Return to Table of Contents Return to last document
Query Query results Find Find again

Man, Myth, Memetics and Malware

David Harley
National Health Service Information Authority, UK

Urs E. Gattiker
Aalborg University, Denmark

About the Authors

David Harley works as a senior manager for the UK's NHS Information Authority. As Threat Assessment Centre Manager, he specializes in risk assessment, alerts, advisories and patch management, and security incident reporting and tracking. As virus management technical lead within the NHS, he is also coordinates virus incident response and plays a major role in the implementation of national solutions. His other professional affiliations have included AVIEN, AVAR, Team Anti-Virus, TruSecure, the WildList Organization and EICAR. His publications include a number of books, conference papers and articles in the security and anti-virus fields.

Mailing Address: National Health Service Information Authority, Aqueous II, Aston Cross, Rocky Lane, Birmingham B6 5RQ, United Kingdom; Phone +44 121 333 0126; Fax: +44 121 333 0334; Email: david.harley@nhsia.nhs.uk, macvirus@dircon.co.uk.

continued on page 2

Descriptors
Memetics, urban legends, viruses, chain email, junk mail, policy, education, gateway filtering, social engineering, misinformation, hype

Reference to this paper should be made as follows:
Harley, D. & Gattiker, U.E. (2002). Man, Myth, Memetics and Malware. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (ISBN: 87-987271-3-3) pp. 29-63. Copenhagen: EICAR.

Urs E. Gattiker is Obel Family Foundation Professor of Innovation and Technology Management at Aalborg University, where his research focuses on IT security, innovation, and entrepreneneurship. He is a board member of several high-tech start-ups and also of a venture fund. Memberships in professional associations include such as EICAR (board member), US Academy of Management and the American Psychological Society. His publications include a number of books, articles in refereed publications such as journals, best paper conference proceedings and others.

Mailing Address: Institute for Production, School of Engineering, Fib-16, Aalborg University, 9220 Aalborg, Denmark. Phone +45 32 95 50 90 or + 44 70 9237-6036; Fax: +44 70 9237-6036 (dial 3 for fax or 2 for voicemail); Email: Urs@EICAR.org

Man, Myth, Memetics and Malware

Abstract

Hoaxes, urban legends, spoofs, chain letters preceded the Internet but quickly adapted to the new communications media. By 1997 several conference papers and other articles addressed the issue. However, hoaxes continue to proliferate and computer users continue to react inappropriately.

More people can recognise crude hoaxes. However, the load on support staff arising from related nuisances hasn't necessarily decreased. The focus has changed, but policies, strategies and information resources haven't kept pace with the convergence of different email phenomena: viral marketing, spammed hoaxes, spammed viruses, and viruses which piggyback hoaxes. Increasingly, malware writers, spammers, and hoaxers use similar social
engineering and mail-manipulation techniques to trick the recipient into accessing tainted resources like misleading text, infected programs, or pornographic or booby-trapped web sites.

This paper reviews identification heuristics, policies and strategies, going beyond dictionary and simple heuristic detection of hoax virus into the context of other channels of malice and misinformation.

Introduction

On many sites, more resources are consumed in dealing with viruses that don't and can't exist than in handling 'real' viruses (Overton, 2001). (We use the term "site" here in the same sense as RFC 2196: "…any organization that owns computers or network-related resources…the site has the ability to set policies and procedures for itself with the concurrence and support from those who actually own the resources.") (RFC2196, 1997)

Alerts of this sort are not computer viruses in the same sense as boot sector viruses, file viruses, macro viruses etc., but, rather, are examples of social engineering.

Social engineering is often associated with gaining unauthorised access to systems, but the term can also be applied to exploiting the victim's good intentions and lack of in-depth technical knowledge in order to inspire fear and confusion. Typically, this amounts to a denial-of-service attack. The user is unable to make full use of the resources available to him/her because of fear of the imaginary attack. The administrator is besieged by panicking users and has to expend time and resources on reassuring them, validating reports, providing user education, keeping support staff informed, and so on (Harley 1997). This form of psychological manipulation differs from the programmatic replication dealt with in the course of day-to-day malware management, in that the infected "software" is in the mind of the victim. This process is often considered in the context of "memetics", which deals with the transfer of memes (the "unit of cultural inheritance") from brain to brain.

This study aims to shed light on the concept of social engineering in the context of malicious software and memetic replication, contributing to the current discussions about fighting malware and hoaxes.

The purpose of this paper is to advance knowledge about hoaxes and urban legends, and to shed light on the understanding of these terms and their use in a society where Information Technology (IT) is ubiquitous. This was done by: (1) providing some definitions of such terms as hoaxes, urban legends and social engineering; (2) discussing the problems; and (3) outlining some possible solutions for organizations, users, and system administrators.

Literature Review

Gordon, Ford and Wells (1997) included useful analysis of underlying mechanisms and some still-valid hoax detection heuristics. However, the paper also suggested, convincingly enough, that hoax defences were best built upon a set of "trusted sources of information" in conjunction with a healthy scepticism.

This does not mean that it is enough to refer the average user to standard resources, such as vmyths.com or the CIAC hoaxbusters web site. If the precise variant of a particular hoax isn't there, the user may still need to refer back to a more competent authority. Even a systems administrator who isn't particularly virus-literate (not a rare-enough occurrence) may need more than these web pages can offer. A real threat may be derived from or based on a hoax (or indeed vice versa), and may not have reached one of those pages when the user needs it. A hoax may not be listed under the name by which the enquirer knows it. Nomenclature varies between vendors even with real malware, and there is no naming convention in hoax management. Some sites have taken what is sometimes referred to as a 'dictionary approach' by publishing a hoax encyclopaedia. These (not unlike their "real virus" equivalent) are notoriously time-consuming to maintain. Some anti-virus vendor sites and independent sites do so very well, but others are somewhat patchy in their coverage.

Harley (1997) addressed this issue from a system administrator's perspective, emphasising hoax detection heuristics and containment by enforcement of sound customer management policy. A version of this document was expanded into the EICAR Urban Legends Project (EICAR Task Force – Critical Infrastructure Protection -- http://Security.WebUrb.net/trust) and spawned an FAQ on email abuse with particular reference to hoax management, and this paper represents the final phase of that project. (See also Harley, Slade & Gattiker, 2001, Chapter 15)

Jones' Good Times FAQ (1995) is one of the earliest examinations of the subject, but contains some excellent, still valid material, including the parallels between hoax alerts and other chain letters and the memetic references of Dawkins and others. Such writings have included specific material on non-electronic chain letters and real computer viruses in his writings, as well as some useful examples of how coincidence can be misused or misunderstood as part of the process of myth creation (Dawkins 1976, 1993, 1995, 1998; Blackmore, 1999: Dennett, 1991: Dennett, 1995).

Other writings have made extensive reference to hoaxes and other chain letters in the context of memetics. This populist approach to research into metaviruses ("viruses about viruses") may be of more interest to social theorists and academics than to hard-presses system administrators, but at least offers some interesting insights into the social mechanisms underlying.

The above short summary indicates that whilst there exist some sources about hoaxes, myths and malware, a comprehensive and updated overview is currently lacking.

The next section provides an overview of the problems we experience with defining urban legends, chain letters and email, as well as hoaxes and panic attacks, media alerts and other issues that help create myths and urban legends.

The Problem

As this section suggests, chain letters, email or hoaxes nearly always include a replicative mechanism and are based on social engineering whereby the user is being asked to perform an action (e.g., contribute to an effort or warn a colleague).

In this context we can build upon the above but use the following expanded definitions for social engineering:

> Social engineering builds on a person’s desire to be helpful and responsible, whereby the individual is presented with information that will result in actions that would not have been performed otherwise.

However, this is actually a special case of this definition (Harley, 1998)

> (Skilled) psychological manipulation of an individual or set of individuals to produce a desired effect on their behaviour.

The above does not put forward a value judgement. Hence, social engineering can be positive or negative but, regardless, is closely linked to manipulation of the individual targeted. In the positive sense, it could protect a person from information or actions that might be harmful to his or her well-being (e.g., protecting a child from being exposed to certain harsh realities). A hoax is objectionable because it exploits a victim’s desire to be helpful and responsible. Regardless of positive or negative connotations related to social engineering, moral and ethical issues are never far away. Hence, if the object pursued does justify the means applied is at the core of the matter (Gattiker, 2001, Chap. 5).

Below we expand further on these issues, discussing chain letters, hoaxes and panic attacks, media viruses, malware as well as what is usually described, somewhat loosely, as spam.

Urban Legends

Urban legends (ULs) are a somewhat amorphous class of fantasy/semi-fantasy. The alt.folklore.urban FAQ defines an urban legend as follows:

- "appearing mysteriously and spreads spontaneously in varying forms;"
- "containing elements of humor or horror (the horror often "punishes" someone who flouts society's conventions);"
- "making good storytelling;"
- "does NOT have to be false, although most are, accordingly, ULs often have a basis in fact, but it's their life after-the-fact (particularly in reference to the second and third points) that gives them particular interest."

