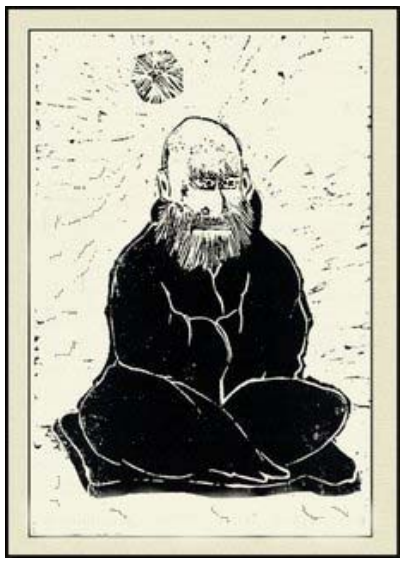
A Matter of Trust

A Special Report on Trustworthy Computing



Zentelligence (Research) Ltd

Introduction & Executive Summary

This report represents an assessment of Trustworthy Computing (TWC); Microsoft's personal vision of security and a broader exploration of the present threat directed towards business and the national critical infrastructure from the Internet.

This is not a technical document. It presents a top-level impression of the current information security situation and offers an independent assessment of the impact and direction of Microsoft's Trustworthy Computing initiative.

The last twelve months have witnessed a worrying escalation in the number of vulnerabilities, which can lead to Internet-based attacks on organizations and the compromise of their information infrastructure[1]. 2002 was also the year that saw the launch of Microsoft's TWC initiative, a significant re-purposing of the company's strategy, which now places security as the principal priority in all its products, changing it from an optional setting to a default, in order to meet the twin challenges of information risk and Internet crime.

Recent incidents, such as SQL-Slammer[2] in January and a critical Win2K/IIS (vulnerability [3] in March of this year, have exposed potential vulnerabilities in Microsoft's products, the difficulty in deploying them securely, and the challenges of keeping them secure as threats evolve over time [4]. While the company offers an ambitious vision of a more secure future through the next generation of Microsoft products, in order to achieve a higher degree of market confidence in TWC, the company has to find ways of tackling many thousands of published and un-published vulnerabilities. These can potentially 'compromise' millions of un-patched legacy products running under licensed and un-licensed versions of Windows-95, Windows-98 and Windows NT across the globe.

The Devil in the Detail

Are Microsoft products more vulnerable than the alternatives and in particular, those available from the Open Source community?

---

[1] More than one million UK businesses are vulnerable to hacker attacks according to a study by Microsoft, 65 % of small and medium-sized businesses in the UK have no form of intrusion detection system, while more than 15% do not even a basic firewall.

[2] Estimated SQL-Slammer incurred damage estimated at between $950 million and $1.2 billion in lost productivity in the first five days worldwide.

[3] MS-03-007 WebDAV – IIS/Windows 2000

[4] Forrester Research notes that while Microsoft's patches for the last nine high-profile Windows security holes predated such attacks by an average of 305 days, too few customers applied the fixes because "administrators lacked both the confidence that a patch won't bring down a production system and the tools and time to validate Microsoft's avalanche of patches."

Independent research now suggests that the accusation of generic weakness in Microsoft's products, when contrasted with Linux, is statistically exaggerated. Microsoft's market share makes it the proportionally the biggest victim but the argument used against the company, is equivalent to insisting that Fords are statistically less safe than Ferraris, because more of the former which makes more models, are involved in more accidents.

The results of the most recent Symantec Internet Threat Report, illustrates how Internet threats have intensified and evolved in many ways, while remaining relatively stable along other criteria. Although the number of overall attacks decreased last year the overall number of vulnerabilities rose alarmingly. Symantec documented 2,524 new vulnerabilities in 2002, up 81.5% from the previous year.

Symantec's analysis is supported by Internet Security Systems (ISS X-Force[5]), who have reported that the number of computer security incidents and attacks detected at businesses worldwide [6] has soared by 84% between the fourth quarter of 2002 and the first quarter of 2003, fuelled by a surge in the number of mass-mailing worms, according to ISS[7]. Of all the events reported by businesses in the quarter, the top categories were "suspicious activities", which includes scanning networks for vulnerabilities and accounted for 73.5% of total events, and unauthorised access attempts, which accounted for 11%.

Both Microsoft and experts in the Open Source community would agree there is only so much an organisation can do to secure its software environment. Properly configured, patched and updated there is little to choose between them. The critical factors are represented by the speed of response on the part of Microsoft or the Open Source community to an 'outbreak', on the scale of SQL-Slammer and the commitment of the customer organization to a sound security policy as found in the international information security standard, ISO/BS7799.

To Educate and Protect

Microsoft's greatest challenge lies in convincing the world that TWC can work in practice rather than in principle. Its commercial rivals might argue that the Windows architecture has taken the world down a blind alley, which is intrinsically insecure and incompatible with the demands of Internet security. Microsoft supported by the evidence, now has to prove otherwise by delivering tangible results through the evolution of TWC and by providing better education, information and reliable patches and support to its existing customers. Trust is however a two-way relationship and without customers adopting a consistent and sensible approach to information security, there is only so much protection that Microsoft or any other software company can offer. A vendor can create the software equivalent of Fort Knox with all the doors and windows locked 'out-of-the-box' but beyond this point, the burden of responsibility moves towards the customer to ensure that the level of security in place, matches the needs and size of the organization involved.

---

[5] XForce's Internet Risk Impact Summary (IRIS) report draws information from more than 400 network and server-based intrusion detection sensors located at businesses on four continents and spanning all major industries.

[6] The report tracked 20 industry sectors over the quarter and found that retail businesses were attacked the most, accounting for 35% of attacks, financial services accounted for 11.5%, healthcare and manufacturing 9% each, and federal and local government accounted for 1%

[7] Computer Weekly – CW360.Com - 7th March 2003

In the National Interest

The monthly report to the Prime Minister from the e-Minister, Patricia Hewitt and the e-Envoy, Andrew Pinder, offers a metric of national progress against the commitments announced in the Government's UK Online strategy. In a departure from the traditional format, which clearly illustrates concern on matters related to information security the March report to Tony Blair provides a brief summary of government activity since October, focusing solely on issues surrounding electronic security. Initiatives addressed in the report included the new online information security guide for small businesses and the Warning Advice and Reporting Point scheme established by London's eGovernment agency, London Connects.

The Prime Minister would have had good reason for a personal interest in electronic security, as on the 23rd March the 10 Downing Street website[8] was briefly rendered inaccessible following a coordinated denial of service attack protesting Mr Blair's role in the war with Iraq.

Over the last six months, I have been examining the question of information security and the Internet in the public and private sectors. I've collected the opinions of civil servants, MPs', MEPs' the Police, and leading experts from the different interests that divide opinion in the IT industry: Microsoft, IBM, Red Hat, Symantec and many more. When I mention my interest in the security of the public sector I find reactions can be very different. With government as an important customer, the IT vendors are happy to discuss their own vision of the future for information security but in contrast, some parts of government have been reluctant, reflecting the broad concerns, which led to the matter being included in the report to the Prime Minister.

If November of last year was notable for the eSummit, a well-orchestrated celebration of the Prime Minister's 2005 vision of joined-up government and 'Broadband Britain', then December offered a less well-publicised but equally significant gathering in a quiet London hotel. This was the UK's first ever eCrime congress sponsored by the National Hi-tech Crime Unit (NHTCU) which attracted an audience of high-ranking delegates from law-enforcement agencies and governments around the globe, who gathered to listen to a keynote speech from Home Office Minister Bob Ainsworth MP.

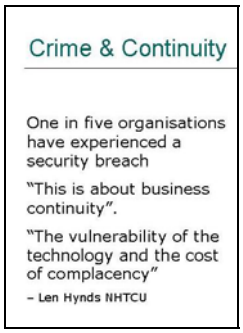
The irony of the two events taking place within weeks of each other did not pass unnoticed. On the one hand, we are presented with an agenda of national importance, one that involves a radical transformation of the public sector and with it, Britain's emerging role as an example to other countries. In contrast, there were the conclusions from the eCrime Congress, that the Internet and its foundation

[8] The No10 site reportedly runs on Microsoft's Internet Information Server on Windows 2000

technologies are open to organised criminal abuse [9] on a scale, which remains to be grasped. At the conference, I presented several of the challenges associated with the collection of accurate statistics but Internet crime defies jurisdictional geography and like the drugs trade, it leverages the criminal code weaknesses of the poorer states. As a Ukrainian police officer commented:

"I have ten men, three large cities and very little budget in a country with many other urgent priorities"

Today, we talk in terms of the Internet and its growing importance as part the 'National Critical Infrastructure' [10]but we might as easily think in terms of Swiss cheese when presented with relatively simple matters of information security at the organisational level.



