Global Information Assurance Certification Paper

Using Computer Worms to Carry Hidden Information

Ron Friedland
GSEC Option 1
June 3, 2004

Abstract

The history of secure communication and data storage has been one of successive measures and countermeasures growing ever more sophisticated. Even when the technology of securing information seems unshakable, there are back doors that break even the best schemes. Now a variant of a malicious computer technology shows some promise at being able to transmit secure data discretely.

Computer worms and viruses were originally developed for benign applications. Corruption of benign programs and malicious programming have made many viruses virulent and destructive. This parallels the situation with biological viruses where some can be beneficial and some are destructive. The computer virus is shown to be a potential carrier for hidden information in a way that overcomes many of the strongest objections to using viruses for beneficial purposes.

Secure Communication

Imagine the following scenario: Government agents are convinced they are on the trail of a terrorist sleeper cell. The malicious operatives seem very secretive and suspicious to the G-men. They have money when they need it. They only go out for necessities and then only send their youngest roommate to smile and interact with the public. They lead a wasted lifestyle. The television is always on and they are constantly surfing the web for pornography. The agents monitor all web traffic. Every site the suspects visit is inspected. Every link, every picture, every bit of text, every cookie is analyzed. One day they visit a favorite porn site on the web and a computer worm downloads. Their system is taken over and a chaotic picture of the Devil in Hell comes on the screen and warns them of the evils of carnal pleasure. The agents retire to their favorite bar and celebrate the seeming misfortune of the suspected terrorists. “They can’t surf the web any more,” the senior agent says with a laugh before he downs another drink. Inside the dingy apartment the terrorists smile. They don’t need to surf the web any more. A secret message was buried in that satanic image. Their orders have come.

The transfer and storage of secret information can be a “life or death” issue. Mortal enemies need to communicate with their forces in ways that can’t be read by the other side. There are several ways to accomplish this task, each method having its strengths and weaknesses. The skilled communicator will have a toolbox full of methods and the choice of which one to use in the proper circumstances. The best choice is one that the enemy does not suspect and cannot counter.

The direct, physical transfer of information from one operative to another is often the first method of secret communication. It can consist of a whispered message or a note passed in class. It requires no special hiding of the content of the message. Modern technology has provided us with storage devices that are easily concealed and carry large amounts of data. Classic methods of contact provide a channel for the transfer of these devices without the ability of hostile operatives to monitor the content remotely. In the right circumstances, this is an effective tool.

However, passing messages is an old practice and is foiled by the same low-tech detective work that has worked in the past. One weak point is the ability of hostile agents to determine who the operatives are and to monitor their activities directly. The identification of one member of a group can lead to the monitoring of all the contacts of that operative and destroy the secret nature of a clandestine group. The capture and detention of an operative at the right time can reveal the preferred method of transfer of information and, if the message is clear, can disclose the contents of the secret communication. Humans are more easily intimidated into revealing secrets than are machines and an operation can be compromised if a susceptible agent is in custody or has turned against his former allies.

In order to secure the information being transferred, the content can be altered in such a way that the message is meaningful to the target of the transfer but is incomprehensible to a stranger reading the message. This can be accomplished by the use of prearranged codes. Admiral Yamamoto signaled Nogumo's fleet to proceed with the attack on Pearl Harbor in 1941 by exhorting them to "Climb Mount Nitaka!"[1] There was no mountain to climb but the signal was clear to those in the know. The operation proceeded. The code had been prearranged. It is difficult for a naïve eavesdropper to decode such messages, so they can often be sent anonymously knowing they might be intercepted but not understood. However, the need to prearrange codes may give rise to codebooks that can be procured by an adversary who will now be able to understand all transmissions. This also limits the messages only to those that have been anticipated.

If the codes substitute for words rather than for sentences the number of possible messages increases. However, these are also vulnerable to manipulation if the carrier is under hostile control. American censors monitored messages sent overseas during the World War II era. One message read, "Father is deceased." The language seemed unnatural. The censor restated the message as, "Father is dead" and had it sent. A reply came back quickly. "Is father dead or deceased?"[2] With that one move of the censor's pen, enemy communication was disrupted and two operatives were disclosed.