ULs' often owe their creation to unknown originators. They diverge over time into variant forms. In their 'pure' form, they generally survive through their intrinsic interest as a story, and may well be re-told, re-created or passed on more-or-less verbatim by people who don't actually believe them to be factually accurate, or completely accurate. They do, however, have interesting parallels in form and content with some forms of abuse dealt with in this paper. ULs' may usefully be regarded as a broad class of which certain types of chain letter. For instance, they can be seen as a sub-class - classic virus hoaxes would fit well into this group. ULs' rely on unsubstantiated testimony Indeed, urban legend watchers often refer to "FOAF" (Friend Of A Friend) hoaxes, and note the implied moral subtext that often accompanies such stories (http://www.urbanlegends.about.com/library/weekly/aa082497htm).

Chain Letters and Email

According to the Oxford Reference Dictionary a chain letter is "a letter of which the recipient is asked to make copies and send these to others, who will do the same." [ORD] However, CIAC (Computer Incident Advisory Capability) quotes Webster's Dictionary: "A letter directing the recipient to send out multiple copies so that its circulation increases in a geometric progression as long as the instructions are carried out." This perhaps makes the mechanism a little clearer.

Note that by these and similar definitions, the chain letter or email:

- does not have to contain fraudulent or mythological material;
- may include a 'replicative mechanism' (an appeal to forward the message); but
- does not have to contain an appeal to pass it on to everyone in the known universe (or even the recipient's entire address book), such as:

> Schicke diese Mail min. an **5** freundliche und intelligente
> FRAUEN und bereite ihnen hierdurch einen schönen Tag!
> (send this mail to a minimum of five friendly and intelligent
> WOMEN and make their day more enjoyable herewith!)

Furthermore, the above email may also have the characteristic of:

> “Being [an] efficient [replicator] [which] may consist in accumulating a better collection of words on paper…such mutations can happen again and again, and the result will eventually be a heterogeneous population of messages all in circulation, all descended from the same original ancestor but differing in detailed wording and in the strength and nature of the blandishments they employ.” (Dawkins, 1996, Page 171)

Dawkins was using as an example the St. Jude letter, which was doing the rounds of the postal services many years before there was any such thing as ARPAnet. Nonetheless, it summarises rather well the Good Times school of hoax described below. It's arguable that all chain letters (including virus hoaxes) can be regarded as memetic "viruses of the mind" (Gordon, Ford, Wells, 1997).

The CIAC chain letters page (http://ciac.llnl.gov/ciac/) describes the classic chain letter structure in terms of a tripartite model embracing:

- Hook
- Threat
- Request

According to this model, the object of the hook is to catch your interest - for example, an appeal to greed (Make Money Fast), fear of technology (virus hoaxes), or sympathy (cancer victim hoaxes).

The threat is meant to persuade the recipient to keep the chain going. Traditional chain letters threaten bad luck. Virus hoaxes threaten the destruction of systems. At least one chain letter threatens unlimited spam if you don’t forward it. Sometimes the threat is to others: if you don’t forward, a little boy’s dying wish won’t be honoured, or cancer will continue to flourish.

The request is the objective of the letter. For instance:

- **pyramid schemes** and similar ask you to forward money;
- **virus hoaxes** ask you to ‘help’ others by disseminating ‘information’;
- **mydek** type hoaxes ask you to generate money for medical research by forwarding identical messages.

Mailing list sales pyramid schemes ask you to send money, add yourself to the list, and sell on the list, or another token product. However, all chain letter requests include a '***replicative mechanism***' operating *via* social engineering rather than *via* viral code (a computer program).

In fact, it has been suggested (Harley, 2000) that the crucial **difference between** an **urban legend** and a **chain letter** may be that the **latter includes an explicit replicative mechanism**.

One of the upcoming problems in this area is that unsolicited mail is seen as more acceptable than it was in the early days of the Internet. In the heyday of the Good Times

Hoax, it was possible to say with some confidence "Reputable security vendors don't pass on alerts and advisories as chain letters." However, a more recent overblown but genuine warning issued by SANS based on an FBI alert *did* include an appeal to pass the warning on, as well as several other characteristics suggestive of the classic virus hoax. In fact, it may be as well that the warning *was* overblown: the heated, over-capitalised tone and the fact that it was issued on April 1st inspired widespread disbelief. So far, anti-virus vendors seem, in general, to have resisted the temptation to include such an appeal in their advisories and press releases, but it may not be safe to rely on their continuing restraint in such a competitive market.

Even frankly commercial solicitation is becoming legitimised through the use of evasive techniques such as **viral marketing**. This can include material such as surveys that are not necessarily overtly or by intent commercial. For instance, hotmail started offering free services whereby use thereof resulted in the client involuntarily distributing advertising. Yahoo! and Web.de as well as many others have followed suit.

Viral marketing efforts from free services offered by portals may be attached to any email sent from such a service; three examples are listed below from hotmail, Yahoo! and Web.de

- Get your FREE download of MSN Explorer at http://explorer.msn.com
- Do You Yahoo!? Yahoo! Sports - live college hoops coverage http://sports.yahoo.com/
- Darf es ein bisschen mehr sein? Mehr Speicher, mehr Mail, mehr Erlebnis, mehr Prämie, mehr WEB.DE. Der WEB.DE Club - http://club.web.de

While in the above case, viral marketing through the customer may be accepted because it is in return for a free service; nonetheless, the recipient’s consent was never obtained beforehand. Accordingly, viral marketing may reflect various levels of choice. Table 1 outlines the distinctions that could be made.

Table 1: Viral Marketing, “Being Co-opted” and Outright Spam

	Person Subscribes to Free Service – “No-Chain”		**Chain Letter & Spam**	
	Free M-Mail Service	Free Newsletter	Chain Letter – Received from a Friend	Chain Letter or Spam from Party Unknown to Recipient

Originator of Message is Client/Custom-er, Friend or Party Unknown	Friend sends you an email from his or her hotmail account	Subscriber receives newsletter that may contain advertising (e.g., SANS) or be free of any advertising (e.g., Security.WebUrb.net)	Personal friend receives an email message asking one to pass it on to one's own friends Friend mails message to you and others passes on a letter or message received via email to some friends.	Party has collected email addresses on the Internet (e.g., search engine or CD-ROM containing thousands of addresses) Person or firm sends message to thousands of email addresses
Recipient of Message or Content	Email sent from hotmail has commercial message attached to the bottom of the message	Subscriber is permitted to pass on copyrighted information to friend interested in material	Friend receiving chain letter must decide to either delete or possibly forward message to another party/friend message and must decide to pass it on or else decide against this.	Gets email that might ask him or her to do some things

Message attached or or contained in email	Get your FREE download of MSN Explorer at http://explorer.msn.com	"Tip A Friend" You are granted permission to forward INFORMATION SECURITY THIS WEEK to colleagues and friends who are interested. But please do not SPAM.	Schicke diese Mail min. an 5 freundliche und intelligente FRAUEN und bereite ihnen hierdurch einen schönen Tag! (send this mail to a minimum of five friendly and intelligent WOMEN and make their day more enjoyable herewith!)	ADS FILE FINDER – Document Management and Imaging Software for home & small business use. It lets you convert important documents into Digital images, index each one for easy access and file them on the hard disk of your computer and/or CD Rom.
1st Step-Recipient	No-choice	Subscriber bought into service and in turn receives newsletter	Recipient gets email from friend	Recipient gets email from party unkown (spam)
2nd Step - Recipient	Usually not worfwared beyond 1st recipient	Recipient must decide if content is of interest to colleague – than forward	Recipient decides to disgard or forward message to another party	Recipient discards information – possibly reads or even forwards to friend

Note. The above Table is in part derived from Gattiker, Pedersen & Perlusz (2002).

As Table 1 suggests, spam and chain letters may come in various forms. If the person subscribes to a service (e.g., hotmail), advertising attached to every email sent may be needed to pay for the service that is offered free to users. Hence, hotmail and Yahoo! web-based email provides a by-line with advertising (see Table 1). In this case, the recipient must cope with this advertising that enables the provider to offer the free email service to his or her friend who mailed the message. Research indicates that recipients are not offended by such advertising. But its extensive use has resulted in many recipients simply ignoring such commercial messages, thereby questioning the effectiveness of such marketing efforts (Pedersen, Gattiker & Perlusz, 2001).

The 2nd example is the free newsletter. Here the recipient opted-in by subscribing to the service. If undesirable, he or she will unsubscribe. Whilst the person can forward the newsletter, this implies that the subscriber forwards it only to a person that is interested in the content. This is similar to letting a friend share a newspaper. The newsletter does not encourage spamming, whereas the recipient has no choice in accepting the hotmail advertising by-line on an email sent by friend using this service. Negative outcomes are, however, limited based on research. The story is somewhat different in the last two columns.