To illustrate this view, there was yet another embarrassing 'leak' before Christmas of a confidential Foreign and Commonwealth Office document to the US-based web site Cryptome.Org. The Sunday Times, which now makes a point of watching Cryptome for salacious gossip, picked-up a confidential memo which described the visit of Russia's Defence Minister, Sergei Ivanov to London and what was discussed between our governments over dinner. There was the normal polite discussion on Iran and Chechnya and weapons of mass destruction but according to the memo:

"Chernov, one of Ivanov's staff at the PUS' dinner launched a diatribe about the threat which the internet and an 'uncontrolled information space' posed to world security. He depicted the Internet as the major global threat over the next 5-10 years."

The Statistics of Crime

Statistics are a problem for any of us attempting to grasp the scale of the growing information security challenge to our society. In December 2002, in an open letter to Members of Parliament, I noted that October 25th 2002 set a new record for attacks on computers on a global basis[11]. At the eCrime congress, Len Hynds, the Director of the National Hi-Tech Crime Unit, reported that over 80 % of UK companies have now been attacked or aggressively scanned for weakness from the Internet; PricewaterhouseCoopers reporting that one in five organisations have experienced a security breach.

---

[9] The US Federal Bureau of Investigation has referred 48,252 fraud complaints to federal, state and local law enforcement agencies in 2002 triple the 16,775 referrals it made in 2001. According to the 2002 Internet Fraud Report, victims of internet fraud lost $54m in 2002, up from the $17m they lost in 2001.

10 If thirty motivated people with hacker skills and $10 million were to attack us today, they could bring this country to its knees". Mike McConnell – Former Director of the United States National Security Agency.

11 In 2002, Symantec documented nearly 50 new vulnerabilities each week, a rate that was more than 80% higher than the rate recorded during the prior year.

eGov monitor

Simon Moores

This article appears in eGov monitor Weekly, the most informative round-up of electronic government and public sector ICT. To receive this publication apply here.

9 December 2002

The Mandate of Heaven

By Dr Simon Moores

"Parliament", said my distinguished friend "has always leaked like a sieve".

I'm researching the thorny issue of 'Confidence in Public Sector Computing' and we were discussing the dangers presented by the Internet. In his opinion, information security is an oxymoron, which has no place being discussed in a Parliament built upon the uninterrupted flow of information of every kind, from the politically sensitive to the most salacious and mundane.

With the threat of war hanging over us, I asked if MPs should be more aware of the risks that surround this new communications medium? More importantly, shouldn't the same policies and precautions that any business might use to protect itself and its staff, be available to MPs?

Also in December, winner of the New Statesman media award, eGov monitor, reported that government departments have experienced more than 9,000 digital attacks on their IT systems so far this year. Over half of the attacks on UK government systems this year, were reportedly directed towards the Cabinet Office and its agencies, which during 2002 suffered some 5,857 attacks, with 1,167 of these occurring in October alone.

Ministers revealed the security threat to government in responses to a series of parliamentary questions tabled by Labour backbencher Brian White MP and Liberal Democrat MP, Richard Allan, stressed the importance of improving information security in a 'Today' programme interview on Radio 4.

One large metropolitan council interviewed averages 26,000 emails each day and in a single month, last year, experienced 988 separate virus attacks from 26 separate viruses. Significant cost and effort goes into content filtering and the council's head of IT receives between ten and twelve discovery requests each month for the purpose of internal investigations involving email and its content.

The Vocabulary of Risk

Symantec's latest Internet Threat Report, amalgamating both Symantec Managed Services and Security Focus data for the last six months of 2002, reveals how Internet threats have intensified and evolved in many ways, while remaining relatively stable along other criteria. Although the number of overall attacks decreased last year the overall number of vulnerabilities rose alarmingly. Symantec documented 2,524 new vulnerabilities in 2002, a gain of 81.5 % from the previous year, which, as we have read was bad enough in its own right.

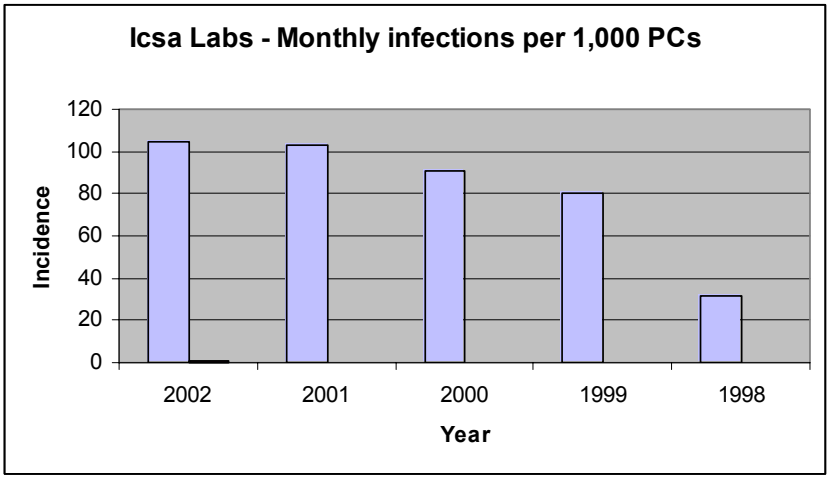
Symantec argues that despite this decline in overall attacks against business, many organizations, such as those in the financial services sector, experienced a sharp rise in attack volume and relative attack severity, while other companies, such as tenured security monitoring clients, substantially reduced their risk profile. Attack volume by country of origin was mostly consistent with past studies. 80% of attacks were launched from systems located in only 10 countries, and the United States was by far the largest source of attacks.

Approximately 60% of the documented vulnerabilities were easily exploitable either because sophisticated tools were widely available for use by the 'wannabe hacker' community' or because exploit tools were not required at all. As you might expect from this news and by leveraging the vast supply of vulnerabilities, the more malicious of these virus authors introduced several successful blended-threats over the past six months.

A British Computer Society study reveals that Most IT departments are unprepared [12] to deal with viruses and 'cyberterror' attacks and reveals a lack of security policies. Attacks from within continue to be seen as the principal threat to IT security: internal fraud and abuse are rated as a high or medium threat by 72% of IT managers.

In line with the increase in risk, companies are taking more time to recover from virus attacks, according to a new report, and costs are rising. However, they are now more likely to suffer from a string of small attacks throughout the year, rather than from a single major attack.

IT Week reports [13] that a survey by Icsa Labs of organisations with more than five hundred PCs, found they took an average of twenty-three person days to recover from each virus disaster in 2002, up from twenty days in 2001. Icsa Labs [14], defined a disaster as a simultaneous attack on twenty-five or more PCs, or an attack causing major damage.



The average cost of recovery from each disaster increased from £45,000 in 2001 to £52,000 last year. About three-quarters of organisations said the virus problem was worse in 2002 than in 2001. The monthly infection rate among 306 medium to large firms increased to 105 per 1,000 PCs, up from 103 in 2001, and 91 in 2000.

Four viruses in nine months caused the eighty disasters reported in 2002. This differed from previous years, when most disasters were reported in a single month and were caused by a single virus - for example Melissa in 1999 and Loveletter in 2000.

---

[12] Less than 50% of IT departments have formal procedures for dealing with threats such as a bomb or a fire, and only 33% have a plan if a virus beats their anti-virus software, according to the study by the BCS and Henley Management College. Even though 91% of senior IT managers questioned have security policies in place to avoid or reduce threats, only a minority have contingency plans if policies are breached. – CW360.com [7-4- 2003]

[13] Madeline Bennett, IT Week [31-03-2003]

[14] Icsa Labs, a division of security specialist TruSecure

Email attachments were the most frequent source of attacks, and infected 86% of firms. Internet downloads and Web browsing were responsible for 11% and 4% of infections respectively.

The main problems caused by viruses were loss of productivity and unavailability of machines. Lost data and corrupted files were also key concerns. Icsa Labs advised companies to keep using desktop antivirus solutions in conjunction with email gateway or SMTP server protection, file attachment filtering and Web browsing defences.

Chasing the Dragon

Statistics frequently need to be taken '*With a pinch of salt*', in the absence of a single, authoritative and integrated source of information capable of presenting an impartial and evidential view of the growing security problem now facing both the private and the public sectors. The eCrime congress called for better and more centralised reporting to assist the NHTCU which sees its efforts "undermined by under-reporting" which impacts on the accuracy of its threat assessment task. But reporting, though useful, like any crime figures, only offers a picture of what has happened while most organisations are calling for better predictive information in the fight against Internet crime.