Being able to send messages openly has its advantages, but the vulnerabilities

can be devastating. In those cases in which more complicated messages must be sent, using ciphers is an option. Ciphers use methods of substitution and transposition to obscure the content of the messages they bear. Simple ciphers have been used for over two thousand years. In the simplest substitution cipher one letter is substituted for another. The method can be as simple as substituting the next letter in the alphabet for each letter in the message. In this way the message, "THROW THE BALL" becomes "UISPX UIF CBMM". In transposition ciphers the order of the characters in a message is changed. One of the simplest methods is to reverse the order of each pair of letters. In this way the message, "THROW THE BALL" becomes "HTOR WHT EABLL". If both substitution and transposition ciphers are used in the same message the new cipher now becomes "IUPS XIU FBCMM". Enciphering can be done electronically. Increasingly complicated methods have been developed and broken.[3]

Electronic methods of enciphering have been developed that appear to be invulnerable to direct attack.[4] The trick is to use an algorithm that requires a large key containing several bytes of information to direct the encryption. The key can be so large that it is, effectively, secure against brute force attack by guessing possible keys. The vulnerabilities lie in other areas such as protecting the identity of the key both in storage and in transport and in finding alternative methods of breaking the code. The Allies broke both the German and the Japanese encryption routines in World War II with powerful results. When the Japanese were planning their attack on Midway in 1942 they used a method of coding that gave the allies precious few insights. All that was known in one case is that an attack was planned on "AF". The Americans were uncertain about the identity of AF. Commander Joseph Rochefort, chief of the Combat Intelligence Office, who suspected that Midway was the target, solved the problem. He knew only a few of the encoded words in the Japanese code but what he did know was critical. He directed the American communications on Midway to announce clearly that the freshwater condenser had broken and the island was now short of water. The Japanese code announced a shortage of water on "AF". With only a small fraction of the code broken and a clever insight, the contents of a vital message were disclosed.[5]

Even when the contents of an encrypted message remain secure, the mere act of sending and receiving encrypted messages provides information to an adversary. Lines of communication are disclosed. Communicating with suspect sources identifies potential adversaries. Correspondents who want to transfer secrets are at risk of divulging information even if their adversaries never see the information they are passing. Traffic analysis looks at the frequency and length of messages and can detect patterns that indicate activity and impending action.[6] If those who communicate choose continuous or frequent transmission, they clearly indicate an association. Selecting intermittent transmission makes the lines more obscure but allows for traffic analysis.

There is an element of security in being able to transfer information through an indirect connection between the parties and a method seemingly so benign that monitors will see little amiss when the message is transferred. Misdirection is a powerful tool to this end. In some cases, the misdirection can be quite effective.

The Allied secret agent Cynthia was a seductive woman of great importance to the intelligence community in World War II. She once had convinced a sympathetic official to disclose the contents of his safe to her in the dead of night. To their mutual horror, the noises outside indicated that they were moments away from being discovered. Cynthia acted quickly and demanded that both of them take off their clothes. When the guard arrived to check on the reason for activity in the office late at night he saw a couple preparing for a passionate encounter. The guard apologized and left without questioning the breach in security.[7]

Misdirection can work in electronic media also but without the excitement of the Cynthia story. Steganography is the art of hiding information within another set of information. Pictures, music, text, and executable code have all been used to hide content. In one form of steganography, text may contain hidden messages if letters or words are extracted in a particular pattern. This paper contains steganographic references to the identity of the author and two associated educational institutes. In another form of steganography, a gif picture is modified from its matrix of 8 bit pixels to contain the most significant bits of the cover picture and to have the most significant bits of the hidden picture placed in the position of the least significant bits of the cover. The hidden information can be graphic, text, or some other format. The content can be encrypted to prevent the information within the carrier from being disclosed to an outsider.[8]

It is the goal of steganography to keep the carrier image intact while containing the hidden information. Hiding an image within another is the rough computer equivalent of painting over another painting. The casual observer will see the picture on top and not know that another lies beneath it. The informed observer will know to strip away the upper image and reveal the hidden picture below. The suspicious observer will probe the bottom layers to see whether any recognizable image is present.

Techniques do exist to disclose the presence of steganographically-hidden information. Since an effective way of testing the detectors is to test them on data originating with known steganographic algorithms and since many of the detectors work by reversing known steganographic algorithms, there is the potential that unpublished steganographic algorithms might evade detection.[9] Since steganography can be combined with encryption, even if the ruse is detected, the information contained in the message will not be compromised. Still, the attempt to communicate lends itself to traffic analysis, identification of operatives, and jamming. The ideal steganographic carrier will be one that

effectively hides the secret information and that can transmit such that it is easily overlooked.