The third example is a chain letter example but the onus is on the recipient. For instance, when one of the authors received the chain letter about the women, he forwarded it to his daughter and two other friends because the content (not listed in Table 1) was simply funny. However, he deleted the by-line that encourages the recipient to spam.

The last example represents the majority whereby somebody collected or purchased one's email from somewhere and simply spams in order to sell a service. Many of us get several of these each day.

An example not included above from the experience of one of the authors concerns a charitable concern that mailed all its employees an appeal for contributions with an exhortation to "Pass on this message to **all your friends**, colleagues and relations".

This example is particularly unfortunate. It surreptitiously passes on the responsibility for compliance with data protection and privacy legislation (especially as applied to mailing lists) from the advertiser to the first wave of recipients. Those who pass on such mail are also likelier than the chain letter originator to suffer the consequences of old-time Internet protests such as mail-bombing, subscription-bombing, flaming, reporting abuse to ISPs, and forwarding of malicious software.

As Petersen, Gattiker and Perlusz (2001) found in their study, this trend is now also invading cellular and mobile phones by having advertisers and others use short-messaging services (SMS) to reach potential clients and others. But the authors make a distinction between:

A) Using a free Web-based SMS messaging service, while the receiving party gets SMS with a viral message, such as "*Gratis SMS sent fra myorange.dk*" attached.
B) Signing up to receive quality content through SMS (e.g, virus alert), while advertising is being attached in some form such as a URL for getting more information about the event/problem (http://Alert.WebUrb.net)
C) Sending SMS spam to a recipient, whereby advertising is the content of the message sent to the recipient.

In some cases the person may have opted in the type of service outlined under c above (i.e. signed up for such a service), however, in an increasing number of instances this is not the case (e.g., SMS spam). Moreover, email sent to a cellular phone may cost the recipient in contrast to a message sent from a true SMS gateway in some countries (e.g.,Germany – Vodafone). Where such messages are free for the mobile phone subscriber (e.g., Denmark), large portals (e.g., Yahoo!, Jubii) have been forced by telecommunication providers to either stop offering users this free service of sending an email to a mobile phone or else pay a fee. During late 2001, all Danish portals took the service off their sites and today; only telecommunication providers offer such services for free from their SMS gateways.

One of the side effects of the transfer of the chain letter to the IT and wireless age is an increase in bulk. Where terrestrial chain letters used to ask/order that the recipient pass the letter on to a fixed number of secondary recipients, their electronic equivalent is less restrained: after all, it's probably less effort to forward email to an entire address book than it is to forward selectively. Similarly, fast-burner viruses/worms have tended to raise the number of intended targets (address book entries) to the maximum attainable.

Hoaxes and Panic Attacks

As the above suggests (see also Table 1), chain letters and email entail a (memetic) replicative mechanism and may also represent viral marketing techniques used to reach possible customers via email or SMS. Of course, chain letters are not always sent in pursuance of a legitimate or illegitimate commercial or fraudulent agenda, and neither is bulk email.

Virus and other security related hoaxes do share a characteristic replicative mechanism with chain letters. However, security related hoaxes are particularly noticeable for the fact that they nearly always trade on technophobia, a characteristic they share with some "Friend Of A Friend" (FOAF) urban legends.

Why is technophobia such a successful social engineering technique? Recently a sign in a bookshop was observed to read: "We apologise for any inconvenience caused by implementation of a new computer system." This is actually rather typical of the popular expectation of information technology. We expect it to go wrong. Possibly we expect it to go wrong more often than it really does, since alleged computer malfunction (or virus action) is so often used to cover human error. "We can't do it because our computers are down." "We can't recover the contents of your hard disk because it was attacked by a virus." Perhaps the real significance of the Y2K phenomenon is not that so little happened, but that so many people took for granted the inevitability of massive global disruption and death by COBOL. Thus, we seem to find it surprisingly easy to believe in extreme 'punishment' for the mildest lack of caution.

Generally, the Good Times derivative school of hoax are out-and-out fictions. They rely in many cases on the gullibility and lack of technical expertise of the victims. More importantly and unpleasantly, these hoaxes depend on the recipients' altruistic urge to warn as many people as possible about what they believe to be a genuine danger. A number of close-related or derived hoaxes (Irina, PenPal Greetings, Deeyenda, It Takes Guts to Say Jesus, Join The Crew) are 'alerts' about viruses (metaviruses) using a very similar array of "special effects". These are described as spreading over the Internet and having some destructive effect when email or newsgroup postings are read. The hoax victim is warned not to open mail with a specific Subject: field and asked to pass on the warning to as many people as possible.

The heyday of the Good Times virus (in terms of its maximum impact) and its primary variants was around 1994-1995 (Jones, 1995). However, the following extract from a report by the Y2K Risk Assessment Task Force chaired by Sam Nunn illustrates that the mythical “Nth complexity binary loop” characteristic of a common version of the Good Times hoax, survived into the 3rd Millennium.

> “Three other malicious viruses will actually lock a processor in a divide by zero loop, which, if left running for a sufficient amount of time, will overheat the Central Processing Unit, causing it to melt down and effectively reducing the computer to scrap metal"

Variations on this hoax model continue to appear. Older versions resurface as new generations of newcomers to the Internet fall into the same old traps. Frequently, the only significant difference between one hoax and another is the subject line under which the destructive message is supposed to be sent. The continuing cutting and pasting from one variant to another has the beneficial side-effect of making this class of hoax peculiarly susceptible to detection by a well-documented set of heuristics noted by a number of commentators. In fact, this is the only well-documented class of hoax.

Thus some have slipped into the trap of assuming that because this class is conceptually simple to deal with, the hoax problem has been contained. Sadly, this is not the case. While these may still constitute the bulk of chain letter warnings, and are indeed not difficult to handle, even when received in quantity, it’s often the more rare, less obvious types of hoax and associated threats that generate the most work per incident.

Hype Alerts and Media Viruses. The Y2K phenomenon was also fed by the hyping of risks by vendors and consultants, with a vested interest in dramatising risk. Hype alerts, like virus hoaxes, may resemble the sort of horror story so common among urban legends. Accordingly, the perceived horror results in those who fail to take due precautions and buying into the vendor's solution in being punished or suffering negative effects. No wonder mail that exploits these fears lands with a FUD (Fear, Uncertainty, Doubt) on so many electronic doormats.

Alerts are often used as a marketing device by anti-virus vendors and related organisations (factors and consultancies, for instance) seeking to increase revenue. There's a fine line here between responsible dissemination of vital information and trading on the fears of the public. Unquestionably, some anti-virus vendors cross the line from time to time, and factors or consultants acting on their behalf may (not necessarily deliberately) compromise the vendor's good name by overstating their own authority and competence – for example, advertising claims made by a distributor for anti-virus software (What have SIRCAM, 2001).

Other security organisations pose a particular threat of spreading misinformation. They are perceived as authorities because virus management is a security issue. However, just as not all virus experts are experts in other areas of security, not all security experts are virus experts.

- They may be misled into over-estimating the impact of a particular threat, or the size of the contribution of a particular vendor.
- They may misrepresent the nature of a threat, not understanding it properly themselves, or wishing to pass it off as an example of a threat they feel more comfortable with, but which it doesn't truly represent (Intrusion Detection specialists have a habit of claiming a spurious authority in virus management).
- They also tend to favour a full disclosure model in discussing virus issues, because that's what happens in other security areas (Gordon, Ford, 1999). Lengthy discussion of the full/partial/non-disclosure debate is beyond the scope of this paper, but one of the side effects of this orientation is that lengthy snippets of or even complete virus code (sometimes altered to reduce the functionality, sometimes extensively commented) may become more generally available than is desirable. Security Through Obscurity is poor security, but malicious code freely available for copying and modification by those with malicious intent is no security at all (see also Full disclosure and security, 2002).

Organisations may make (sometimes fraudulent) use of fear of malware to sell products that may or may not be related (Y2K, backup software, recovery services, content analysis tools, outsourcing of security services).

As Gattiker and Kelley (1994) and Harley (2002) have suggested, the media may fail to discriminate between:

- Security experts,
- Computing experts,
- Anti-virus experts,
- Hackers versus ex-hackers,
- Hackers versus crackers,
- People who know a little more than they do, and
- Virus-writers.

Organisations with no claim to in-house security/malware expertise may seek to earn brownie points and profit indirectly from the goodwill thus generated. Often this works to the disadvantage of the recipient of such advice: it's noticeable that fast-burning mail viruses/worms inspire a flood of alerts and advisories offering not only generalised warnings to 'be careful' and specific means of identification of individual viruses, but also instructions on manual removal. It is true that commercial anti-virus software often fails to completely eradicate the side effects of malware that modifies the host environment by (for instance) modifying Word's standard menus or Windows registry settings. Nevertheless, advising everyday users to risk their systems by playing with REGEDIT.EXE imposes a heavy responsibility on the advisor to ensure the accuracy and clarity of their instructions. Unfortunately, such aspirant advisors are not always scrupulous.