In the words of Microsoft's Chief Security Strategist, Scott Charney [15], speaking at the eCrime congress in December, "*More than half of all computers operate in an unmanaged environment*". While it's hard to arrive at accurate figures, a significant percentage of systems are protected by either limited security or are accessible through default passwords, such as "Administrator". The British hacker, Gary McKinnon, 'Solo' caught by 'Operation Sidewalk' last year, caused at least $1.3 million worth of damage among United States government systems through the relatively simple exercise of installing a remote access 'PC Anywhere-type' program on inadequately protected servers.

Since the tragedy of 9.11, the US government is far more attentive than most to issues of information security and yet McKinnon allegedly compromised over ninety sensitive systems from his flat in North London.

Increasingly, the Bush administration also worries that Islamic extremists may be among the owners of U.S. companies involved in sophisticated computer activity. In Dallas, at the end of December 2002, a posse of FBI agents arrested the operators of Infocom, an Internet service firm allegedly financed by a leader of the militant [16] Palestinian group Hamas [17].

[15] See Scott Charney on the threat of cyber terrorism

[16] See Giles Trendle on Palestinian cyber-militancy – The Colonel's Network Warfare

[17] See Simon Moores on middle-eastern cyber-terrorism www.zentelligence.com or www.arabgov.com

In February, CW360 reported that the NISCC (The National Infrastructure Security Co-ordination Centre) had raised the prospect of cyber-attack by Islamic militants, as a possible consequence of war with Iraq. Symantec most recently pointed at Iran and Kuwait as the most frequent source of cyber-attacks from Tier-2 countries,[18] over the last six months of 2002. However, the NISCC appears to be more concerned about is the threat from 'The enemy within', a 'fifth column' of cyber-militants, described as 'terrorist-groups "who may actively seek to plant people inside IT departments of critical organisations".

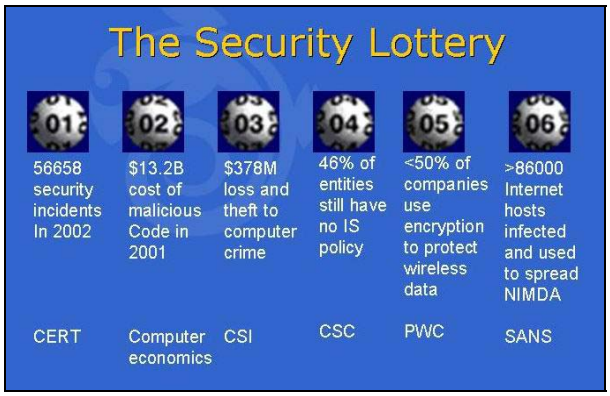
Following the invasion of Iraq, the Arab online publication, Zawya.Com, picking-up on a press release from the Mi2G Intelligence Unit in London, reported a significant increase in the number of attacks on online systems in March. According to Mi2G, The main operating system targeted is Linux. It comments that "One of the main pro-Islamic anti-war attacker groups-Unix Security Guards-is a macro-hacking group with members from Morocco, Egypt, Eastern Europe and Gulf countries. As a result, the number of attacks against Linux online systems has crossed Microsoft Windows in March. Some 71 % of all digital attacks recorded in March are against Linux systems and only 24 % are against Microsoft Windows".

In the current international circumstances, the public sector is feeling more vulnerable to the prospect of information risk than ever before and the possible existence of a fifth column may been entertained but is rarely expressed, due to the political sensitivities involved in profiling.

[18] Tier One countries are more than one million users – Tier Two countries are less than one million users

An Elusive Technology

In its 'Technology Trends for 2003', Red Herring Magazine concludes that software-based information security has been and will continue to disappoint. It states that "If software, the traditional approach to providing security, had been working, then businesses wouldn't have lost an estimated $1.7 billion to security breaches since the September 11 terrorist attacks. Software , by its very nature, is soft, it's easy to change, damage, or destroy. Chips, on the other hand, are made from hard silicon; a tougher nut to crack".



The magazine points out that "Intel plans to include security features in its next generation of microprocessors. The company hopes these chips will ensure that computers are secure the moment they are turned on, thwarting a common hacker's trick".

What Red Herring is referring to, is a well-developed plan from the TCPA (The Trusted Computing Platform Alliance) for the incorporation of security features into existing and future processor chips because "software performing sophisticated encryption eats up precious computer cycles on devices like PDAs and laptops." The idea is an enhanced hardware and Operating System-based 'Trusted Computing' platform that implements trust into client, server, networking and communications platforms and by "hardwiring the process onto chips, encryption speeds can increase anywhere from 10 to 10,000 times".

This new expression, a new 'Trusted Computing Platform', suggests, that any predecessor was, if not untrustworthy, then rather less than perfect in matters involving security. This problem brings us to where we are today, at the beginning of 2003, looking back at a disastrous record of security incidents and exploits and wondering how long it will be before any new approach to the challenge 'Trusted Computing' can inspire real confidence from those at most risk from the technology they rely so much upon.

Defend, Recover and Manage

In January 2002, Microsoft's founder and Chief Software Architect, Bill Gates, stepped forward to announce a radical shift in the strategic thinking of the company. He argued that Trustworthy Computing should be built on four pillars: reliability, security, privacy, and business integrity.

All of Microsoft's software engineers are taking part in security training programmes. In software releases, no sample code is being installed by default, VBScript is turned off by default in Office XP Service Pack 1, and Internet Information Server web server is switched off by default in Visual Studio .NET. To track and measure its progress, Microsoft has created a framework for the security objectives of Trustworthy Computing: Secure by Design, Secure by Default, Secure in Deployment and Communications (SD3+C).

Secure by Design

Microsoft's stated objective with secure by design is to eliminate all security vulnerabilities before a product ships and to add features that enhance product security.

Secure by Default

The key idea of secure by default is to 'turn off' services that are not required in many customer scenarios. This reduces the "surface area" available for attack. Making a conscious decision to invoke these services increases the likelihood of their being appropriately managed and monitored.

Secure in Deployment

Microsoft views Secure in deployment as "equally or even more critical because the operation of computers is an ongoing activity". Secure in deployment involves managing and coordinating the protection, detection, defence, and recovery of critical systems means having the right policies and procedures in place to tie these activities together.

The Skoda Principle

If Microsoft made cars and not software, how might Jeremy Clarkson describe Trustworthy Computing on the BBC's 'Top Gear'? "Designed in America and so it's huge?" "It handles like a Giraffe"? It doesn't work off-road?" It was not so long ago that the thought of a Skoda achieving a favourable comparison with an Audi, seemed as improbable an idea as associating the name of Microsoft, with any serious suggestion of secure computing.

Microsoft may be a market leader but like Skoda, it has consistently suffered from an image problem in an area of strategic importance. As Ian Lloyd of the Open Group comments, "Microsoft hasn't established trust only convenience and few businesses have any other option than to go with the flow".

While Skoda, has achieved new respectability for its cars, even from the cynical Mr Clarkson, Microsoft, still cannot shift the weary cynicism that surrounds claims that its software holds security as 'The' number-one priority and that the evidence of its SD3 strategy is already beginning to show. This new commitment to security and trust, confronts the company with new problems. This led one Microsoft executive to remark, "Trust is not something that you can enforce, it's a process and the results are frequently invisible".

I Fear the Greeks

"I fear the Greeks, even when they bring gifts[19]" is a quote from the Iliad and it expresses the attitude of many I have spoken with in relation to the substance of Microsoft's Trustworthy Computing initiative. While in this case, 'Trust' describes a grand technology purpose, our own experience of trust involves honest partnership. Consequently, Microsoft will have to prove its commitment to TWC by being more open and honest about its software than at any time in its history. The company needs to re-build confidence in the platform, by proving to its customers, without a shadow of doubt, that any product release schedule is no longer influenced by the marketing-department or Wall Street's quarterly reporting demands but rather by fitness for purpose regardless of cost and possible delay to future products. This is the company's commitment to its customers but until the world is convinced, many organizations will choose to follow the advice of the Persian proverb, "Trust in God but tie your camel".

