloaded from the Internet at no cost and are among the best available today. In addition there are several excellent products currently available in the marketplace that have survived the test of time.

We all need to be reminded that the best defensive technique is backing up all of your important files regularly. With proper backup we can recover from most kinds of attacks.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

**Use of Encryption - Why, When and How**

Data encryption is a powerful tool that can provide privacy and confidentiality in the storage of data and in the communication of data. If you ascribe to the philosophy that privacy is one of the basic human rights that everyone is or should be entitled to then cryptography provides one of the tools to enable us all to carry out that right. If your philosophy is that law enforcement and governments should have the ability to deprive citizens of that right by being able to view or intercept and view private data and communications at their discretion then cryptography is what is used by criminals to thwart that ability. The notion of "if you have nothing to hide then you shouldn't mind" is a naive and foolish. In every society where this authority has been granted it has been abused to the detriment of its citizenry.

Who is "right" is really a matter of emotion and opinion - and I suppose power. If citizens knowingly entrust the servants of the people with the authority to intercept, eavesdrop and intrude into private communications, papers and affairs then they have the power. If law enforcement and/or government usurp that authority without the knowledge of the citizens then George Orwell's prediction in 1984 has come true.

In any environment, business or private, there are pieces of information that are confidential that need to be stored and/or communicated. The risk as a result of that information falling into the wrong hands has varying degrees of severity. It may be proprietary information that would put a competitor at an advantage if known to them. It may be information controlling capital or the movement of capital. Once again if that information were known then actions could be taken to intercept or divert the capital. Therefore, we use encryption to protect sensitive communications and confidential data storage.

The tools to accomplish this come in many flavors. To the untrained or unknowledgeable one encryption product (algorithm) might seem as secure as the next but that couldn't be further from the truth. For example WordPerfect has a data encryption function. Many unsuspecting folks use it believing that they are successfully protecting their stored documents. Any hacker knows that a program called **WPCRACK** is freely available on the Internet. This program derives the key phrase from the encrypted file thus enabling anyone who has **WPCRACK** to decode a WordPerfect encrypted file without initially knowing the key phrase. A similar cracker program is also available for Microsoft Word.

The lesson to be learned is that simply because a vendor has a reputation for excellence in one arena does not automatically mean that they also possess that same level of expertise in another. The example cited above could have easily been avoided by calling upon a cryptographer of stature for advice in selecting the encryption algorithm and in its use. It is important to understand that an algorithm of superior strength can be weakened or undermined in that strength by poor or ill-conceived usage.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

**Some History**

Modern cryptography really came into its own in the mid 1970's. In 1975 the U.S. Government invited proposals for a data encryption standard that could be certified to provide a given level of protection. One of the algorithms submitted was called Lucifer (devised by IBM). It was a block cipher with a key length of 128 bits (this attribute is often confused as the ONLY gauge by which the relative strength of an algorithm can be judged). The National Security Agency (NSA) is the code making and code breaking agency for the U.S. It is the largest single user of computers, and largest single employer of mathematicians and cryptographers in the world. They had a great deal of influence in the creation of the final algorithm today known as the DES (Data Encryption Standard). This algorithm is one of the most commonly used encryption algorithms in use in business today.

The final DES consisted of a symmetric block cipher with a 56 bit key. The 56 bits can be described as follows: the total number of possible permutations of any given message encrypted using the DES algorithm is $2^{56}$. That's a lot of different messages considering that only one of those is the real one. At the time of its creation it was estimated that with all of the available computing power in the world it would take hundreds of years to find the key. Things have changed since then, It is currently estimated that NSA can decrypt such a message in a few minutes or less with the equipment that they have available.

The DES has been shrouded in controversy ever since its certification. NSA has been accused of designing a "back door" into the algorithm. It has also been accused of deliberately diminishing the DES's level of security by reducing the possible number of permutations (56 bit key instead of the 128 bit key in the original Lucifer design). Of course all of these allegations have been denied, however, this introduces politics into the equation of privacy.

**The Politics of Encryption**

War has caught us that knowing what the enemy intends to do gives us an advantage. WW II was influenced dramatically by cryptography - some say that it determined the outcome. The Allies were, from the very beginning and throughout the war, able to decode the communications of both the Axis powers and the Japanese. The United States has considered data encryption and its tools the domain of the intelligence community and has legislated that (under the ITAR regulations) cryptographic hardware and software fall into the classification of munitions. As such they strictly regulate the export of items that fall into that category. Moreover, there is a strong conviction on the part of the U.S.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

Government and law enforcement that they and only they should have the right and authority to be able to decode any and all communications. The rationale apparently is that without that ability law enforcement cannot deal with crime prevention effectively. The intelligence community rationalize it by using the "threats to national security" argument for their justification. Since both sectors wield significant influence and power, a new concept in cryptography has emerged. It's called escrow encryption. The U.S. Government is actively pursuing the notion that no one should be allowed to have strong encryption (meaning that they can't break it) and should "trust them" not to abuse their power. This from a government with a chronic history of the abuse of power.