Real Malware. It has been observed elsewhere (Harley, 2000) that the viruses described in common hoax types tend to resemble Trojan Horses rather than real viruses: all explosive payload and no credible replication mechanism. Apart, of course, from the metaviral, psychological mechanisms employed by all "viruses of the mind". Nonetheless, there is a degree of convergence between hoaxes (and related fictional nuisances) and real malware, which has considerably complicated the hoax management task.

Some virus authors have long chosen to exploit the victim's desire to protect their system as a means of gaining access to that system. For example, real anti-virus software infected with a virus (Smeg), or Trojan Horses or virus droppers masquerading as anti-virus software (Red Team). However, in recent years virus authors have made a conscious effort to blur the distinction between hoax viruses and real malware, as a thread on alt.comp.virus that included the author of Red Team and other malware authors made clear.

It is no longer true to say that one cannot contract a virus by reading text email. Certain VBScript worms can exploit the misleadingly named Preview facility in some versions of Outlook, for instance, allowing the execution of scripts present in the body of the email rather than accompanying the message as an attachment. Nor is it possible any more to say that viruses are not spread via email with a specific subject header. Nowadays, a number of worms do spread in mail with one or more characteristic headers (though a degree of polymorphism to forestall simple filtering by subject field, message text or attachment filename is becoming *de rigeur*).

But **when is malware not malware**?

- **Viruses and worms** are definable by their replicative mechanisms, and commercial anti-virus software sooner or later detects them.
- **Trojans and backdoors** are defined less by mechanism than by their presumed intent, and are detected by some anti-virus and anti-Trojan programs.
- A **Remote Access Tool** (RAT) can drift in and out of legitimacy according to the prevailing legal climate and the consequent degree of nervousness displayed by the legal department.

However, **joke programs**, **fluffy screensavers** and even **games** are freely traded by email and downloaded from the Web. They occupy an ambiguous niche in the anti-virus pantheon. Many are detected by anti-virus software, but not consistently. Two products may variously detect the same program as a joke and as a Trojan. Unfortunately, it is not always obvious what lies behind the classification of a specific joke as malicious. Games are never likely to be routinely identified as malicious by standard anti-virus software, but detection may be offered to corporate clients concerned about the trading of non-productive, unapproved and possibly unlicensed software.

This ambiguity reverberates into the twilight zone between malware and hoaxware. Screensavers are a popular target for hoax virus alerts (Budweiser frogs, for example). One screensaver incorrectly identified by a particular virus scanner as virus-infected (false positive), progressed to a chain-letter hoax/semi-hoax (Ghosts).

The PKZip/PKUnzip compression/decompression utility has been caught up in the malware arena several times. It was a popular target for Trojans masquerading as legitimate programs, and it was incorrectly identified by a widely used anti-virus product as being infected with Maltese Amoeba. After one short-lived Trojanized version was discovered, a vaguely related alert consumed bandwidth totally disproportionate to the significance of the threat and then got a further lease of life attached to one or more full-blown hoaxes.

There is a malicious/joke program called wobbler or wobbling, sometimes found in a file called CAIFORNI.EXE. However, there is a hoax about a virus called wobbler, wobber etc., found in a file called CALIFORNIA. Its reputed destructive effects bear no resemblance to the 'real' wobbler. However, a major vendor at one point identified the joke as a Trojan, and that may have sparked off the hoax.

There are AOL password stealers that masquerade as buddylist.exe, mentors called 'buddies' being a feature of AOL culture. Is this the basis for the Buddylst hoax/semi-hoax? And, of course, there are cases of hoaxes inspiring malware claimed to be the original of the hoax (Proto-T, GT-Spoof). Not to mention AOL4FREE, which mutated into several variations.

The anti-virus industry does not, popular misconception notwithstanding (Harley, 2000) write and distribute viruses to keep its members in a job, but it may have contributed significantly to the hoax problem, in spite of itself, as the examples above suggest.

Furthermore, malware authors have sometimes used supposed or actual anti-virus software as a means of distribution. This may be done by infecting a legitimate program or a self-extracting archive file containing a legitimate program with a virus; by distributing a program claiming to be legitimate but actually a virus dropper, infected document, Trojan horse etc. Alternatively, mail may contain an URL or active link to a malicious site, or a malicious script: indeed, spammers increasingly use HTML mail containing VBS or similar code to link directly to a web site which may include other vexatious features.

Spam. Spam is a term applied to a number of abuses involving the indiscriminate use of email or newsgroup postings to broadcast ‘information’. In an Email abuse FAQ document, this author (Harley, 1999-2001) has used the following broad classifications, following a number of Internet and printed sources (Schwartz, Garfinkel; Barrett).

Usenet spam:

- EMP (excessive multi-posting) - messages posted individually to each of many groups (classic spam)
- ECP (excessive cross posting) - one message crossposted to many groups (velveeta). (one message - many groups in Newsgroups header)
- Commercial postings

Email spam:

- UCE - unsolicited commercial email (junk mail)
- UBE - unsolicited bulk email - sent in bulk to many addresses. May be commercial, but by no means invariably: like its Usenet counterpart, UBE is often used as a means of soapboxing.

Spammers often spam with the intention of advertising a product or a web site (especially sites where each hit earns money from a sponsor), but other motivations may apply, including aggressive violation of remote systems/system users, revenge (compare mail-bombing and subscription-bombing). A not uncommon example of revenge spamming involves implication of a disliked person (especially an anti-spammer) in spamming activities by using their site as a relay, fraudulently inserting their details into the mail headers, using their details in the body of the message etc. The victim of this sort of revenge spam subsequently becomes the victim of various sanctions applied by anti-spam groups and individuals (cf. Spamming, 2001).

Virus/Trojan distribution also features as motivation – virus/worm writers are known to have made use of newsgroup and email spamming techniques to inject real viruses into the wild.

A scam is an attempt to con money or services or information out of the victim. Scams always involve an element of deception, and may be distributed as spam or a chain letter, among other means. Sub-species such as pyramid and Ponzi schemes are considered at greater length in an earlier paper [Harley, 1998].

The (Partial) Solution

Section 1 above outlined the type of problems and challenges system administrators and users must cope with as far as hoaxes, ULs, malicious code and viruses are concerned. In this section we outline what partial solutions can be pursued to reduce the threat and annoyance caused by hoaxes, ULs, spam and viral marketing to mention a few.

Known-Something Identification

One approach, of course, is to check reliable sources of information on current hoaxes and chain letters (the Dictionary or Encyclopaedia approach). (See appendix for a list of such resources).

Anti-virus vendors are often good sources of information regarding real viruses and worms, and some Trojan Horses. Some also have good sections on hoaxes and chain letters, and there are many sites run by independent security organisations and other groups and individuals that also include such information, as well as lists of other types of email nuisances such as hype alerts, scams, and spam. Some web sites are also associated with specialist mailing lists such as SPAM-L. This approach works well enough, over time, for virus detection. Classic virus detection is based on a cycle of get sample, analyse sample, add identification and disinfection (where feasible) to the product: sooner or later, detection becomes more-or-less fixed throughout the spectrum of relevant products. Other types of malware are more problematical. Most anti-virus software detects some Trojans, but not necessarily all possible Trojans. Other objects intermittently detected by anti-virus software include Remote Access Tools, Distributed Denial of Service programs, and joke programs. While these can cause problems not germane to this discussion, identifying them using standard anti-virus detection by search string is not usually one of them. However, very few vendors try to make substantial information available on every virus they detect. As long as their software detects a given threat and reverses its effects properly, publishing information on a known and established threat is often of secondary importance, except as a public relations exercise.

Detection of hoaxes, spam etc. is rather different. There is no absolute standard for software that attempts to detect these types of abuse, though such software certainly exists. However, detection is largely in the eye of the beholder. There are sites that contain excellent information on a wide range of hoaxes and chain letters: however, no-one co-ordinates the sharing of hoax 'samples' among all qualified and interested parties. Furthermore, some have only local currency, and may not become widely known outside a given physical or virtual locality. There is no standard naming convention, so it's easy to miss a hoax that isn't listed under an obvious name. Spam is even more problematical. It's not particularly usual to archive spam messages with a view to detecting it: in any case, the main problem with spam is less with recognising it than with the sheer weight of it.

Automated detection using more-or-less exact identification is less straightforward for hoaxes and spam than it is with virus detection. Search strings have to be rather carefully chosen, and their actual position in the message is unpredictable. Spam filtering, in particular, therefore tends to be heuristic in nature.