Protect and Detect

In defence of its development record, Microsoft argues:

"While the Internet offers tremendous value by opening up new levels of integration with partners, suppliers and customers, it also exposes business systems to new forms of malicious attacks. Despite heightened concern over security, recent incidents

[19] Virgil

exposed potential weaknesses in Microsoft products, the difficulty in deploying them securely, and the challenges of keeping them secure as threats evolve over time. These product vulnerabilities were exploited during recent incidents for three primary reasons":

1. Security boundaries have blurred or dissolved. When valuable data was stored in only a handful of large mainframes that could be accessed by relatively few users, it made sense to rely on the LAN to provide a security barrier. This is dramatically different from the situation today, where confidential and valuable data is distributed widely and accessed by users inside and outside of corporate private networks.

2. New threats have appeared. The architects who designed the foundations of today's systems and networks did not conceive of the innovative threats created by security researchers and hackers. For example, the wide use of Perl and Web-based scripting languages on Web servers has enabled attackers to write exploits in these languages - something that simply wasn't possible years ago.

3. There are more potential attackers. More computers, more Internet connections and sophisticated automated hacking tools mean more opportunities at less effort for attackers. The attention given to successful attacks also encourages new ones. In addition, the payoff for stealing data or disrupting operations at a target, weighed against the likelihood of not getting caught, makes computer-based attacks much more attractive than conventional attacks

While all of these arguments in its defence are valid, Microsoft, the company that most represents the notion of software in the imagination of the public, has become a victim of its own remarkable success. The rapid emergence of the Internet, took the company by surprise and its open-sided 'commodity' approach to software design left it more vulnerable to security exploits than it was prepared for.

Perception is Everything

Having occasionally being accused of being a company in 'Denial' Microsoft has spent the last seven years reacting to the security flaws in its products, through a process of patching instead of 'biting the bullet', establishing leadership and assuming responsibility for latent state security in its software, as reflected by the new SD3+C strategy.

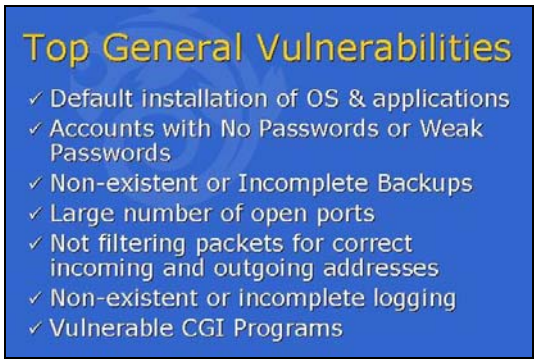
Most recently, Microsoft was recognised for the security work of the last twelve months by the SANS Institute, a leading US research group for systems administrators and security managers, which, in February, presented the company with awards for demonstrating leadership in three security categories. Microsoft won the awards for leadership in the provision of automated security updates; security training for software developers; and the testing of software for security vulnerabilities.

Progress takes time and Microsoft appears temporarily trapped between an uninspiring history and a promising future. The company's success and its unfortunate record as a convicted monopolist, has made it the largest 'Soft-target' in the business software industry. While other platforms, such as Linux, may be reportedly no more secure than Windows, it is Windows that represents the bulk of reported security exploits and it is Windows that represents the 'glue' that connects much of today's wired society.

Absence of Evidence

While many observers [20] would perceive Microsoft as having the most vulnerable platform and products on the market, The Aberdeen Group, in a report published in November of 2003 suggest otherwise:

"Contrary to popular misperception", the report says, "Microsoft does not have the worst track record when it comes to security vulnerabilities. Also contrary to popular wisdom, UNIX and Linux-based systems are just as vulnerable to viruses, Trojans and worms. Furthermore, Apple's products are equally at risk, now that it is fielding an operating system with embedded Internet protocols and UNIX utilities. Lastly, the incorporation of open source software in routers, Web server software, firewalls, databases, Internet chat software, and security software is turning most Internet-aware computing devices and applications into possible infectious carriers."



Aberdeen writes that Microsoft products had no new virus or Trojan advisories in the first ten months of 2002, while Unix, Linux and Open Source software went from one in 2001 to two in the first ten months of 2002, that in the same 2002 time period "networking equipment" (operating system unspecified) had six advisories and Mac OSX had four.

Symantec, arguing from a statistical perspective is very close to the Aberdeen Group position when it comments:

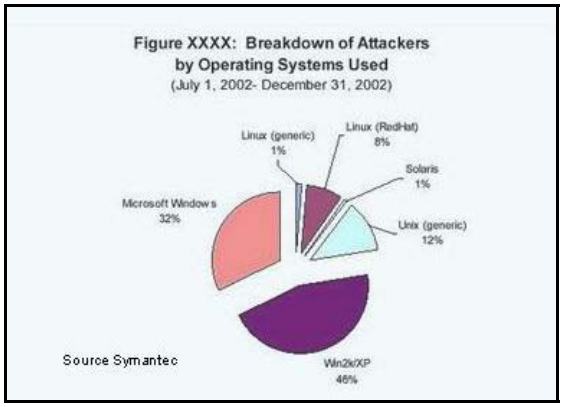
“A number of widely used open source applications were trojanized with backdoors over the past year. The attacks targeted high profile distribution sites that had taken significant efforts to protect themselves. This may serve as a warning not only to other open source projects, but also to commercial software vendors. Rather than targeting individual systems, attackers are clearly exploring alternative ways of impacting a large number of systems in a short period of time”.

What both the Symantec and the Aberdeen reports suggest, is that while reported vulnerabilities on different systems can vary on an annual basis, the overall vulnerability and incident trend continues to increase[21], as reported by other sources, such as Mi2G. While Microsoft claims to be doing everything in the company’s

[20] See Forrester Research ‘Can Microsoft be Secure’ – March 2003 - Forrester maintains Microsoft has suffered unfair criticism of its security efforts, claiming the company's track record is "both better and more complicated than conventional wisdom suggests

[21] Symantec reports that over the past year, 1,200 new 32-bit Windows viruses and worms were released, a substantial rise from the prior year. Maintaining this trend, malicious code submissions during the fourth quarter of 2002 consisted predominantly of Windows 32 threats, as opposed to script- or macro-based threats. Furthermore, three of the Top 5 virus/worm threats reported by Symantec Security Response during the fourth quarter were classified as Win32.

power to strengthen the security of all current and future products and has been awarded Common Criteria[22] security certification for Windows 2000, the company carries an impressive legacy of Windows 95 and Windows NT installations that remain connected to the Internet with inadequately configured firewalls or weak or non-existent passwords.



According to research conducted by NTA Monitor between October 2002 and January 2003 Web server flaws[23], poor authentication mechanisms and faulty log-out facilities remain the most widespread e-commerce security vulnerabilities.

The most regular and serious flaw described by the NTA research was the lack of security behind the "firewall, exposing root access web server flaws and offering hackers access to critical business systems.

NTA echoes the principles of Microsoft's own SD3+C strategy in recommending that the most effective counter-measure lies in the design of e-commerce systems with security as a foundation rather than an afterthought; implementing a secure design across all layers - network, operating system, web server and application. Trustworthy computing then becomes a shared responsibility in which the vendor plays a critical role but one which is only partially effective without commitment from the customer, much like a bank note torn in half, where one side has no value without the other.

The Open Group's Ian Lloyd also identifies the present problem as being a consequence of a lack of standardisation in the IT security industry, claiming that "There are too many different point solutions" and that "No effort goes in – Digital Risk – standards to support interoperability" where trust services fail to recognise the business requirement on which they are predicated.

[22] Common Criteria Security Certification is a government award - See http://www.commoncriteria.org/

[23] While Open Source Apache is recognised to be the most popular Web server, free-ISP-type homepages represent the majority of Apache installations where Microsoft's IIS retains a strong presence in the Enterprise.

No Quick Fixes

An interview with Craig Mundie

When Microsoft's Craig Mundie delivered his 'annual report' on the company's trustworthy computing initiative. He illustrated the deployed population of different versions of Windows within a total active user base of approximately 400 million. The largest installed base remains Windows 95, while the first results of the SD3+C initiative "remain in the earliest stages of deployment". What Mundie said, was important from the customer perspective, as it clearly details the company's intentions in relation to trustworthy computing and it may be useful to study the text of his speech.

"So we know", says Mundie, "that in practice it's impossible for us to remediate the threats that we know exist in the world today in systems that were designed in 1991, '2 and '3 and deployed in '95 and which are actively still in use today... Now, we know that these waves just keep rolling through and they will ultimately change, but it shows how long the threat exists of bad things happening and why it's not completely possible to fix every old system".

"The message here is that there will have to be two tradeoffs that have to be made, and to some extent the events of last September (9.11) have facilitated us in making one of those tradeoffs or changes."

