Timesavers international Pty Ltd
Have the Time of your Life!

SUBMISSION NO. 14

ABN 99 108 493 214
Po Box 870
Alstonville NSW 2477
Australia
Telephone: 61/0 2 66 295 358

Date: 26/6/09 - 11 pages

Attention: The Secretary of the Committee

This submission is primarily concerned with sections (e) and (f) of the terms of reference for the The House Of Representatives, Standing Committee on Communications - Inquiry into Cyber Crime -

Overview of submission

A new approach to computer security is needed to combat the emerging trends of attacks on computers today as the current security approaches, which are primarily reactive, have inherent vulnerabilities. In our submission we have identified what we feel are particular vulnerabilities for computer security and have provided details of security software and systems we have developed to specifically to address these vulnerabilities. The submission is provided in three parts as follows:

1. Description of the current situation
2. Flaws in the current computer security industry and solutions

    2.1 Ineffectiveness of conventional security software
    2.2 Lack of control of the end users

3. Conclusion

Timesavers International Pty Ltd has developed a new security software, called CyberForceField (CFF), which offers a new method of protection, without the need for any updating whilst repelling all malware and user attacks, whether from external attacks or internal staff pilfering data. We have also designed a series of techniques called CyberMartialArts (CMA) a series of tools and instructions that allows users to apply CFF security in uniquely customized ways. Whilst our new solutions concern PCs with Microsoft Windows Operating Systems (90% of computers), the same approach can be applied for Mac and Linux Operating systems which have similar vulnerabilities as Windows.

1. Description of the current situation (June 09) in the computer security industry:

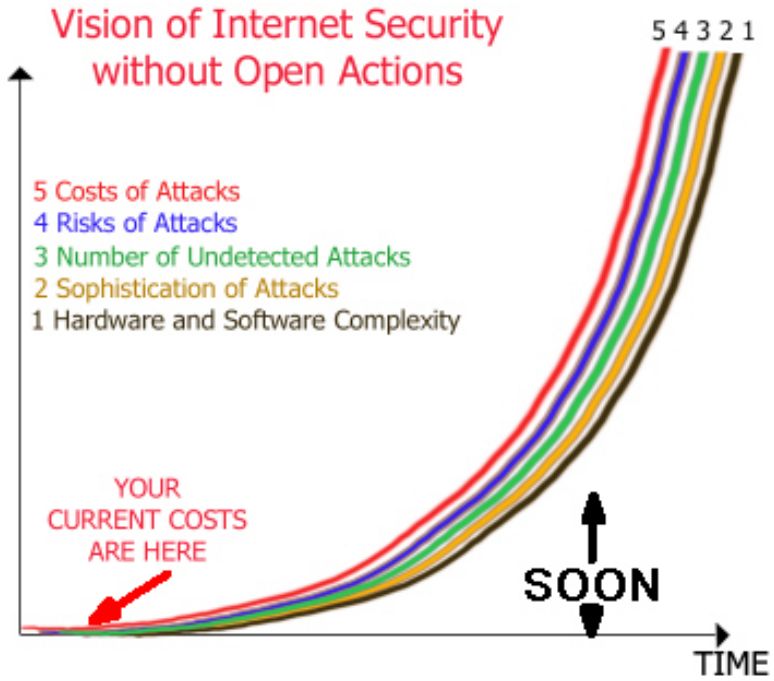
The threats in the computer security industry are growing exponentially due to increased growth of connectivity, extensibility (upgradability) and complexity of computer systems. Computers communicate with more and more devices, software and hardware, which are all evolving at increasing speed and complexity. A virus can hide in the microchip of a printer, a motherboard or in electronic equipment connected to a computer, even a mobile phone.

In addition, the majority of programmers are using programming languages which have inherent security flaws and they can lack an awareness of these vulnerabilities. Likewise, the majority of the end users have very little knowledge of computer security, have no idea about how to check that their security software has been compromised, what an attack looks like and what to do when it happens. To make things worse, the speed of communication is increasing rapidly too and thus the potential for attacks and the consequent damage that can occur is escalating.