One of the techniques that had been explored for the steganographic transmission of information is in picture files on third party web pages.[10] Thus any contact between the communicating parties might seem to be casual and unrelated to the transfer of secret information as the communication could be accomplished without the two parties ever directly contacting each other. It seems to be a secure channel, but there are countermeasures available. The web host could scan for steganographic images and alert authorities whenever one appears. Pictures could also be wiped clean of steganographic images before they are accepted for display on a third party's web page. Even more troublesome to those trying to communicate by these images is the possibility that the steganographic images could be altered such that the hidden data is scrambled. In this way the communicators could be identified to a degree, the secret communication denied, and deception forced on those who rely on this channel. Even if the messages do get through, a raid on the computers of those who communicate through steganography could yield steganographic or encryption software and forensic techniques can disclose copies of deleted images on a disk.

There is another method of communicating secret information electronically that is more secure, at least for now. No special steganographic or decryption software needs to be present, yet the messages can be hidden and scrambled securely. A scan of the web page that carries the secret information might yield nothing of interest to the unsuspecting investigator who analyzes every image, yet the information can be transmitted selectively to the intended receiver without him having to click on a particular image. Secret information can be transmitted selectively, disclosed to the intended recipient, and then wiped out automatically leaving no trace of message or enabling software. To understand how this is done we need to examine the computer virus.

New Uses for Computer Viruses

Several physical attacks have plagued humanity throughout our existence. As horrible as they are, they are tangible and we know how to counter them. Cyber attacks are another kind of threat. Malicious software, known as malware, threatens to take down essential elements of today's society. Electrical power, banking, communication, and transportation are all dependent, to some degree, on networked communication and have some degree of vulnerability to assault. Self replicating programs can work their disruption through a launch and forget strategy. Software kits abound that allow even a relatively unsophisticated user to design such malware and to configure the damage that it can do.[11,12] The potential of such programs is just beginning to be recognized. They disclose themselves like a wild animal raging at the system, prepared to do maximum damage. Yet they can be tamed and trained to perform subtle, sophisticated tasks.

A common label for malware is “computer virus” although the virus is only one kind of malware. Viruses and worms have the ability to replicate themselves, infect other computers by transmitting their information over electronic links, and to disrupt the system with their payload, an optional part of the program that specifies an action to perform that is often intended to be destructive. The virus needs a carrier such as an email message while the worm can transmit itself without intervention from the user. In this way, the worm resembles a cookie that can multiply and reinfect. The creation of new viruses is countered by the enhancement of disinfection programs that seek to prevent virus attacks or to minimize the damage once a system has been infected.[13] There is a perpetual cycle of the introduction of new or improved viruses and the establishment of countermeasures. It is very similar to the way in which viral attacks occur and are countered in biology.

New biological viruses arise from time to time and infect a population. If a virus kills everyone it infects, it soon runs out of susceptible victims and the remaining population is genetically immune to it. This kind of virus has a relatively short existence. Recent research indicates that this may have happened to the Chimpanzee population about two million years ago with the AIDS virus. The AIDS virus now no longer infects Chimpanzees.[14] When a virus hits an individual, the victim develops an immunity against the virus, as is the case with smallpox, and, often, to related viruses as is the case with vaccinia and smallpox.[15] These viruses are well known because of the damage they cause. However, there are viruses that cause less damage and persist in the host population. The common cold is rarely fatal but it lingers, persists in the population, and mutates to reinfect otherwise immune victims.[16] Bacteria have viruses also, called bacteriophage. The bacteriophage “lambda” has been studied extensively. When it infects a cell it makes a decision whether to grow and kill the host or to remain dormant within the cell and to survive as a part of its host.[17] The major killers such as smallpox and AIDS get a lot of attention and vast campaigns seek to eradicate the disease. The less virulent infections exist happily in greater abundance than their greedier cousins.

So can it also be with computer viruses. The virus payload need not be destructive, disruptive, or even readily visible. The less visible it is, the more likely it is to escape detection. Such invisible viruses can be engineered to be less virulent and to carry payloads that can have beneficial effects. Such is also the case in medicine where genetically engineered viruses are being investigated as potential vectors in the remediation of genetic defects.[18] Computer viruses can also be engineered to control their replication and conditions under which they will infect.[19] By applying rules as to when the virus should transfer, the program can transmit to some users while remaining invisible to others.

Rules may help manage the transfer of viruses but are counterproductive when considering payloads. The new computer virus payload can be nearly anything

ranging from executable code to pictures, sound files, or text. All of these can be vectors for steganographic data.[20] Since quality control is not usually a priority in virus construction, poor grammar, imagery, or code that might contain hidden data that would normally compromise the quality of the carrier will not seem so out of place. Rather than taking deliberate steps to download data, the malware can transfer on its own, as a worm or even a cookie, when a site is visited. Specific signals can help determine which users get the virus and which ones never see it. The virus can be prevented from reinfecting once it has been transferred, thus avoiding the proliferation of the secret data. All support software can be hidden within the virus and an infected user can deny, plausibly, that it was his intent to have that information on his computer.[21]

One of the ways in which the presence of steganographic data is disclosed is in low information content signals that vary more than would be expected. [22] Less information can be hidden in quiet passages than in noisy ones or in soft, white space than in a swirling mix of color. Since code, pictures, sound files, or other steganographic carriers that might be present in malware might reasonably be expected to be chaotic in a program intended to be disruptive, disclosing a steganographic message by analyzing relatively stable components of the carrier might be especially difficult because they are so rare. Decryption routines capable of making sense of the hidden messages could also be contained within the executable code of the virus. The virus can disclose its message with the proper signal and keep it hidden otherwise.