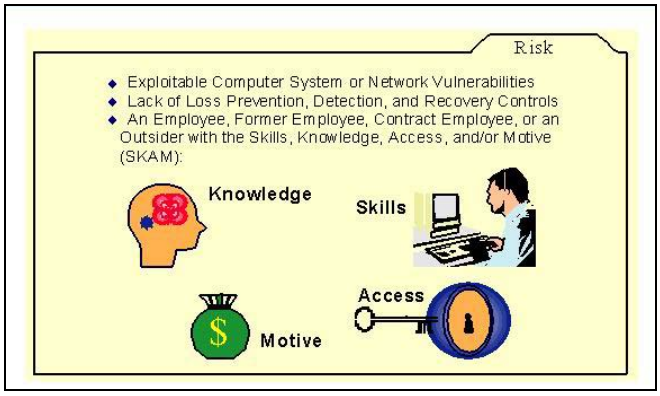
"We have decided", says Mundie, "that we will begrudgingly forsake certain app compatibility things when, in fact, they don't allow us to have a default configuration that opts for more security. In the past, the biggest thing that happened to us was IT managers would come to the company and say, hey, all those new features, they're great, all that new security stuff, that's great, but whatever you do don't break my app. So just turn it all off and trust me, we'll fix the apps and then we'll turn it all on. And the reality is that never happened".

"And so we're going to tell people that even if it means we're going to break some of your apps we're going to make these things more secure and you're just going to have to go back and pay the price."

"Naturally, being secure is going to cost money, but if you are insecure because you're unprepared to foot that bill, then your insecurity stems from your own irresponsibility":

"And the other thing is that the customers, whether they're individuals or corporations, are going to have to make a decision about when and how much they spend to get these machines to be more secure. And to some extent you can do it by insulating them, to some extent you can do it by putting things around them or in front of them that protect them, you know, firewalls in some sense. And then in some cases, you

can just replace them when you get new machines or new software or both that have intrinsically better capabilities".



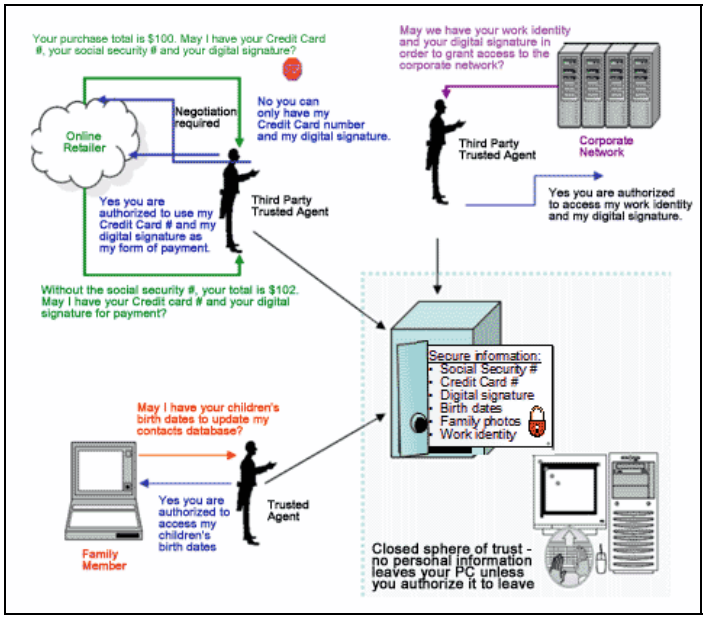
Mundie also referred to the next version of Windows, Longhorn, which will support the Intel-based hardware (TCPA) architecture described as the Next Generation Secure Computing Base (NGSCB) – still widely known as Palladium - , a security and digital-rights management technology which is still at least two years away and which will offer a trusted security environment within the hardware framework.

The Next Generation Secure Computing Base

The Next Generation Secure Computing Base (NGSCB) is to be included in a future version of Windows, possibly in Windows XP successor Longhorn, scheduled for release in 2005.

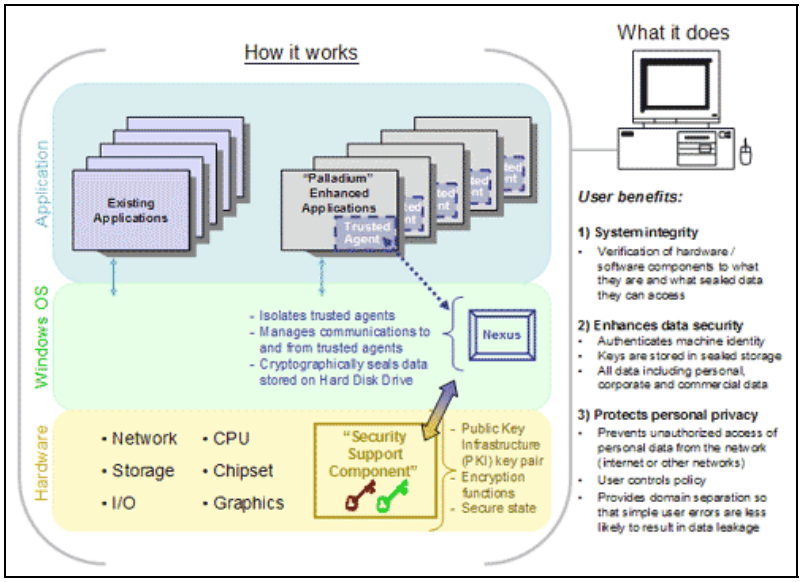
Chip makers Intel and Advanced Micro Devices are working with Microsoft on the technology NGSCB includes a new software component Windows called a "nexus" and a chip that can perform cryptographic operations called Security Support Component. The technology creates a second operating environment within a PC that is meant to protect the system from malicious code b providing secure connections between applications, peripheral hardware, memory and storage.

Future antivirus applications, for example, can run in a secure execution environment to guarantee that the application is not corrupted.

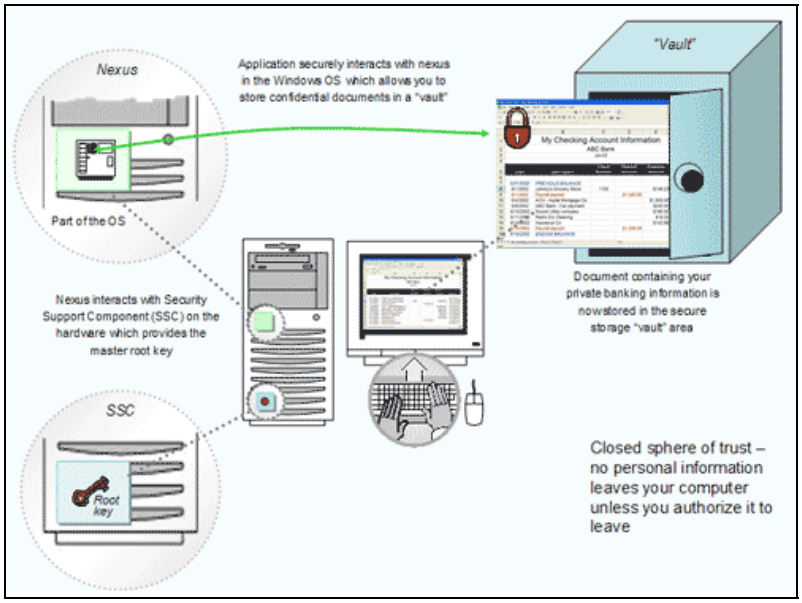


In a Web interview, Adam Barr, a former Microsoft developer, was asked, "What's the story on Palladium (NGSCB)? Is this Microsoft's latest attempt to regain control of the industry?"

Barr answered, "Palladium is at its heart a fairly simple idea, which is hardware support for storing keys and performing cryptographic operations on those keys. It's true one of the uses of this could be for Digital Rights Management, but Palladium is just one component that a (Digital Rights Management) DRM system could potentially use to make it more reliable and hack-proof."



"What Palladium is doing", says Barr, "is going after a security problem that really isn't addressed by current software, and trying to solve it. Microsoft has to fix all the other problems first: make design decisions that favour security over ease of use, make the system easy enough to administer that people actually do so properly, and cleaning up all the bugs. Then it can attempt to write a Palladium system that is trusted".



In summary, the solutions that will appear from Intel and Microsoft tomorrow, offer little immediate comfort to organisations facing by an escalation in the digital threat environment today. The harsh reality for most customers may be found buried in Symantec's 'Managed Service' statistics and between the lines of Mundie's speech. This message clearly passes a significant level of responsibility back to the customer. It argues, that if you are not using the most up-to-date versions of Microsoft software, in conjunction with state-of-the-art Firewalls and supported by ISO/BS7799 information assurance policy, then information security will remain very much a lottery, often determined by accident and a hacker's personal interest in the victim's domain or business.