Addressing what the U.S. does may not seem particularly relevant to what we do in New Zealand or the rest of the world but that couldn't be further from fact. The U.S. is currently in the process of attempting to hijack the Ad Hoc Group of Experts on Cryptography Policy Guidelines - a sub-committee of the Committee for Information, Computer and Communications Policy specifically set up by the **OECD** to establish cryptographic standards amongst OECD nations (New Zealand is a member). When I say hijack, I mean load the sub-committee with like minded individuals so that their (the US's) agenda can be carried out. It is the position of the U.S that only law enforcement and intelligence professionals should be members of this committee and that strong cryptography should only be available to those two groups. Of course with no input from other sectors strong encryption for the masses will ultimately be outlawed. That means us.

**Escrow Encryption**

The current initiative in escrow encryption is generally referred to as Clipper, however, that is really only the name given to one of the chips in which the escrow algorithm called Skipjack is implemented. Its computer counterpart is the Capstone algorithm implemented in the Fortezza chip. The way it works is that encryption between parties is carried out in the normal way, however, lodged with two escrow agents (both are arms of the U.S. Government) is the escrow key or more precisely each escrow agent possesses one half of the key. If government or law enforcement decided that they wanted to have access to your communications or encrypted files, they would, theoretically, obtain a court order and take it to the escrow agents to obtain the two halves of your key and proceed to decode your communications or files. The escrow key (or "family" key) is a secondary key that unlocks the algorithm to them. However, the algorithm is secret. The exact details of the production of "family" keys is secret. All "family" keys will be produced by NSA. Of course, THEY would NEVER retain any of those "family" keys for future use. Moreover, the actual number of unique "family" keys is unknown. If the system were used by nations other than the U.S. these facts would remain the same.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

For the reader that assumes that law enforcement or government should be able to view any and all communications that everyone might engage in, this type of encryption presents no problems. For those of us who believe strongly that **privacy is one of our most basic human rights**, this presents a big problem. One of the attitudes that I have noticed during the seventeen years that I have lived in New Zealand is that most folks seem to believe that anything that is secret is bad and/or illegal. For the reader who ascribes to that view, I direct your attention to the book by Sissela Bok called *SECRETS: Concealment & Revelation*. It is an excellent exposition of why each and every one of us needs privacy and secrecy in our day to day lives and dispels the notion that it is automatically bad or in some way illegal.

**Newer Algorithms**

Concurrently, from the time that the DES was certified by the U.S. Government, cryptographers in the public sector have engaged in continuous development. Several notable approaches have emerged, been tested and continue to provide strong encryption. There are a couple of symmetric block ciphers of note. The first is the 128 bit IDEA (International Data Encryption Algorithm) developed around 1990 by Xuejia Lai and James Massey. This is thought to be one of the most secure today. To give you an idea of exactly what that means: if you had a computer capable of doing one billion encryptions per second AND you could array one billion of these machines to work in concert, a brute-force attack, on a single message encrypted using IDEA, **would take $10^{13}$ years to find the solution.** By anyone's standards that's a long time. In cryptographic terms it is considered computationally secure. The interesting thing about IDEA is that it is not owned or controlled by the U.S. and can be licensed through Ascom Systec, Ltd., a Swiss company.

The second is a variable key length (up to 448 bits) block cipher, called Blowfish, developed in the last couple of years by Bruce Schneier. It's pretty new and has been scrutinized but thus far no one has been able to defeat it.

Another that is currently being used is called Triple DES. This uses the DES algorithm but does the encryption in three passes. Using two different keys. This improves the apparent security of the DES to 112 bits or 2 to the 112 power different possible permutations of any single message.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

**Public Key Crypto-Systems**

In the late seventies another approach was developed called public key cryptography. Instead of having only one key to perform the functions of encryption and decryption public key systems require two keys. One with which you encrypt and another with which you decrypt.

The weakest point in the use of cryptography is the exchange of keys. If keys can be intercepted, then there is no need to attempt to "break" an encoded message. Asymmetric key ciphers eliminate the need to exchange secret keys. This is a very attractive feature because it allows strangers to communicate immediately in a secure way. To put it into terms that are readily understandable: two organizations can do business, that is, exchange confidential or financial information with the expectation that no one else can view and interpret that information. This can include the simple ordering of goods using a credit card number over the Internet with the confidence that no one along the path of your communication can interpret the encoded portion of your order that contains your credit card number. **NOTE: Communication on the Internet requires that any given message be passed through several intermediaries before it ultimately reaches its destination. At ANY point along that path the message can be recorded, viewed or misdirected at the discretion of the operator at that node.**

There are a few such systems that have emerged as being stable and secure. The first to receive attention is the RSA algorithm developed by Ron Rivest, Adi Shamir and Len Adleman. They issued a challenge in August 1977 to decrypt a message encoded with a 429 bit key. They predicted that it would take 40 quadrillion years with the technology of the day to crack the code. In April 1994 after eight months of effort using 1600 computers the message was solved.