Not all viruses are meant to be harmful. The concept of a beneficial computer virus or worm has its precedents. Koh is a memory resident boot virus that, with permission, encrypts the hard drive. It has weak and strong encryption and will deactivate if the user supplies the same password supplied when the information was originally encrypted. It even allows the user to uninstall the virus. Since it has access to the boot sector, it can deny an unauthorized user access to the system. [23]

Such a virus is not meant to spread at random. It can exist without self-duplication capabilities. It is generally transmitted to a machine with the owner's knowledge and agreement. The feature that distinguishes it as a virus is the ability to "infect" the boot sector of the hard drive. Such a program is novel, but the inability to self-replicate calls into question whether this is really a virus, although that capability could easily be added to the program.

Perhaps the first worm ever programmed was intended to be beneficial. John Shoch, working with Jon Hupp, devised the worm to send a specific program to every computer in his local network. It saved him the time of loading each computer directly and it enabled the computers to speak more directly with each other. The new kind of program gave computers the ability to pass along data and instructions automatically among themselves.

The science fiction literature of the time seemed more concerned about this type of program than Mr. Schoch was. The 1970 movie Colossus: The Forbin Project depicted two supercomputers that took over the world once they were allowed to communicate between themselves on their own. Schoch even got the name of the program from the "tapeworm" program that was used in John Brunner's novel The Shockwave Rider to destroy a sinister computer network.

Schoch designed his worm to be well behaved. It would run at night and sleep during the day and was designed to save system resources. It was careful not to overwrite files. It seemed to be working well until 1978 when the nocturnal worm went from being a housecat to being a vampire beyond the control of the programmer.

A small worm was set loose in the network and became corrupted. The corrupted file crashed the host computer and spread, causing other computers on the net to crash. Rebooting an infected computer did little good. Even if it were cleared of its worm, there were plenty more waiting to come on board. Before the internal self-destruct command could be activated major damage was done the network. Although spiders and bots still survive as programs on the net, a worm or computer virus intended to be benign still has the ability to rise up and raise havoc. [24, 25, 26]

Fred Cohen, a leading advocate for the beneficial uses of computer viruses devised a self-replicating program that would automatically compress certain files to save disk space. It died a quiet death when disk space became cheap and plentiful.

One of the greatest opponents of the use of beneficial computer viruses is Vessilin Bontchev of the University of Hamburg's Virus Test Center. He lists twelve problems with using beneficial viruses. Dr. Bontchev's ideas apply to those viruses that are intended to persist and provide service several times. However, a worm or virus containing steganographic information may need to have a short lifetime for security reasons and exists for different reasons than previous beneficial viruses.[27]

The twelve Bontchev problems are that beneficial viruses are (paraphrased):
difficult to control,
wasters of resources,
difficult to identify and remove,
prone to bugs,
incompatible across platforms,
inefficient,
inclined to function without consent,
prone to invalidate tech support,

a disguise for true malware,
a disguise for research to develop malware,
a resource drain without consent,
a way of minimizing the public's skepticism of malware. [28]

None of these drawbacks are a problem for the use once and throw away communications tool that's intended to remain a secret. Even if the virus communication is reused, the presumed buggy and inefficient nature of the tool can be used to disguise hidden information. Self-replicating software ceases to be self-replicating once its "time to live" has expired. The previous concepts of beneficial computer viruses have all assumed that the programs should persist and be generally available. The Bontchev objections are directed to this kind of program. The fact that the general distribution of a beneficial virus can be problematic only means that the use of a virus to transport sensitive information might be even more appropriate. Instead of programming viruses with a "time to live" they might be programmed with a "time to evolve" after which they transform from a carrier of information into true malware with no information content. In the right hands a shortcoming of a program could be a feature in a new application.