Identification Heuristics

Malware heuristics. Welcome to the age of the fast burner. A few years ago, viruses spread comparatively slowly, being mostly diskette-borne, though under some circumstances a file infector could spread across local networks with impressive speed. The first Word macro viruses altered this picture: since people were far more likely to exchange documents than they were executable files, email started to overtake the floppy disk as the infection vector of choice. Eventually, viruses/worms that mailed themselves out to addresses in the victim's address book started to become a major problem – partiallydue to the blurring of the borders between real threats and hoax viruses described above, but (most alarmingly) because of the vastly increased speed of dissemination this mechanism allows.

A fast burner that 'gets lucky' can go global within hours or minutes of its introduction 'into the wild', so that by the time vendors have a fix, melted down mail servers and oversubscribed vendor web-sites constitute serious obstacles to distribution of updates and patches (Harley 2000; Wells, 2000).]

How does this relate to hoax detection heuristics? This type of threat turns heuristic detection into a necessity for more than one reason. At one time, the average anti-virus administrator could gamble on not being one of the first victims of a new virus - mostly, the first victims were seen as being the big corporates, universities, and multi-nationals - and wait for the monthly or even three-monthly anti-virus update cycle to revolve. Now, however, almost any site may become one of those first victims: the first wave of infections may hit hundreds or thousands of sites before a vendor can update its web site or analyse a virus/worm and produce a fix. Conventional scanner heuristic analysis is a fine-grained approach that works on individual files/attachments, but attacks like this may also call for a coarser-grained approach, such as discarding, bouncing or quarantining all attachments; all attachments with a suspicious filename extension or double extension (*.txt.vbs, for instance); multiple instances of identical mail; mail with the same Subject header; mail with identical attachments.

Can this coarser-grained approach be integrated with gateway-filtering approaches to other invasive content? Though such filtering is best done by corporate organisations at the perimeter (as opposed to at the desktop), the filtering criteria vary widely, as indicated below.

While tools for content analysis can be and are packaged together with virus detection tools, the degree to which they can be integrated is severely limited by the divergent nature of the relevant technologies. Content filtering is nearest to virus-specific detection when it focuses on very specific lexical objects: proscribed web sites, domains, source addresses. However, it is more common for such tools to use fuzzier matching techniques, looking for strings suggestive of pornography, fraud, hoax material etc. This more heuristic approach is harder to automate, and entails trade-offs between transparency and service. In general, more transparency/automation entails a degree of denial of service as borderline traffic is discarded (Filtering software: Inaccuracies and mistakes, 2001). There is, perhaps, a parallel here with rate-limiting as a means of countering Distributed Denial of Service attacks: service is maintained at a reasonable level, but at the cost of losing some legitimate traffic.

Chain Letter Heuristics. Chain letter characteristics are pretty straightforward, though not particularly susceptible to automated recognition. "Pass this on to everyone you know, otherwise something undesirable and possibly virus-related will happen." "Pass this on to everyone you know and something wonderful will happen." Of course, a chain letter doesn't have to specify 'everyone you know'. This heuristic works so well only because most chain letters are unoriginal and greedy, chiefly concerned with reaching as many people as possible, as fast as possible, like a fast burner virus/worm that mails itself to everyone in the victim's address-book. A hoax author who rediscovers the principles of sparse infection and delayed gratification in order to achieve long-term survival might change the face of malware/hoax management yet again.

Hoax/Spoof Detection Heuristics. A number of observers (Harley, 1995: Gordon, Ford, Wells, 1997) have noted common features of the classic Good Times derivative hoax family. Indeed, some more recent authors (Schmauder, 2000) have fallen into the trap of assuming that nearly all virus hoaxes are like Good Times derivatives in using extensive capitalisation, just as once upon a time it was assumed that because Lehigh infected COMMAND.COM, that was how all viruses worked. In fact, this author no longer believes that a high match rate against the heuristics listed is sufficient proof of either fraudulent intent or complete inaccuracy: nevertheless, such a score does suggest caution. In combination with a sufficiency of technical knowledge to assess the likely accuracy of an alert, an informed observer can still hope to evaluate most alerts with considerable confidence.

The characteristics below do not constitute incontrovertible proof of fraudulent intent. However, they do suggest at the very least a degree of carelessness that casts doubt about the quality of the information contained.

- Undated, or no realistic or verifiable date. "Yesterday" or "just issued by..." isn't good enough. However, a convincing date doesn't prove that it's not a hoax.
- No best-by or expiry date on warning. Nonetheless, the presence of such a date doesn't prove that a warning is accurate.
- No identifiable organisation quoted as the source of the information. Nonetheless, association with an identifiable party doesn't prove that that party is, in fact, the source, and verifying the source does not, *per se*; validate the actual information as correct.
- The organisation quoted, as the information source, is one not normally associated with the dissemination of virus information (FCC); or an organisation whose expertise in security/anti-virus is questionable (AOL, Microsoft, CNN, ZDNet); or an organisation that doesn't exist at all. Note that there are hoaxes that claim to quote highly convincing information sources such as real anti-virus vendors and their representatives, CERT etc. These attributions are intended to add 'Credibility by association'. Claiming to quote the FCC is a particular give-away - the FCC is not in that particular line of business, and has stated that it never will issue virus alerts. Nevertheless, Good Times and some of its variants continue to claim to be quoting it. In fact, organisations, publications and individuals with less claim to relevant expertise have certainly issued or forwarded such warnings, sometimes to comic effect, all of which adds to the problem.
- The affected hardware, application, mail client etc. are not specified. Again, this is not conclusive: anti-virus vendor advisories often assume that the entire computing world uses PCs, and frequently that a particular version of Windows is universally employed. On the other hand, claims that a virus plays tricks with mail software/address books, but that don't specify the type of mail client affected, are a possible indicator that the information is unreliable, hoax or not. Similarly, claims that information such as passwords or credit card details will be leaked without specifying which passwords are targeted, or where the virus looks for credit card details, may indicate intent to frighten rather than inform.
- Immediate and devastating damage when the 'infected' email is opened. Hoax viruses rarely seem content with popping a rude message up onto the screen, preferring instead to render targeted systems unusable. In fact, if the viruses described in many hoaxes really existed, they wouldn't be viruses at all: they'd be Trojan horses with no reliable means of replication, since they'd burn themselves out on every system they landed on and trashed.
- No discrimination is made between opening the email, opening an attachment without executing embedded or attached code, and actually executing code: note, however, that it has never been entirely accurate to say that just reading mail is safe from any kind of malware [Harley, 1995-2001].
- It's claimed that no means of detection or recovery are known. This is a fairly dependable heuristic. In general, it's possible for an anti-virus vendor to supply detection for a newly discovered threat within hours, or less. There are exceptions, though. It took anti-virus vendors many months to implement detection and disinfection of macro viruses properly, and for a while the best help a vendor could offer was guidance on disabling auto-macros. It's not impossible that a completely new threat could arise which would require similarly extensive re-engineering, but it happens rather rarely. Nowadays, 'fast burner' virus/worm threats present almost the opposite problem [Harley, 1998]: patches and interim drivers for detection and disinfection of the threat is usually quickly implemented. However, the sheer volume of demand for the

fix and other malware-related drains on network resources may consume so much bandwidth that distribution mechanisms buckle under the strain [Harley, 2000; Wells, 2000]. In summer 2001, for instance, some organizations reliant on vendor web sites for updates and intranet web-sites for secondary distribution chose to block port 80, the port normally allocated to HTTP, as a measure for restricting immediate damage from (and re-distribution of) Code Red, and were thus obliged to make use of alternative mechanisms. Recovery is a more complex matter, and depends on the tools available to the victim, what backup strategy has been employed, and so forth. A virus warning which doesn't take these factors into account is automatically suspect.

- Virus described in terms of confusing pseudo-jargon such as the Good Times "Nth-complexity infinite binary loop", or with the use of inappropriate terminology such as "a Trojan virus". Unfortunately, most users of computers and the Internet do not have the technical expertise to distinguish between geekspeak (an inability to write in English rather than jargon) and technobabble (technical-sounding gibberish). Even the computer-literate may be confusing by the tendency among security experts pontificating outside their personal areas of expertise to invent jargon, misrepresentations of virus/anti-virus technology, and even examples of viruses mysteriously known to them, but not to the anti-virus establishment.
- Reads like a news item or press release, but there's no indication of its origin.
- Hoax alerts tend to be concerned with self-replication, not with pointers to further help or information. They rarely include verifiable sources of further information. Fake URLs are common though, as are URLs pointing to inappropriate/suspicious sites. It's easy to set up a web page without having to supply any sort of verification/authentication (free of charge, so credit card details aren't necessary), so a genuine web page can contain very unreliable information. An alert that claims to originate with Symantec, but includes a pointer to a site on geocities.com, suggests foul play. A geocities or angelfire site doesn't prove malice in itself, though: there are plenty of well-meaning amateurs and guru wannabes offering security information, some of it genuinely useful.
- Full details of the source of the information or a contact within the originating organisation for further clarification. There is unlikely to be a digital signature or any sort for authentication. However, the presence of a digital signature is not, in itself, proof of a bona fide alert. Many people don't bother or don't know how to check these.
- Surfeit of upper-case letters and exclamation marks is a danger sign. Real advisories are less likely to overstate the urgency of a virus problem than hoax alerts. Hopefully...
- Consistently poor spelling, grammar, syntax and presentation. Anti-virus companies rarely employ illiterates to write press releases or advisories.
- Claiming to originate with a known anti-virus vendor is another common indicator. It is not unknown for anti-virus companies to 'hype-up' a virus in press releases, or on their web sites, but they don't broadcast alerts to every mailing list on the Internet. Yet...
- Claims that superhackers have 'somehow' managed to write a program to do something that was previously thought to be impossible invite deep suspicion. (1) Anti-virus experts spend much time out of the public eye exchanging ideas about 'nightmare scenarios', and responsible individuals tend to keep such discussions away from the marketing department and journalists. Nonetheless, if it's possible, someone has probably hypothesised it. (2) Belief in the supernatural powers and intellects of hackerz and crackerz, virus writerz, and other 3l33t kewl d00dz is not common among anti-virus experts. Alerts that indicate such a belief are likely to originate with a member of one of

those groups, a journalist, or a security expert talking about a field outside his own competence.