You may have noticed earlier in the paper that I have described the computational security of IDEA and it only had a 128 bit key as compared to the 429 bit key cited above. It is important to understand the difference in approach between a symmetric block cipher and a public key cipher. Solving the public key cipher does not depend on a brute-force attack strategy. In the case of the RSA algorithm the two keys are based on very large prime numbers. The attack strategy is to factor these prime numbers and then derive a solution. The symmetric block cipher does not depend on large prime numbers for any part of its activity and therefore this attack strategy does not work with them. A simple guide to comparative levels of computational security is as follows:

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

| Symmetric | | Public Key | |
|---|---|---|---|
| **56** | is equivalent to | **384** | **size of** |
| **112** | is equivalent to | **1792** | **keys in** |
| **128** | is equivalent to | **2304** | **bits** |

What is to be learned by the solving of the RSA-429 message is that the RSA algorithm must be used with large key sizes - 512 bit keys or larger - preferably 1024 or greater in order to provide strong protection.

Another public key system is Pretty Good Privacy (PGP). It was developed and introduced by Phil Zimmermann in 1991 and has become the world de facto standard for ordinary citizens of all nations. This is a hybrid system which incorporates three different algorithms to provide sufficient computational security for the common man. These include RSA (used to protect the randomly generated keys used with IDEA to encrypt the main body of the message), IDEA (used to encrypt the main body of the message) and MD5 (a one way hash function developed by Ron Rivest and used in this incarnation to create an authentication signature for the message). PGP has become freely available from Internet sites around the world. In your search for potential archival sites ignore the U.S. (refer to the references at the end of this paper for some likely starting points). If you're outside the U.S. and try to download a copy from MIT, for example, that download will be stopped and in fact constitutes an offense under U.S. law. There are also Windows front ends to drive PGP that make it a little more user friendly as well.

Unfortunately for Phil, the U.S. Government has viewed PGP's proliferation very negatively. In fact the FBI and other agencies have investigated Phil with the intention of prosecuting him for the export of string encryption to destinations outside the U.S. without the required export approvals. They have spent the past four years on that investigation and in January of this year decided not to proceed. During that time Phil has had to put up with a lot of Government harassment. In fact, we were returning to the U.S. from Curacao in 1994 through Miami after speaking at a conference. I proceeded through Customs with no problem - it took 5 minutes. Eight hours later Phil emerged somewhat bedraggled to continue his trip home. Of course he'd missed his flight by then.

New Zealand has a community of interest in cryptography. There are at least two public key systems that have been developed here in New Zealand. The LUC system was developed by Peter Smith of Auckland. It makes use of Lucas functions in the generation of primes. It's too new to determine how secure the algorithm is at this point. There is some talk of an unpublished paper describing how to break at least some implementations of it. Another is RPK developed by Bill Raike of Auckland. Dr. Raike's system is based

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

upon the mathematics of finite Galois fields. Once again it is too new to be certain of its real level of computational security but it does show promise.

Another firm in Christchurch (CES) has developed an analog stream cipher and implemented it in hardware form (called SignalGuard). It does not consider data in any way. It transforms the analog signal once it has left the modem for transmission over a telephone line. This is a unique approach to encryption and offers a level of security which is at this time unknown to the writer.

There are products that we can purchase here in spite of the U.S. ban on the export of strong encryption. For example, Fujitzu distributes a product called TeamWARE Crypto that makes use of the FEAL-8 algorithm (NZ$215). It runs in the Windows (3.x and '95) environment and is non-intrusive and pretty easy to use. This type of product is ideal for protecting sensitive data stored on portable computers. It is important to note that trends in crime seem to favor the theft of portable computers (more than 200,000 were stolen in the U.S. in 1995). In fact there are documented cases of the targeting of specific executives and the theft of their machines - not for the hardware but what is contained thereon. Any business person that routinely uses their notebook computer to store sensitive business information should be using such a product.

**PGPfone, Nautilus**

There is another use for encryption. That is in voice communication. There are a few micro based systems that are currently available on the Internet that facilitate secure communications. Two such systems are Nautilus and PGPfone. Both require multimedia machines in the Pentium range with high speed modems and sound cards. Nautilus makes IDEA, Triple Des or Blowfish available for the user's choice of encryption algorithms. PGPfone offers Triple Des or Blowfish and is available for both Mackintosh and Windows '95 environments. Both systems make it possible for two people with multimedia computers to communicate securely over the phone. In the past only diplomats and governments had that capability. Once again, real privacy has been made possible for the ordinary citizen through the use of cryptography.