Conclusion

The use of a computer virus as a vector for secret communication can introduce plausible denial in legal settings. It can obscure that a secret message was even sent deliberately. It can provide a context that makes it easier to store encrypted, steganographically-hidden data without it being obvious that a message was contained. It can hide itself from view from unintended recipients yet still transmit its contents to the proper target. It can provide a self-contained decryption algorithm that responds to a given context or key and that can destroy itself after use. It can blow up in the face of a naive analyst who might be inclined to disinfect the system and destroy the virus that contains the wanted information. That would provide an ironic method of hiding the secret information.

This is not the end of the utility of computer viruses. The same positive features that can apply to biological viruses may have their counterparts in computer viruses. Since computer viruses are currently regarded by many only as undesirable malware, they provide a method for hiding secret transmissions. Computer viruses can cross international lines when direct communication might be prohibited. The current low opinion of the beneficence of the computer virus provides an opportunity for secret communications today, but recognition of the capabilities of the virus may open new doors as quickly as the old ones close. If suicide bombers are willing to sacrifice their own lives for nefarious ends, the temporary sacrifice of a computer system for the sake of secure communication might seem very affordable.

As Albert Szent-Gyorgi said, "Discovery consists in seeing what everyone else has seen and thinking what no one else has thought."[29]

References

1. Pearl Harbor Attack – 1941 http://history.acusd.edu/gen/WW2Timeline/Prelude23.html (2001)

2. Kahn, D. The Codebreakers Macmillan (1967) http://www.jjtc.com/Security/sbib01.htm

3. http://www.tech-faq.com/cryptology/substitution-transposition-cipher.shtml

4 Unruh, Bill (1998) http://axion.physics.ubc.ca/crypt.html#IDEA

5. Prange, Gordon W. Miracle at Midway McGraw Hill (1982) 45-46

6. Orsulic, Josko Traffic analysis Experimental Reference Center for Cryptographic Data Protection (1996) http://pgp.rasip.fer.hr/pgpdoc2/pgpd2_60.html

7. Stevenson, William, A Man Called Intrepid Harcourt, Brace, Jovanovich (1976) 336-338

8. The Stego Archive http://www.stegoarchive.com/ (2003)

9. Guillermito A Few Thoughts about Steganography
http://www.guillermito2.net/stegano/ideas.html (2004)

10. Bagnall, Robert J. Reversing the Steganography Myth in Terrorist Operations:
The Asymmetrical Threat of Simple Intelligence Dissemination Techniques Using Common Tools
SANS Institute (2002)

11. Tarala, James Virii Generators: Understanding the Threat SANS Institute (2002)

12. Pearson, David Psst…Hey Buddy, wanna create a virus? SANS Institute (2003)

13. Trend Micro Virus Primer (2004)
http://www.trendmicro.com/en/security/general/virus/overview.htm

14. CNN Chimp disease clues to AIDS (2003)
http://www.cnn.com/2002/WORLD/europe/08/30/aids.chimp.dna/

15 Centers for Disease Control and Prevention SMALLPOX FACT SHEET **:** Vaccine Overview
(2003) http://www.bt.cdc.gov/agent/smallpox/vaccination/facts.asp

16 The Common Cold Center The Common Cold
http://www.painforum.com/en/1/ngcfcold.html

17. Ptashne, Mark A Genetic Switch Gene Control and Phage Lambda Blackwell Scientific Publications and Cell Press (1986) 3-5

18. Human Genome Project Information How Does Gene Therapy Work? (2003)
http://www.ornl.gov/sci/techresources/Human_Genome/medicine/genetherapy.shtml#work

19. Cole, David administrator cmc.net personal communication (2004)

20. Kessler, Gary Steganography: Creating and Detecting Hidden Messages (2004)
http://www.sans.org/webcasts/show.php?webcastid=90476

21. Cole, David op cit

22. Kessler, Gary op cit

23. Metropolitan Network BBS Inc., Bern, Switzerland (2003) http://avp.ch/avpve/boot/koh.stm

24. Benefits of the Computer Virus http://greyowltutor.com/essays/virus.html

25. CNET Fast-Spreading Code is weapon of choice for Net vandals
(2004) http://att.com.com/2009-1001_3-254061.html

26. Schoch, John F., Hupp, Jon A.
The "worm" programs—Early experience with a distributed computation
Communications of the ACM v25 #3 (1982) 172-180
http://portal.acm.org/citation.cfm?id=358455&dl=ACM&coll=portal

27. Moorer, Greg The Case for Beneficial Computer Viruses and Worms
csrc.nist.gov/nissc/2000/proceedings/papers/601.pdf

28. Bontchev, Vesselin Are 'Good' Computer Viruses Still a Bad Idea?
http://vx.netlux.org/lib/avb02.html

29.http://quotes.telemanage.ca/quotes.nsf/quotes/14a842e0c54873be852569800003ff24