The majority of specialists and experts are not addressing the fundamental flaws of computer security, and consequently are giving misleading advice. At school, students are not being prepared for the level of skills they will need to respond appropriately to the computer threats of the future. Tools for hacking computers are evolving very fast and some of these, such as “botnets” can allow hackers to control entire networks sometimes involving several millions of computers.

(reference: Software Security -Gary McGraw - Building Secure Software: How to Avoid Security Problems the Right Way)

Our most famous experts have very pessimistic visions of the future of cyber wars, and no clear solution to propose.



2. Flaws in the current computer security industry and solutions

We have identified 10 fundamental flaws of the computer security industry today, which we have classified into two broad categories, concerning **the ineffectiveness of conventional security software and the lack of control of the end users**.

We have designed innovative software solutions to address these fundamental flaws. In the following section we have classified these ten fundamental flaws, provided a description of the impacts and offer our solutions.

INEFFECTIVENESS OF CONVENTIONAL SECURITY SOFTWARE

1) Security software can be corrupted remotely
2) The dangers of AUTOMATIC UPDATES
3) The dangers of scanning hard drives
4) The dangers of uniformity
5) The growing need of resources for security software
6) The vulnerability of computers at ALL times
7) Lack of protection against attacks by a user at the keyboard itself

LACK OF CONTROL OF THE END USERS

8) Little knowledge of the end users
9) Lack of competent trustworthy personal support online for security issues
10) End users have too little control over what the computers are doing

2.1 INEFFECTIVENESS OF CONVENTIONAL SECURITY SOFTWARE

1) Security software can be corrupted remotely

Any communication with the Internet can be hacked. Therefore security software which communicates with the Internet can be corrupted in theory, and is in practice. Conventional security software needs Internet access and exchanges data with the Internet regularly. This communication is a critical security vulnerability in itself.

When your security software does communicate with the Internet:

- Can you trust that the team of programmers in charge of the updates is keeping abreast with the growth of threats online?
- Can you trust that your computer is actually communicating with the manufacturer of your security software and not a malicious site?
- Can you trust that the data reaching your computer hasn't been compromised along the way on the Internet?

Our Solution: The main security software does not communicate with the Internet, protects itself strongly, its behaviour is transparent to the users and stays under their control.

CFF is isolated from the Internet. It is not doing the work of the firewall, monitoring the traffic with the Internet and other computers.
It replaces almost all the security software apart from the firewall, (anti-virus, anti-spyware, anti-rootkits, anti-bots, etc.) Our approach does not require updates, upgrades and patches and therefore it does not require any communication from the Internet.

The administrator can set the special rules of what CFF is doing, thereby giving 100% control. There is no way it can be used to spy on the users or do any damage. CFF does not repair automatically. It does not modify any data apart from its own settings, eliminating the possibilities of errors due to false alerts, wrong interpretations or detections of attacks. CFF has a proactive approach to preventing attacks. This allows it to protect itself strongly.

CFF is using a WYSIWYG (What You See Is What YOU Get) protection. The settings you see are defining what CFF does and the protection you get. What you can see and understand is more trustworthy.

2) The dangers of AUTOMATIC UPDATES

Automatic upgrades and updates are considered the ultimate necessity by conventional security software and we consider them as the ultimate danger. Automatic upgrades are the single most important vulnerability on the Internet and are just as mad as allowing a surgeon to operate on you remotely at any time and for any reason, without informing you about the consequences and risks of the surgeries.

There is a huge confusion between updates and upgrades. Microsoft itself uses the term "update" instead of "upgrade" on a regular basis. We define these terms for clarity in this submission.

> **Update**: involves only data, not programs, it is not dangerous unless the update concerns security settings or unauthorized access to the data!
> **Upgrade**: modifies the programs of our computers and therefore is ALWAYS potentially dangerous as the system can become highly unreliable very quickly.

Updates happen all the time, for example when the clock of your computer synchronizes with the clock of a server online.
Upgrades of programs should ONLY happen when needed, when these programs need to evolve to accomplish new needed tasks.
Automatic updates and upgrades of security software not only make the system totally unreliable, they are used by malicious hackers and malware to infect computers with viruses spreading at record breaking speeds.