The Argument for Open Source

Virus Evolution & the Potential for Mass Destruction

By Alan Cox – Redhat Software

This submission discusses the technical possibilities of large-scale automated destruction of personal computers. In addition it looks at why such an attack, although possible is unlikely and at some of the less dramatic but possibly more dangerous possibilities.

Trends in Virus Technology

Early virus technology focussed on infecting the boot blocks (the first instructions read when a computer starts up). Detecting such viruses is very easy and virus design rapidly moved to include viruses that modified executables on the system itself, and viruses that modified the system to conceal infection. Since virus, modified executables are copyable across networks these viruses rapidly became the most common in the internet era.

As Microsoft Windows caught up with “real” operating systems and acquired memory protection and file access control (Windows NT) it became much harder to write a virus that tampered with system files but which could operate as an unprivileged user. Virus writers thus moved to the next easiest conduit for transmission, targeting poor security in file formats and in applications that permit, file transfers (notably email although web browsers have also been targeted). This shift is extremely important to understand, as it is the beginning of a current trend. Viruses, worms and security compromise tools are now fusing into one.

The final technology merging into the same space is that of 'Agents', autonomous systems able to travel around a network acquiring data. In the mainstream, the notion of 'Agents' in this form has remained very much a research field. The accounting of computing resources, security and billing problems for these services are unsolved questions. To the virus writer these issues do not need to be solved, and the use of unwanted viral agents to retrieve and modify data is a very real threat. Viruses that release user data already exist in the wild although their main goal appears to be nuisance value. A viral agent collecting personal data and credit card numbers is not technically difficult to implement.

The final concern in this area is the rapid emergence of viruses and worms targeting the next clear weakness. Users are failing to apply security fixes to their systems. In many cases non broadband users are incapable of doing so due to the size of the updates sometimes required. As a result, worms and viruses are targeting well known security holes, knowing many users will not have fixed them.

The Worst Case Scenario

Most personal computers contain components that can be destroyed or require factory reconfiguration to restore the system. One notorious but easily contained virus called "Chernobyl" targeted a single such weakness. Chernobyl thankfully was not very clever in other ways and did not target anything but the PC BIOS, thus disk data was not lost.

On a typical desktop PC the targets are:

1. Disk Drive -_Many IDE disk drives store the firmware on the platter except for a small loader. If the firmware is erased using drive, update commands the disk requires factory recovery. Drive reprogramming is well understood in the field as people routinely patch the movie industry "region code" support out of DVD drives so they can play movies they legally own and import.
2. BIOS - The initial system software is run from a flash ROM. This can be updated, or erased. It could also be patched to look unchanged but contain added components to randomly perform the other attacks such as disk destruction. Reloading the ROM requires specialist tools or a new ROM chip from the vendor.
3. Expansion Cards -Many expansion cards contain firmware that can be erased, In most cases device would require returning to the vendor in order to fix such an erase

It is thus easy to theorise an economic attack which mixes these kind of destructive agents with a fast spreading virus targeting known security holes and maybe email (One argument for targeting the known security holes is speed of infection, and the fact servers tend to be both exposed this way and the more valuable equipment).

MS-03-007 – "No I am not scared and neither should you be!"

It is questionable what the incentives for such an attack would be. It is possible to key such a fast spreading worm to destroy only boxes meeting a given constraint (e.g. US time zones, English language), however its value as a terror tool is limited by the fact that there is nothing to film, no gradual impossible to stop catastrophe and no perceived deaths. It thus appears your average terrorist could be better employed setting off atomic weapons to topple Cumbre Vieja into the sea.

In addition, it seems questionable that a casual virus developer could pull off such an attack without a large set of machines, a test network and good data on common hardware, along with the needed programming information. However, it only takes one demented genius.

More Likely Threats

The more likely and potentially more dangerous threats will be those based on non-detection. A worm that quietly introduces errors into a company accounting system to frame a director for fraud is massively more dangerous than simply destroying a few computers. There exists a wide variety of other commercially "interesting" attacks – credit card theft, identity theft, bringing down a competitors web site – or even corrupting the competitors' databases quietly and in hard to detect ways so that orders are shuffled and customers become unhappy or shop elsewhere. Government targets are clear enough – tax records, passports, new identities, giving people criminal records, and removing driving license endorsements. The lack of electronic voting in the UK is probably a very good thing given current standards of computer security.

Most government systems are relatively isolated and thanks to historical good luck, we have multiple copies of most data, making it hard to create a complete set of records, or to tamper with all the various records to keep them apparently consistent. In addition, there is very little connectivity between the internet and government – but there is enough for attacks.

Solutions

There are as ever, no silver bullets. Computer security is a process that has to be implemented on many levels. Some of the possible things that could be done are considered below

Fix the Hardware

Adding write-protect jumpers and/or cryptographic checksums to firmware can be used to protect hardware from damage. Already at least one chipset vendor gets this right for the BIOS. Disk firmware could easily require cryptographic keys so that wrong firmware will not be accepted by the drive itself. Many other devices that can be erased could be treated similarly.

Open Document Standards

If the formats of the documents being exchanged, are publicly known, it is much easier to write tools to scan documents for viruses and to verify that the document has no undesirable characteristics? Removing JavaScript from a web page is trivial for example, while removing macros from an MS Word file is not a clear documented process.

Variety of Systems

Very few viruses and worms target multiple platforms and building a cross platform worm is much harder. Critical systems could thus use a mix of hardware and software architectures to get further security in depth.

Auditing

Of all the requirements high quality auditing is important. Even if it is not economically feasible to keep regular backups of a very large data set it is economically feasible to keep cryptographic hashes and thus be able to say what data changed. In many cases, it is possible to keep logs of the changes to a data set. There

are reasonably good standards for audit logging in existence such as those used by the US government recommendation[24].

More Secure Systems

This is perhaps the hardest and most difficult part of the problem to solve. Writing secure computer software is a hard problem that nobody has cracked. Mathematically secure systems such as Eros [25] are hard to get right, extremely hard to prove correct, and harder still to use. Systems such as the NSA secure Linux improve security by trying to turn the current security model from "Nobody will get in" to "If someone breaks in then the harm they can do is limited". Since someone can always get in if clever enough this is an important shift in thinking. The existing standards also fail to provide the needed security. Microsoft recently made much PR noise out of a windows certification for EAL4. However, this is a security level for a system under no real threat.

"The CAPP provides for a level of protection which is appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well-funded attackers to breach system security. The CAPP does not fully address the threats posed by malicious system development or administrative personnel".

Trusted Computing

Trusted computing may well pose more of a threat than a solution. Trusted computing is a 1960's technology which uses a small core "trusted computing base" (or "TCB") permitted to violate rules. The rest of the system is unable to violate rules or harm the TCB. Most focus on this in the PC world is about protecting third party content from the owner of the computer, rather than on protecting the owner of the computer from third party content. The wide deployment of strong tamper-proof encryption is also likely to make it very hard to execute search warrants. While processors will undoubtedly have back doors, the question of who has access to them other than the NSA is of concern to many governments. The UK is perhaps more fortunate in this area as an ally.

Open Source

Open Source systems appear to be more resistant to attack. They allow the auditing of code so that anything placed in the system by hostile agents is identified. In addition, the customer has the power to get code modified or fixed and to make an informed decision having evaluated the actual problem code in the event of a problem. The US DOD survey [26] found the ability to fix software without being tied to a vendor fix was considered an important advantage of Open Source within the DOD.

---

[24] Common Criteria, US Government, 1984 - http://csrc.nist.gov/cc/CC-v2.1.html

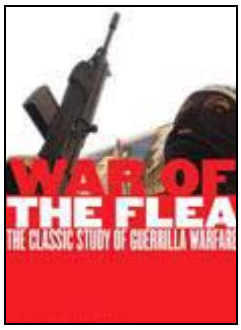
[25] EROS: A Principle Driven Operating System From The Ground Up, IEEE Software, 2002

[26] Use of Free and Open Source Software In The U.S. Department of Defense, MITRE, 2002

The overall security is harder to evaluate, Microsoft for example would claim that Open Source is less secure and point to the total number of published errata. That however ignores the fact that a "base" open source system generally includes vastly more software than a Windows XP CD-ROM, that there are multiple vendors each releasing their own errata, and that many holes found and reported in proprietary software are never made public but merely folded into a service pack or future release. Considerably more research is required in this area in order to separate the lies, damn lies and statistics.