**Other unseen threats - TEMPEST**

It is easy for those of us who are technology oriented to be drawn into obscure and unlikely security threats merely because of the interesting technology involved. TEMPEST is such an area of interest. The average computer user can dismiss the risk attributed to TEMPEST surveillance and so justify that opinion by saying that only governments have the necessary technology to carry out such data interception. On the surface that makes a pretty good argument. However, upon closer inspection we find that devices to intercept such electronic emanations are freely available for a price. Such devices can be purchased (without license or other control) freely for prices ranging from US$2995 to as much as

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

US$29,995. Moreover, with plans for such a device it can be built by an electronics hobbyist for just a few hundred New Zealand dollars. This is not an academic pronouncement nor idle conjecture. Two students in my Computer Security class have done so from plans which I obtained for US$50 - and it works.

As the value of information increases and as more folks become aware that information can be obtained with minimal risk by using TEMPEST techniques its use will surely rise. Without legislation to inhibit the use of that technique and without technology freely available to thwart and defend against TEMPEST attacks there is no reason NOT to make use of this technology.

**Closing Comments**

We live in the age of information and technology. Each and every day of our lives is touched in some way by one or the other. In order to protect ourselves from the many risks associated with both it is incumbent on us all to learn all that we can and use that knowledge to defend that which is most precious to us ("knowledge is power"). The key to computer security is people. The key to good computer security is people that strive to learn all they can about their field and apply that knowledge in a responsible way to protecting the integrity, accuracy and continuity of their information technology.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

**Additional Sources of Useful Information:**

**Cryptography:**

Schneier, Bruce, *Applied Cryptography,* 2nd Edition, New York, John Wiley & Sons, Inc., 1996, **ISBN 0-471-11709-9.**

Schneier, Bruce, *E-MAIL SECURITY: How to Keep Your Electronic Messages Private, New* York, John Wiley & Sons, Inc., 1995, **ISBN 0-471-05318-X.**

Stallings, William, *PROTECT YOUR PRIVACY: A Guide for PGP Users,* Englewood Cliffs, New Jersey, Prentice Hall PTR, 1995, **ISBN 0-13-185596-4.**

Bamford, James, *The Puzzle Palace,* Harmondworth, England, Penguin Books, Ltd., 1983, **ISBN 0-14-006748-5.**

Kahn, David, *THE CODE-BREAKERS: The Story of Secret Writing, New* York, MacMillan Publishing Company, 1967, **ISBN 0-02-560460-0.**

**Viruses:**

Ludwig, Mark, *The Giant Black Book of Computer Viruses,* Show Low, Arizona, American Eagle Publications, Inc., 1995, **ISBN 0-929408-10-1.**

**Networks:**

Cheswick, William R., Bellovin, Steven M., *Firewalls and Internet Security,* Reading Massachusetts, Addison-Wesley Publications Company, 1994, **ISBN 0-201-63357-4.**

**Document Security:**

van Renesse, Rudolf L., *Optical Document Security,* Norwood, Massachusetts, Artech House, Inc. 1994, **ISBN 0-89006-619-1.**

## General:

Schwartau, Winn, INFORMATION WARFARE: Chaos on the Electronic Superhighway, New York, Thunder's Mouth Press, 1994, **ISBN 1-56025-080-1.**

Bok, Sissela, *SECRETS: Concealment & Revelation,* Oxford, England, Oxford University Press, 1986, **ISBN 0-19-286072-0.**

**Periodicals:**

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.

*Computers & Security*, Oxford, England, Elsevier Advanced Technology, 8 issues per year, **ISSN 0167-4048.**

*Computer Fraud & Security Bulletin*, Oxford, England, Elsevier Advanced Technology, 12 issues per year, **ISSN 1361-3723.**

*Network Security*, Oxford, England, Elsevier Advanced Technology, 12 issues per year, **ISSN 1353-4858.**

*INFO Security News*, Framingham, Massachusetts, MIS Training Institute Press, Inc. 6 issues per year, **ISSN 1066-7822.**

*Cryptologia*, Terre Haute, Indiana, Rose-Hulman Institute of Technology, 4 issues per year, **ISSN 0161-1194.**

*Privacy and Security 2001*, Sterling, Virginia, Ross Engineering, Inc., 12 issues per year.

© 1996 H.B. Wolfe, P.O. Box 6079, Dunedin New Zealand. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted by any form or by any means, electronic, optical, or magnetic, without prior written permission of the author.