Our Solution: CFF does not need updates, upgrades and patches

This feature removes the need for the majority of upgrades and updates for other software as well. Adding a few settings in CFF in 1 minute can replace many hours, or weeks of programming to design a security software to do the same task. The main advantages are: reliability; stability; longevity; and low cost. CFF keeps the device as reliable as the day it left the supplier.

The cost of maintenance of the device is drastically reduced due to no infections from virus or malware attacks, no need of upgrades and reduced scanning extends the life of the hard drives. It also reduces significantly the need for upgrades of the operating system and many other programs as most upgrades are needed for fixing security vulnerabilities. This saves internet usage and eliminates down-time involved with updates.

3) The dangers of scanning hard drives

The large majority of conventional security software are scanning the drives. Most attacks are unreported. The scanning is not completely effective in detecting computer threats on the Internet. Malicious hackers can test the malware they design against the scanners of conventional security software and design so it is undetectable before releasing it. Scanning hard drives on a regular basis consumes a lot of computer resources and represents a security risk as this process can be hacked. It ages the hard drives unnecessarily, which is a problem in itself.

Our Solution: No scanning. CFF is a malware repeller and does not scan the hard drives.

Scanners are all potentially dangerous. CFF works by monitoring actions of programs and therefore does not need to scan the hard drives at all. Gamers using CFF have a very fast computer with reliable protection and have a competitive edge in their games.
The scanning of drives is the kind of action that spyware undertakes. Detecting and preventing the scanning of drives reduces the power of malware and allows the users to detect the malware more easily.

4) The dangers of uniformity

If everyone uses the exact same security software and security settings, then the defensive mechanisms of our computers are predictable and the work of the malicious hackers is made considerably easier in designing malware which will not be detected for many years.

Our Solution: Customisation. CFF is totally customisable.

The level of flexibility of CFF's settings is extremely high. Advanced users can design settings to add layers of protection for particular software or data such as the private keys of computer games. CFF can be used to protect the settings of the games which are highly valuable and targeted by spyware. CFF can be set to protect files, programs and settings in ways that no other software can, controlling what data can be accessed by what program and by whom at the keyboard, how the data is accessed and it can even detect attempts to steal private data by a remote or local attacker. Customisations make the work of the attackers much more difficult and risky. CFF can protect software and hardware in unique ways. Layers of protection can be created to give a totally customisable security.

5) The growing need of resources for security software

Conventional security software require more and more memory and resources to handle the regular scanning, updates and upgrades which have to be done more and more often to keep up with the growing threats.

Our Solution: CFF is very small and consumes very few resources.