The War of the Flea

"The guerrilla fights the war of the flea, and his military enemy suffers the dog's disadvantages: too much to defend; too small, ubiquitous, and agile an enemy to come to grips with."



So writes Robert Taber in War of the Flea - The Classic Study of Guerrilla Warfare that represents a metaphor for the collision between Microsoft and the ideology of open source computing. Invariably, Linux is presented as the agile guerrilla winning propaganda victories despite Microsoft's heavier armoury and there are signs that Microsoft is increasingly concerned by the growing perception that governments and large institutions are deploying OSS (Open Source Software) or Linux, when in fact they may be simply considering or piloting the technology.

Can You Have a Trusted Open Source?

In my notes from December's EURIM meeting on Open Standards/Open Source in e-government, I have written two comments. The first is that "Open Source is an unstoppable, disruptive technology" and the second, which is rather more damning of the present climate, simply says "No understanding of Open Standards, how these are put together and how these continue to a (a state of necessary) interoperability", which is the key to future success.

The Open Group's President, Alan Brown agrees there is considerable confusion over 'Open Standards' and add that "Open Source doesn't equal open standards" but that Open Source can overcome some of the challenges that open standards failed at" but this is more appropriate in the process integration space rather than as part of an argument over security. From his perspective, Open Source is really about TCO, (Total cost of ownership) and the question of whether clustering Linux Servers is a more cost effective solution than using Windows or even UNIX. He cites the example of Amazon.Com migrating to Linux as a preferred option for exactly such TCO reasons.

Alan Cox argues that the non-proprietary nature of Open Source computing environment makes it more resistant to attack; in much, the same way as a genetically diverse population can resist an epidemic more effectively than a single group, as history demonstrated in South America following the arrival of the Conquistadores.

Open Source consultant Eddie Bleasdale believes that "It is not in the interest of vendors to encourage vendor neutral computing" and insists that the cost of downtime because of what he views as the inherent security failings of proprietary computing, "outweighs all other costs".

Both opinions can claim a considerable following but the question of security and how best to achieve it, is far from the black and white argument that many would wish it to be and is increasingly an examination of different shades of grey. The Open Group's risk expert, Ian Lloyd remarks: "I don't think (Open Source) is any more or less secure. It is very much a question of how you interpret the statistics. Saying that software is 'secure' is an irrelevancy as the people element is more important than the technology element.

As Alan Cox comments, "Considerably more research is required".

Microsoft believes it is the victim of a substantial element of misinformation where unfavourable comparisons are made between its own software and Open Source equivalents. In particular, the company points to what it perceives as common myths:

- Windows is more vulnerable than Open Source.
- Windows vulnerabilities are worse than Open Source vulnerabilities
- Viruses only affect Windows.
- The Open Source community offers better support and faster response than Microsoft.
- Open Source software is more reliable and more rigorously tested than Windows software.
- Microsoft 'sits' on some vulnerabilities and only 'streams' the patches into Service Packs.

Defensible Context

Microsoft's Vice President, Mike Nash, argues that there is a danger of customers being misled by these and other statements and that there exists a danger of misinterpreting statistics which attempt only to match vulnerabilities against market share without offering the context and methodology which are required before any valid conclusion can be drawn.

Referring to the Forrester Report[27] in an interview with PC World, Nash acknowledged IT managers' ongoing high concern, noted in the report, about the security of Microsoft's products. That means Microsoft should communicate more about what it is doing to make its products secure, he said. Microsoft must simplify the process of distributing and installing software patches, Nash said. For example, the company must extend the benefits of technology like the Windows Update

[27] See Forrester Research 'Can Microsoft be Secure' – March 2003 - Forrester recommends that organisations should re-evaluate the security of default Windows configurations at least every three months; build test environments to ensure patch stability; or subscribe to a patch management service as an alternative.

feature, which automatically downloads patches and updates, to its entire product line he added.

Viva Zapatista

Whether by accident or design, it very much looks as if Microsoft, in its attempts to find a more imaginative way of dealing with the threat that Open Source computing involving Linux poses to its Server revenues, is now reacting differently to 'The War of the Flea'.

If Ernesto 'Che' Guevara were alive today, he might wear a penguin logo on his shirt. Linux has become a popular icon that represents a strong Microsoft anti-culture as much as an alternative software philosophy. Whether the technology Linux offers is better or worse than Microsoft's product inventory, is increasingly immaterial to an army of partisan developers. After all, whatever Linux can't do for you this year, collaboration and a common-purpose will allow the people's programmers to make work next year.

Most recently, Microsoft is beginning to comprehend that it is not fighting the equivalent of a tank battle purely around a question of technology preference. Mirroring the political situation, which surrounds us today, Microsoft is facing an ideological struggle for which it is not well equipped and which ultimately could prove more dangerous to its revenues than the creeping risk of Hewlett Packard, IBM, Oracle[28] and Sun Microsystems promoting Linux to their Enterprise customers.

The $1billion question asks whether Microsoft's charm initiative has arrived too late. For the last four years, I have chaired 'The Great Linux Debate' in London and it is clear that Microsoft have spent this time avoiding constructive argument or engagement. When the company has chosen to become involved then it has been with very little subtlety or understanding of the audience involved. As a result, the company shares some responsibility for the creation of the Linux "*sub-culture*" that it fears most. There are however promising signs that, the company, still trapped in a no-man's land between technology and ideology, is starting to understand the true shape of the Open Source phenomenon and is attempting to define a new strategy, involving its Microsoft.Net® Framework[29] and one more capable of dealing with the technical and ideological arguments that are levelled against the company.

---

[28] Oracle CEO Larry Ellison has predicted that the open-source Linux operating system will soon triumph over Microsoft in the battle for the data centre market.

[29] The security architecture of the .NET Framework is composed of a number of core elements, which include: • Evidence-based security • Code access security • The verification process • Role-based security • Cryptography • Application Domains - See Security in the Microsoft® .NET Framework - An Analysis by Foundstone, Inc. and CORE Security Technologies

End of Days

Trustworthy computing may not be oxymoron but it remains very much an aspiration. The evidence shows that even following the painful and expensive lessons learned from encounters with 'I Love You', 'Code-red', Nimda and SQL-Slammer, business and the public sector remain poorly prepared to deal with digital risk and the threat to business continuity posed by the Internet.

Both public and private sectors silos of 'Excellence' exist where information security is involved. Commonly based around the ISO/BS17799 standard, a mandatory criterion where insurers are concerned[30], examples of good practise contrast sharply with a much larger group of organisations who share a very 'ad hoc' approach to information security.

A problem lies in the continued absence of true standardisation across platforms and security solutions. As the many thousands of published vulnerabilities illustrate, not having installed the most recent version of a software application, a Service Pack or a patch [31] leaves a system open to compromise and even the most up-to-date infrastructure has no certainty of immunity unless it is isolated and physically locked-down.

Addressing this question of generic vulnerability and standards, Ray Stanton of Unisys comments:

"Many organisations would prefer to blame Microsoft for the recent problems associated with the Slammer virus and while yes it is recognised the patches were not easy to implement and were reissued by Microsoft, it is not beyond the wit of man to clearly recognise the fault lies at these organisations own feet. These fixes were issued more than six months prior to the attack! The problem was caused more to bad management practice and poor internal processes - irrespective of the fact there is the lack of 'commonly adopted' standards".

[30] The DTI is proposing to make BS7799 a legal requirement – CW360.Com – 4th April 2003 - Biting the BS7799 bullet

[31] Forrester Research in its April 2003 report 'Can Microsoft be secure', recommends the company work more closely with independent software vendors (ISVs) to make sure that patches work against applications. Forrester notes that designing a patch that won't crash an operating system is one thing, but designing one that is also safe for the applications running on top of it is another.

Stanton adds: "Many good standards[32] already exist and many 'bench mark' organisations have adopted them ranging from the ISFs Standard of Good Practice, BS7799, ISO 17799, ISO 13335 etc and yet many of these organisations still were affected - so tell me lack of standards or again just bad management practices [33]"?

The Human Firewall

Research by the Human Firewall Council, supports Microsoft's contention that the key to security management is the integration of policy and technology even the best prepared companies have a long way to go before their organisations' systems and information assets are adequately protected.

According to a report in Computer Weekly[34], the council has pioneered a sophisticated online assessment tool, the Security Management Index, which allows IT and security managers to compare the performance of their companies against their peers and the internationally recognised security management standard, ISS17999.

More than 1,000 businesses and public sector organisations around the world, including 116 in the UK, completed the 30-minute assessment, supplying illuminating data that reveals just how well - or rather how badly - different sectors of the economy manage security.