Spoofs, parodies and humorous alerts such as the CDA meme virus, the Jeffrey Mogul metavirus, the Morris virus alert, and Bad Times, inspire considerable wry amusement in the informed observer. However, the joke seems to be on the jokers. It seems to be pretty difficult to create a spoof that someone, somewhere won't believe, and most compilers of hoax dictionaries have felt it necessary to include such spoofs. The sad fact is that many of the attributes given to hoax viruses seem to have been derived from earlier spoofs.

Spam Heuristics. Schwartz and Garfinkel (1998) identify two main approaches to filtering by sender address, mapping approximately to the firewall rule-set models of 'explicit deny' and 'explicit allow'.

- "Refuse villains, allow others" (All mail is allowed unless the sender is blacklisted). This approach is hard work, since professional spammers, their customers, and those who use bulk mailers, tend to make use of forged headers and/or disposable accounts. Thus it requires frequent updating and maintenance: a little like using a known-virus scanner but having to enter your own definitions updates.
- "Allow friends, refuse others." (All mail is discarded unless the sender is whitelisted.) This is less work, but discards all mail from unapproved sources, including approved senders using an unapproved mail account. This is only really viable if you're absolutely sure that you'll never want to hear from anyone you don't know.

There are many other heuristics recommended/used from time to time by spam-haters and anti-spam programs.

- Filtering by Subject (i.e. avoid characteristics such as undue capitalisation, multiple $$$ and !!!, give-away phrases such as Make Money Fast.) Unfortunately, spammers long ago learned to evade these heuristics and employ social engineering techniques to trick the recipient into opening the message, including varying the text to include (for instance) the recipient's name to make it appear more personal). Virus/worm writers have learned to use similar techniques to persuade victims to open attachments and to introduce a degree of primitive polymorphism to baffle such measures as procmail recipes for email filtering. Such measures are sometimes of use as a temporary expedient in the early stages of a fast-burner email worm attack, but tend to be discarded when definitions updates are available and distributed. As we've seen, however, this sort of detection works much better for viruses and related malware than for primarily textual material such as spam and hoaxes.
- Filtering by other suspicious or inconsistent header and routing/relay information.

Such filtering can be highly effective, and is often applied by enthusiastic anti-spam system administrators through home-brewed or freely exchanged procmail recipes and similar programmatic solutions. However, automated spam detection is a very dynamic field, comparable in some ways to the virus detection area, but even more fluid, and demanding constant maintenance in the absence of the equivalent of a commercial scanner. Even then, it involves a trade-off between effectiveness at eliminating the encroachment of unwanted material and acceptance of the likely loss of legitimate content.

Savvy system administrators tend to quarantine spam rather than discard it unread, so that they can monitor it and fine-tune their filters (Filtering software: Inaccuracies and mistakes, 2001).

Countering PsychoDoS in the Corporate Environment. There are, it seems, so many avenues of psychological attack, chipping away at corporate resources and confidence, and undermining our ability to use the resources on which we rely (hence the coining "PsychoDoS" - Denial of Service through Psychological manipulation) (Harley, 2000). If we can't rely on bought-in software and expertise to provide absolute protection even from such comparatively clearly defined threats as viruses, what resources are available to the hard-pressed security administrator?

One possibility is to outsource some (or all) of the problem. Can we refer responsibility out beyond the perimeter? ISPs are not necessarily devoted to the idea of taking this responsibility, preferring the approach of "we take no responsibility for the content we carry", reducing their own overheads to enable them to keep their prices competitive. Nonetheless, solution providers are starting to queue up to offer scanning 'out there', and some of them are offering other types of filtering too. Increasingly, we see spam and porn detection bundled with virus management filtering.

However, automated scanning for malware is arguably a little different from other types of content analysis. Very few people would want to stand by their God-given right to receive unannounced malware, though how to *process* infected mail is a more sensitive issue than some providers seem to realise. Technically, however, it entails a few problems. Perhaps the most difficult is maintaining a reasonable rate of throughput in a heavily used network, especially in times of heavy network load such as arises at the height of an attack by a network worm or a mass-mailer virus or worm. Even in less stressful times, though, the conflicting requirements of virus management and maintaining performance levels defined, in many cases, by a formal Service Level Agreement, can prove difficult to reconcile.

Defining and filtering other 'unacceptable' content (spam, scams, chain letters, hoaxes, pornographic, libellous, or politically sensitive material, copyright infractions) presents serious additional problems. Finding a suitable scan-string for a computer virus is comparatively simple, since binary code doesn't involve the ambiguities of human communication.

Other forms of content analysis can be difficult to automate and entails much more complicated legal and ethical issues. Some vendors have tended recently to move away from textual analysis into more complex areas such as the detection of pornographic material by searching for flesh tones and for other forms of image analysis. Opinions vary on whether this can be much more accurate than text analysis (Filtering software: inaccuracies and mistakes, 2001).

Some organisations cannot afford the luxury of trusting outsiders to manage these issues. Even those that do, however, must take decisions on the policies to be implemented on their behalf. Those that don't, have to make the same decisions regarding the technical solutions they choose to implement. Either way, sound research into the broad issues is mandatory, while implementation and ongoing maintenance and administration of filtering tools in-house calls for a significant investment of time, effort, and information gathering.

These, however, are primarily technological approaches, and therefore not in themselves sufficient response to a primarily social problem. Two interrelated approaches are, arguably, equally important: education and policy.

There are two main schools of thought on education: (1) it's crucial; (2) it doesn't work. The balanced approach is probably the best: use it, but don't rely on it. Training should begin with induction and be reinforced and updated regularly (and irregularly, if circumstances call for it). It should address (in a high-level sort of way) malware, hoaxes, chain letters, spam, ethical computing, any other relevant area of security (resistance to social engineering, password management, use of encryption) and above all, it should map closely to the policies in place within the organisation.

Every so often, someone reinvents the concept of hoax education through mass-mail 'pass-back'. Clearly, it makes sense for the recipient of a virus hoax to let the sender know they've been conned and ask them not to continue to forward it. This might be compared to letting a virus victim know that they are a source of infection, as distinct from advising them that they are at risk from any malicious payload. Where the recipient is aware of sound resources, it is a friendly and responsible act to make the sender aware that they can get further information. Within larger organisations, first and second line support teams/individuals may have guidelines to work from which may include a pro forma response. However, the recipient is often just one recipient among many, and it's tempting to mail the information to all recipients, in the hope of raising the level of consciousness generally. This was, perhaps, a more acceptable approach earlier in the game, when traffic (especially spam and other junk) was lighter.

Nowadays, far more people are already hoax-literate (in absolute numbers, though not necessarily relative to the total number of Internet users). This is, therefore, likely to create considerable annoyance on the part of already knowledgeable people who receive one original copy of the hoax, followed by a volley of assurances that it’s a hoax, followed by a spate of secondary mail of variable relevance and interest. (This vexatious sequence of events is most often seen in newsgroups and on mailing lists.)

A variation on this approach involves maintaining a database of mail addresses so that no one receives the same educational message twice. However, this falls short in several respects. The most obvious is that many people have multiple accounts on more than one ISP or local server. Even a single server account may be represented in several ways different enough to thwart any attempt to identify aliases. This may account for the fact that this particular wheel tends to be reinvented and abandoned regularly (one might say cyclically....) In general, it’s probably preferable to address the education issue on a less ambitious, more local scale, using training sessions and suitable electronic and other documentation to reinforce the application of organizational discipline and clear cut policy.

Policies

The above indicates that challenges are numerous and will continue to pose threats or just nuisances for users and system administrators. Nevertheless, some pro-active strategies and actions should be pursued to reduce the negative effects caused by social engineering.

The following suggested policy outlines are based on specimen policies from a recent book on viruses and virus management (Harley, Slade, Gattiker 2001). They won't work for everyone in all respects, but highlight and to some extent address most of the core issues (see also Tips, password, privacy, fraud, spam, viruses, and more, 2001).

Acceptable Use of Facilities

One strategy is to identify clearly how Email and access to the World Wide Web can be used at work. Organizations can specify that the use of email, web, and other network or internetworking resources owned by the employer be intended for work purposes only. Use for purposes not strictly work-related may be acceptable in moderation. For instance, email use may be acceptable but subject to management approval in some organisations, as long as it does not interfere with work.

All use of company facilities is required to be in accordance with all binding laws including but not restricted to:

- Data Protection Legislation
- Copyright Legislation
- Legislation concerned with information and systems security
- Trade Secrets Legislation
- Anti-discrimination Legislation
- Obscenity/Pornography Legislation
- All internal policies
- Other policies and agreements by which the company is bound

It might be considered appropriate to proscribe here the use of company resources for administration of private business ventures. But as a French case has illustrated, a employee’s privacy may prevent a firm from checking email content at work due to suspicion of moonlighting (A Workplace email privacy: French supreme court rules, 2001).

Acceptable Use of Email

Email users should be made aware that while they're using a company account, what they write may be seen to represent the views and policies of the company. They should therefore be required to conform to appropriate standards of accuracy, courtesy, decency and ethical behaviour, and to refrain from the dissemination of inappropriate mail content. Inappropriate behaviour may make not only the employee but also the company open to accusations of libel/defamation, harassment/discrimination, copyright infringement, invasion of privacy and so on (Overly, 1999). Employees may be explicitly required to act in accordance with the company's published policies as well as all applicable legislation and other binding agreements.

Most companies are not inclined, able, or obliged to maintain constant surveillance of employees' use of its facilities, especially where such use is not specifically authorised. However, users of these facilities should not be encouraged to believe that they have an automatic right to privacy. Even if there is a legal justification to such an expectation, mail may be monitored or checked from time to time for reasons of maintaining network support, security or other reasons, as well as for ensuring that it meets prescribed standards.

Email should not be used as if it were a secure communications channel for the transmission of sensitive information or messages. Use of encryption, though, should be in accordance with the company's policy.

Anti-Chain Mail Policy

Chain email is a drain on network resources, system resources, and support staff. Any mail that includes a request to forward widely and inappropriately should be regarded with suspicion.

On no account should mail that warns of viruses, Trojan horses and other security threats be forwarded without checking and authorisation from IT/IS, however trustworthy you consider the source to be.

Some virus hoaxes may have been intended to discourage the forwarding of previously existing chain letters. This is not an acceptable reason for passing on a hoax or chain letter.

Passing on warnings about hoax warnings can be a difficult area. Some individuals and groups have recommended passing on information about hoaxes and chain letters back to other recipients of a hoax or chain letter, and in some extreme instances, to everyone in the recipient's address book.

- Passing on an anti-hoax message to everyone in the end-user's address book, department, or organization with instructions to do the same is simply a chain letter, and not acceptable.
- Passing back an anti-hoax message to other hoax recipients may be justifiable if there are only a few of them and you're reasonably sure they'll benefit from the information. Even then, it is only appropriate to pass it back if it's certain that the information is accurate, and with the approval of the IT department manager or security manager.
- Not all hoaxes are security-related. Do not pass on, for instance, appeals to forward mail to raise money for a worthy cause. Even if it isn't a hoax, it may not be considered an appropriate use of company resources.

Anti-Spam Policy

Employees are often explicitly forbidden to use company resources for the dissemination of spam, junk mail and other forms of inappropriate mass email for private or work-related purposes. Mailing lists specifically set up for dissemination of particular types of work-related information may be exempted from this stricture, as long as the type of information broadcast is appropriate. However, spamming a mailing list is unlikely ever to be considered appropriate.

It is recommended that employees are instructed to react appropriately to spam by reporting and forwarding it to IT support staff, and following their advice on what further action to take, if any. Direct response to spam (including angry replies or following instructions to unsubscribe) can cause more damage than ignoring or simply deleting offending messages. (Damage in this context includes lack of co-operation on the part of administrators who might otherwise be helpful; increased volume of spam, the spammer having ascertained that he has a 'live one'; mail-bombing, revenge spams etc. by a malevolent spammer.)

'Spoofing' or forging mail headers in the headers of email or news-postings may be explicitly forbidden as a means of disguising the source of mass email (there is no legitimate business reason for doing this). It may also be forbidden as a means of making it more difficult for spammers to add an address to their list of targets. The latter may be a legitimate aim, but spoofing is likely to ease the spoofer's burden of junk mail at the expense of other legitimate users.

Acceptable Use of World Wide Web and UseNet

Access is normally permitted as far as is necessary to achieve work-related goals, obviously. Access to sites or newsgroups that aren't directly work-related may be permitted, subject to management approval, as long as this doesn't interfere with work. Access is often specifically forbidden to such resources that customarily carry pornographic material, pirated software and other illegitimate information and resources, such as malicious software (binaries or source code) including viruses, Trojan Horses, Backdoor/Remote Access Tools, password cracking tools, and hacking tools. Measures intended to discourage use of and access to pornographic resources may be particularly difficult to enforce justly unless care is taken to take into account:

- Solicited and unsolicited receipt of pornographic material
- Maliciously targeted, as opposed to untargeted porn spam directed to harvested accounts without reference to the wishes of the target
- Obscene or otherwise unacceptable material forwarded with forged headers, so that an innocent individual (often one of the unwilling recipients) may be implicated in the distribution.
- Mail crafted to take advantage of vulnerabilities or configurations of browser that allow an unacceptable web site to be accessed without the intervention of the end-user. Unacceptable here might be pornographic, or might involve the transfer of malicious software.

Anti-Virus Policy

More often than not, possibly virus-related problems are to be reported to the call centre and logged to the appropriately qualified person or team. Helpdesk and 2nd line support staff attempting to handle such incidents should be expected to advise qualified personnel at the earliest possible point in the incident management process, if they themselves are not qualified. The problem here is that all too many support specialists have an exaggerated opinion of their own expertise.

It's common and very justifiable to forbid the sharing of games, joke programs, and screensavers etc. Any attachment is potentially hostile, irrespective of what it's claimed to be or the trustworthiness of the source. Viruses and worms are characteristically distributed furthest, unwittingly, by innocent third parties, and often masquerade as such frivolities. There are, however, other arguments for such vetoes: their exchange is often associated with other support issues such as compatibility and licence management.

Customers are usually expected to use the corporate standard anti-virus package. Systems running unsupported packages should be regarded as unprotected: this may have general support implications, as well as the obvious security implications. It's appropriate to forbid end-users to disable or reduce the functionality of security software without authorisation.

Unqualified staff (probably including most support personnel) may not pass on warnings of viruses, Trojan Horses and other security breaches without authorisation.

Conclusions and Implications

We have attempted to clarify the problems and outline some possible part-solutions for organizations, users, and system administrators. Various tools such as filtering can be highly effective but unless savvy system administrator continuously fine-tune filters, their effectiveness may be greatly reduced.

Clearly, the problem of mail abuse goes far beyond viruses and hoaxes. However, it is by no means universally agreed that existing management tools can effectively automate the ingress and egress filtering of such abuse. Technical solutions cannot realistically be implemented irrespective of corporate educational strategies and policies, and automation is not a substitute for good quality, honestly intended and properly authenticated information.

Biologists have long been fascinated not only by the mechanisms of sexual reproduction, but the apparent paradox that they don't appear to be particularly efficient (Ridley 1993). One possible answer to the paradox is that sexual reproduction, by disseminating genetic variation, increases resistance to infection. (Sometimes this is referred to as the Red Queen Hypothesis - the process runs like crazy just to stay in the same place, just ahead of the adaptive capabilities of disease organisms.) Perhaps we need to come to terms with the fact that (1) malicious software also adapts to changing environments; (2) that metamalware and related nuisances keep pace with social and technological trends; and (3) that technological solutions aren't sufficient to keep up with social problems and dynamics.

As Table 1 suggests, ULs, hoaxes and spam as well as chain letters require that users become more careful about passing on email messages, newsletters, e-greeting cards and much more. Hence, some educational efforts for, and cautionary behavior by, users can make a difference (When the do’s and Dont’s, 2001). In addition policies that are known by employees and strictly adhered to by the organization should further help in minimising negative outcomes (e.g., sample policies see also Documents- privacy, security and e-mail, 2001)

One of the issues that also must be addressed is how a firm doing business in various countries can best deal with these issues. Even across the EU, privacy legislation is interpreted somewhat differently across countries, whereby in extreme instances, filtering email and checking its content due to spam suspicion may result in lawsuits that could be lost (e.g., Workplace email privacy: French supreme court rules, 2001). Here a more unified interpretation of privacy and data protection rules by European courts would be helpful.

In summary, hoaxes, urban legends, and computer viruses as well as malware are the many facets of an every larger drain on vendor and corporate service desks. Hoaxes continue to proliferate. Unless users begin to behave appropriately and social engineering efforts are less likely to result in behaviours that drain system resources, the problem will mushroom. The issues addressed in this study may provide directions for more work in this area and the ability to reduce the threat from hoaxes, urban legends, spoofs, and chain letters to users and their IT resources.

References

Blackmore, S. (1999). The Meme Machine. Oxford: Oxford University Press.

Dawkins R. (1976/1989). The Selfish Gene. Oxford: Oxford University Press.

Dawkins R. (1993) Viruses of the Mind. In B. Dahlbohm (Ed.), Dennett and his Critics: Demystifying Mind (pp. 13-27). Oxford: Blackwell.

Dawkins R. (1995). River Out of Eden. London: Weidenfeld & Nicolson.

Dawkins R. (1998). Unweaving the Rainbow. London: Penguin.

Dennett D.C. (1991). Consciousness Explained. Boston: Little, Brown.

Dennett D.C. (1995). Darwin's Dangerous Idea. New York: Simon & Schuster.

Documents – privacy, security and e-mail codes for organizations. Available: http://security.weburb.net/frame/docs/docs.html Last access, 2002, Feb. 27

Filtering software: Inaccuracies and mistakes (2001). Information Security This Week, 2, (58) [On-line]. Available: http://security.weburb.net/show/news/2079. Last access: 2002, February 21.

Fraser B. (1997) RFC 2196 "Site Security Handbook" Network Working Group [On-line]. Available: http://www.ietf.org/rfc/rfc2196.txt. Last access 2002, February 25.

Full disclosure and security. (February, 2002). Information Security This Week, 3, (6) [On-line]. Available: http://security.weburb.net/frame/show/news/2400 Last access, 2002, Feb. 27

Gattiker, U. E. (2001). Internet challenges: Cultural, organizational and political issues. Mahwah, NJ: Lawrence Erlbaum.

Gattiker, U. E., & Kelley, H. (1994). Techno-crime and terror against tomorrow's organisation: What about cyberpunks. E. Raubold and K. Brunnstein (Eds)., Proceedings of the 13 World Computer Congress -- IFIP Congress '94, Hamburg (pp. 233-240). Amsterdam: Elsevier Science Publishers.

Gattiker, U. E., Pedersen, P. Ø, , & Perlusz, S. (2002). Privacy and Alerts: Does Giving up Privacy Make Sense? In U. E. Gattiker (Ed.), EICAR Best Paper Proceedings (pp. 157-198). Copenhagen: EICAR (ISBN 87-987271-1-7).

Gordon, S., Ford, R. *When Worlds Collide: Information Sharing for the Security and Anti-Virus Communities* (Virus Bulletin Conference, 1999)

Sarah Gordon, Richard Ford, Joe Wells: *Hoaxes and Hypes* (Virus Bulletin Conference, 1997)

Harley D. (1977) *Dealing with Internet Hoaxes/Alerts* (EICAR News Vol. 3, 2)

Harley D. (2002, February 21)*:* Email Abuse: Internet Chain Letters, Hoaxes, and Spam [On-line]. SherpaSoft. Available: http://www.sherpasoft.org.uk/hoaxfaq/Mis-IT.html. Last access: 2002, February 21.

Harley D. et al. (2002, February 21): alt.comp.virus FAQ [On-line]. SherpaSoft. Available: http://www.sherpasoft.org.uk/acvFAQ/. Last access: 2002, February 21.

Harley D. (2000): De-mythologising anti-virus. Virus Bulletin, April 2000.
Harley D. (1998): Re-floating the Titanic: Dealing with Social Engineering Attacks. EICAR Conference Proceedings.

Harley D. (1999). Nine Tenths of the Iceberg. Virus Bulletin, October 1999.

Harley D. (2000). The Email of the Species [On-line]. SherpaSoft. Available: http://www.sherpasoft.org.uk/hoaxfaq/. Last access: 2002, February 21.

Harley, D., Slade, R., & Gattiker, U. E. (2001). Viruses Revealed. New York: Osborne/McGraw-Hill.

Jones L.: Good Times FAQ [On-line]. http://www.usit.net/public/lesjones/goodtimes.html. Last access 2002, February 21.

Oxford Reference Dictionary (1986). Oxford: Oxford University Press

Overly, M.R. (1999). E-Policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets. New York: Amacom.

Overton, Martin (2001) [Online]. http://arachnophiliac.com/files/av/VB2001_Electronic_Ephemera-1.01.pdf. Last access 2002, March 21.

Pedersen, P. Ø, Gattiker, U. E., & Perlusz, S. (2001). How Much Privacy Are We Willing to Give up for Free on-Line Media Services? In C. F. Altobelli (Ed.), Print contra Online? Verlage im Internet-Zeitalter (Print contra online? Publishers during the Internet era) (pp. 157-198). Munich: Reinhard Fischer.

Ridley, M. (1993): *Is sex good for anything?* (New Scientist 140;1902)

Schmauder, P. (2000).Virus Proof: The Ultimate Guide to Protecting Your PC.Prima Tech

Schwartz, A. & Garfinkel S. (1998). Stopping Spam. Sebastopol CA: O'Reilly & Associates Inc.

Spamming (2001). Available: http://security.weburb.net/frame/faqs/spam.html Last access, 2002, Feb. 27

Tips. Password, privacy, fraud, spam, viruses, and more. (2001). Available: http://security.weburb.net/tips/tips.html Last access, 2002, Feb. 27

Joe Wells: *Denial of (Anti-Virus) Service* (Virus Bulletin, June 2000)

What have Sircam, Hookers and Symantec in Common? (September, 2001). Information Security This Week, 2, (52) [On-line]. Available: http://security.weburb.net/show/news/1758 Last access, 2002, Jan 3

When the Do's and Dont's of Safer Computing and Sex: The Ropes to Skip. (November 21, 2001). WebUrb News Column, 2(8). Available: http://news.weburb.net/frame/columns/ISSN16009665V2N8.html
Last access, 2002, Feb. 27.

Workplace email privacy: French supreme court rules...causing many future headaches for firms. (2001). Information Security This Week, 2(58) [on-line] Available: http://security.weburb.net/show/news/2005. Last access, 2002, Jan. 9

APPENDIX: INFORMATION RESOURCES

http://www.Vmyths.com/ [Rob Rosenberger's site: specific hoaxes, constantly updated news, personal opinion, myths and urban legends, links. An essential resource.]
http://www.Vmyths.com/fas/fas1.cfm [Rosenberger's very useful article on 'false authority syndrome'.]

Urban Legends:
http://urbanlegends.about.com/
http://www.urbanlegends.com
http://www.snopes.com/ [Urban legends reference pages]

Hoaxes, Chain letters:
http://www.korova.com/ [wide-ranging, but includes hoax info/hoax du jour]
http://ciac.llnl.gov/ciac/ [wide-ranging security resource with pages on hoaxes and chain letters.
http://www.virusbtn.com/ [Virus Bulletin: obviously oriented towards real viruses, but includes a hoax resource]
http://www.trusecure.com/html/tspub/hypeorhot [wide range of security info and resources including hoaxes and this alert assessment service]

http://arachnophiliac.com/ [Electronic ephemera FAQ and reference site by Martin Overton.]
http://Security.WebUrb.net/newsboard [constant updates on viruses, hoaxes and other security threats including an emailed weekly newsletter for subscribers in collaboration with EICAR]

Anti-virus vendors with hoax info:
http://www.f-secure.com/
http//www.stiller.com/
http://www.sophos.com
http://www.symantec.com/
http://www.nai.com/

Vendors with content analysis/filtering solutions:
http://www.integralis.com
http://www.antivirus.com
http://www.checkpoint.com
http://www.cai.com
http://www.nai.com
http://www.Enologic.com

Spamfighting

http://www.cauce.org [information resource - legislation, FAQs, links]
http://www.euro.cauce.org/ [European equivalent]

http://www.claws-and-paws.com/spam-l/ [SPAM-L FAQ and mailing list; links to further resources]
http://www.spamcop.net/ [spam report/action service]
http://combat.uxn.com/ [spamfighter tools/resources]
http://www.samspade.org/ [email abuse resources]

Many anti-virus vendors have mailing lists for news of current threats and definitions updates, though some are rather hype-enhanced. Some sometimes touch on current hoaxes, hype alerts etc. Organisations such as CERT, SANS etc. maintain mailing lists that may include virus/worm-related (and even less often, hoax-related): however, the quality of information therein is variable and rarely updated as situations change (new information, variants, vendor updates etc.). Bugtraq and NTBugtraq include virus/worm related advisories and exploits, and sometimes lengthy discussion: however, the quality of information here, too, can vary widely.