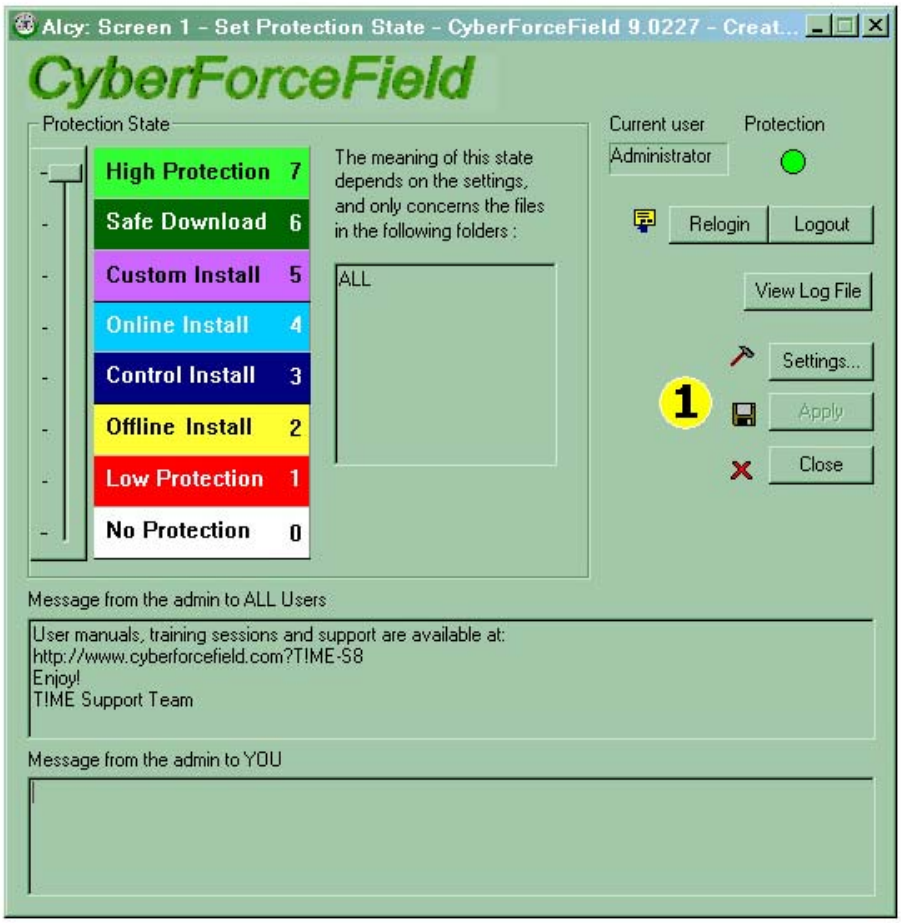
This is a huge difference with the majority of conventional security software. CFF's installation program is about 500 Kb and can be sent by email. It does not consume many resources as it only focuses on dangerous behaviours which is relatively rare as the malware is repelled in the first instance. To do this, CFF consults a very small database compared to the one needed by traditional techniques. It has a small footprint on the hard drive and uses minimal resources, freeing up important system memory. Actions happen without delay, the device will run much faster than with conventional security software.

6) The vulnerability of computers at ALL times

Conventional security software either allows the upgrade of programs at any time or shows pop ups to the users which can easily be disregarded or mistaken. If the computer is able to install any software at any time, such as an automatic upgrade, then it is also vulnerable to attacks at any time. Most attacks start with the installation of an unauthorised program. Installations of programs are the most dangerous action a computer can do, as all infections start this way.

Our Solution: Protection state.

Is it not logical to reduce the protection of the computer only for the times when a dangerous action is needed? To control the time when the computer can be infected by a malware should be the first and most important control of the end users. CyberForceField has a unique protection state level (see image below):



The only time when the malware has a chance to be installed in the computer is during the installation of software. By controlling when and how these installations occur and by monitoring the actions of the programs used during the installation, we reduce considerably the chance of malware infections even when we install an infected program because we can detect dangerous behaviours of programs.

The "Control Install state" allows an installation by backing up the files which are modified during that time. This can be used to monitor dangerous behaviours of software and back up on the fly the data needed to recover from a malware infection.
The "Custom Install" state is a revolutionary step forward: it allows the complete monitoring of the programs we install during and after their installations. **In other words, CFF can force programs to behave safely even before they are launched for the first time**.

7) Lack of protection against attacks by a user at the keyboard itself

The majority of conventional security software can be easily disabled within a few minutes by a user at the keyboard.

Our Solution: CFF is Multi-users and can protect against attacks at the keyboard.

CFF protects itself well. It can protect against all kinds of attacks at the keyboard, even in safe mode, apart from attacks such as the robbery of the computer itself. Because of its capabilities for extreme customisation, it can monitor the actions of the users at the keyboard, the programs and data they can access and detect dangerous behaviours such as attempts to access important or sensitive high security files with unauthorised programs.

2.2 LACK OF CONTROL OF THE END USERS

8) Little knowledge of the end users

End users have little knowledge and understanding of what the computer is doing in relation to security. They rely entirely on their security software and, as computers become more and more complex, have little interest in learning about security. Besides, conventional security approaches are no longer adapted to the current threats, as a result, they are at risk of being tricked easily by an attacker in taking the bait of an attack.

Our Solution: CyberMartialArts (CMA).