The index shows that eight out of 10 organisations score 70% or less. Three out of four organisations do not fully implement their security policies and only one in five actively reviews them and keeps them up-to-date.

- Four out five could be breaking the law because they do not have adequate compliance programmes
- Eight out of ten have not fully implemented business continuity plans
- Only one in four has fully implemented access controls
- Only two out of five have fully implemented personnel security policies
- Fewer than 20% have proper incident reporting procedures
- More than half do not have a system of asset classification and control
- The average score for organisations that completed the index was 52 out of 100

The results provide unequivocal proof that most organisations think of security as a problem soluble through technical fixes, such as installing a new firewall or a better intrusion detection system, rather than a management problem for the whole organisation

---

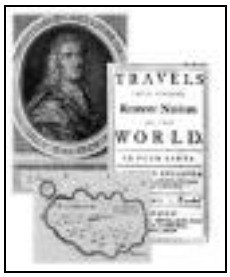
[32] For further information on standards ISO/BS 17799 see http://www.xisec.com/

[33] British Computer Society research suggests that better education of staff is needed: only 50% of managers believe that a security culture is fostered in their organisation, and they feel that low priority is given to promoting such a culture through education and training. Just over 40% of organisations provide IT security training, and 26% recruit IT security professionals. Cw360.com [7-4-2003]

[34] Computer Weekly - Thursday 27 March 2003 – Bill Goodwin – 'Security specialists expose damning lack of rigour'

Gulliver's Travels

The message that underpins Trustworthy computing is tangled in a much broader ideological struggle with elements of the Open Source community, who insist that the Microsoft platform is intrinsically insecure and because of its architecture and engineering, will always be that way.



The evidence however contradicts this view and suggests that when properly configured, Windows is no more or less susceptible to attack than any Open Source product but Microsoft's market dominance and its multiple-version legacy, make it the most attractive and the principal target of the cyber-criminal seeking to maximise potential for damage caused by hacking or malicious code.

Most of us, have at one time read 'Gulliver's Travels'. A few of us may also remember why the Lilliputians were at war and had been as long as anyone could remember. This was the result of an argument over which end of a boiled-egg, should be opened and eaten first. The larger end or the small?

What are the facts? Is good security policy as simple as making a strategic choice between Microsoft and Open Source software? Of the two, which presents the least security risk to business, offers a better return-on-investment and is more developer friendly? The answer may be hard to find but business is trapped in the middle of a propaganda battle, where the truth is scattered in a muddy no-man's land between the two colliding ideologies.

Pareto's Theory in Practise [35]

What is more certain is that Trustworthy Computing, like 'Peace in our time' says more about responsibility than technology. The responsibility and the commitment of Microsoft towards making security the default rather than an option, regardless of the inconvenience this may appear to cause its customers and the acceptance of a shared responsibility on the part of the customer. As Ray Stanton of Unisys suggests, all organisations should have a policy that addresses the most common problems, described by the CERT (Coordination Center)[36], the FBI and NTA Monitor that are between them, responsible for 80% of the inconvenience and damage caused to organisations.

[35] The 80/20 rule

[36] The CERT® Coordination Center (CERT/CC) is a centre of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development centre operated by Carnegie Mellon University

Richard Archdeacon, Director of Consultancy Services for Symantec, believes that an improved information security posture can come from better reporting and more accurate statistics. He comments:

"The challenge for any organisation in attempting to gather meaningful statistics from firewall logs and other sources remains the sheer volume of data, which conceals the information that might warn of an attack or a potential vulnerability; the needle in the haystack. Until this problem is resolved through the availability of more accurate and immediate reporting, businesses will continue to work largely in the dark where information risk is involved".

Conclusions

A series of conclusions follow from this report:

1. eCrime is a rapidly growing problem and is regarded as a serious business continuity threat to both government and the private sector. Businesses need to fully recognise the implications, the nature and scope of information risk and manage the threat using documented and audited:
    a. Policies
    b. Standards
    c. Procedures
    d. Records
2. Regular penetration testing and reporting is not simply advisable it should be included as a precautionary element of any sensible IT security policy[37].
3. Independent statistical evidence and research suggests that while its market share makes Microsoft's products the most frequently attacked, when properly configured, they are no more or less open to compromise than Macintosh or Open Source products.
4. The true Open Source argument involves return on investment rather than security. Focusing on the latter prejudices the decision-support process and presents a distraction.
5. Trustworthy Computing (SD3+C) involves more than a commitment to the development of a more secure and reliable software environment on the part of Microsoft. It demands equal commitment to security 'best practise[38]' on the part of the customer if it is to halt or even reverse the present trend in cybercrime.
6. To increase market confidence, not only must Microsoft continue to build more 'trust' into its software but it must also ensure that in the event of a sudden pandemic, such as was seen with SQL-Slammer, the company can be frank about the problems it faces, reacting fast enough to inform and protect its customers before business interruption reaches its peak. Security patches, when released, need to be immediately effective and problem free [39]in order to inspire greater customer confidence.

If 2002 started with the introduction of Trustworthy Computing then perhaps 2003 should be the year of responsible computing. From a purely security perspective and drawing on the story of Gulliver's Travels, it's the infrastructure in the centre of the egg which we are all trying to protect and how an organization chooses to arrive there and from which end of the security infrastructure, Open Source or proprietary, is simply a matter of judgement.

---

[37] "60% of networks are penetrated over 30 times a year" – PriceWaterhouseCoopers

[38] ISO/BS7799 adoption

[39] Forrester Research recommends Microsoft should improve its patch management processes and should develop a single and consistent set of tools for both applying patches and mitigating security risks.

The Author

Managing Director of Zentelligence (Research) and for eighteen years Chairman and CEO of The Research Group, Dr Simon Moores has also chaired many well-known IT User Groups and Forums. These have included the Lotus Forum – The Java Forum, The Microsoft Forums - The eGovernment Forum, Security First and The ASP/xSP Community.

Acting as an advisor, Dr Moores has assisted The Foreign & Commonwealth Office and Trade Partners UK and has represented the Office of The e-Envoy, as an 'Ambassador', at both EEC and International Government events and conferences. .

A broad-spectrum information technologist, Dr Moores is widely recognized for his independent, forthright and often controversial opinions, writing and publishing research in Computer Weekly, CW360, The Observer and many other national and international publications.

Acknowledged as a leading independent authority on Microsoft and its strategies, Simon Moores has appeared regularly on BBC News, Sky Television News' 'Business Report', Jazz FM radio, Channel 4 News, CNN, CNBC and Bloomberg television and radio.

Acknowledgements

The author would like to thank the following for their comments, cooperation, advice or contributions, which have assisted in the preparation of this report and related research on both Open Source and the Critical National Infrastructure:

Alan Cox – Red Hat Software (UK) Ltd

Stuart Okin – Chief Security Office – Microsoft (UK) Ltd

Dr Steve Marsh – Director of Security Policy, Information Assurance and Resilience – Office of the e-Envoy

Alan Mather – CEO eDelivery - Office of the e-Envoy

Detective Chief Superintendent Len Hynds – Head - National Hi-Tech Crime Unit

Detective Constable Tony Neate - Industry Liaison Officer – NHTCU

Richard Allen (MP) – Liberal Democrat

Malcolm Harbour (MEP) - Conservative

Derek Wyatt (MP) - Labour

Mark Bailey – IT Security Officer – The House of Commons

John Lyons - Crime Reduction Officer - NHTCU

Peter Newport – Managing Director – Quizid Technologies

Andrew McLauchlan – Executive Chairman – Identrus

Dr Detlef Eckert - Senior Director Trustworthy Computing – Microsoft (EMEA)

Peter Cummins – Business Critical Services – Microsoft (UK) Ltd

Dr Ilia Fortunov – Senior Architectural Consultant – Microsoft (UK) Ltd

Chris Kadwill – ICT Manager – Luton Borough Council

Richard Archdeacon – Director of Consulting Services (Northern Europe) Symantec.

Mike Tierney – Sales Manager – Public Sector – Symantec (UK) Ltd.

Allen Brown – President & CEO – The Open Group

Ian Lloyd – Director of Active Loss Prevention Initiative - The Open Group

Ray Stanton – Director of Security – Unisys (UK) Ltd

Nick Coleman – Head of Security Services – IBM

Eddie Bleasdale – Managing Director – Net Project Ltd

Dr John Manferdelli – General Manager – Windows Trusted Platform Technologies – Microsoft Corporation.

John Chirillo – ‘Author of Hack Attacks Denied’ – ‘Hack Attacks Revealed’ – ‘The Hackers Encyclopaedia’