CMA is a totally new concept made possible with CFF: the art of defending a computer is only possible with the flexible tools necessary to control it. According to us, Security cannot truly exist without control and understanding. CMA uses a full range of techniques to build custom protective layers which can trap or stop the most experimented attackers and the most sophisticated malware. Several belt levels help evaluate the level of skills of the students in CMA.

CMA focuses on 100% protection, even against brand new threats. Conventional security software has very poor detection and prevention rates for new threats. 99% detection

rate would not be good enough today and they currently have much lower rates (reference Proactive tests of av-comparatives.org – May 2009). We believe CyberMartialArts will revolutionize the way computer security is taught at school and will set a new standard. For more information about CMA, click here.

9) Lack of competent trustworthy personal support online for security issues

There is no reference we can use to appreciate the level of competence of a support person in relation to computer security.
Conventional support is not addressing the flaws mentioned above.

Our Solution: Competent support team trained in CyberMartialArts

A team of people trained in CyberMartialArts using face to face communication tools such as Hotconference and Web Site Communicator. The various belt levels of CMA provide a scale of reference to appreciate the level of knowledge of the support person in relation to a security issue. The communication face to face makes it easier to authenticate each other and the communication is much more effective.

10) End users have too little control over what the computers are doing

End users have far too little control over what the computer programs can do, have too little knowledge to understand the impact of the actions of the programs, and little interest in learning more. They do not have the tools to enforce our privacy laws.

Our Solution: Open Actions

We have created and launched the concept of OPEN ACTIONS: transparency of all the operations, activities, transactions of the computer which can impact the security or the privacy of the end users. To learn more about "Open Actions" click here.

The following can be achieved with ease, using CFF and CMA:

* Compartmentalisation of the computer functions and data.
* Control of the users: the data they can access and modify.
* Control of the software: the data it can access and modify.
* Access to sensitive data from external disks can be blocked.
* Any file (or folder) can be monitored (highly important for the privacy laws).
* Attempted breaches of security are listed with full details of the events.
* Data can be invisible to Windows, but still accessible by authorised users.
* Control over the Windows operating system, negating all vulnerabilities in Windows.

Examples:
Action 1: To access the file containing private emails. (or any other sensitive files containing private data, private chats online, important databases, address books, accounting records, password files, etc.)

Action 2: To format the hard drives

Action 3: To alter a particular setting stored in the “registry”, very important files of the operating system.

Action 4: To install a new program in the computer.

With “Open Actions”:
These actions are totally transparent to the administrator of CFF who can
- Assign permissions to perform these actions to legitimate programs and users at the keyboard.
- Restrict the type of access (read only, modify, copy, delete, hide, etc.)
- Detect the programmes and users responsible for attempts of breaches.
- Keep a historical record of all attempted breaches.
- Detect malicious behaviours of programs and users at their first attempt, not after the damage or breach has occurred (proactive protection).

3. Conclusion

The flaws of the computer security industry are huge and have not been addressed for over a decade. All these points make the combination CMA with CFF the most effective approach to handle an exponential growth of computer threats and can revolutionize the way computer security is taught particularly in schools where we believe the CyberMartialArts component of our system will have high appeal.

The exponential growth of malware online forces us to change drastically the way we approach security and privacy online.
CyberForceField (CFF) and CyberMartialArts (CMA) secure the Windows Operating system to a new level, never attained before, and can make a difference in the computer security industry, the economy of the country, and the world.

Our security software business is a small enterprise with an incredibly innovative product that offers a new model for security. The challenge for our organisation, like many innovators, is changing the current thinking processes. We cannot fix the problems we have using the same thinking that created these problems. New approaches need to be taken. The role of government in helping to raise awareness of these new approaches is paramount. It is very difficult for new entrants to the industry to compete with the brand power and market awareness of existing security providers. Government intervention should not be about providing handouts, but about providing the opportunity for genuine, independent testing of new and innovative options.

Please feel free to contact me if you require further information.

Alcy Infinity
CEO, Timesavers International Pty Ltd

http://www.timesaversinternational.com
http://www.cyberforcefield.com
Tel: 02 6629 5358
Email: