The Register®
Biting the hand that feeds IT

Original URL: http://www.theregister.co.uk/2007/02/26/windows_boxes_at_sea/

Windows for Warships nears frontline service

By Lewis Page
Published Monday 26th February 2007 12:15 GMT

Analysis Everyone knows the differences between Windows and other operating systems. Steve Jobs has recently spent colossal sums telling us that most malware is written for Windows; also that using Windows is no fun and, even worse, seems to involve wearing a tie.

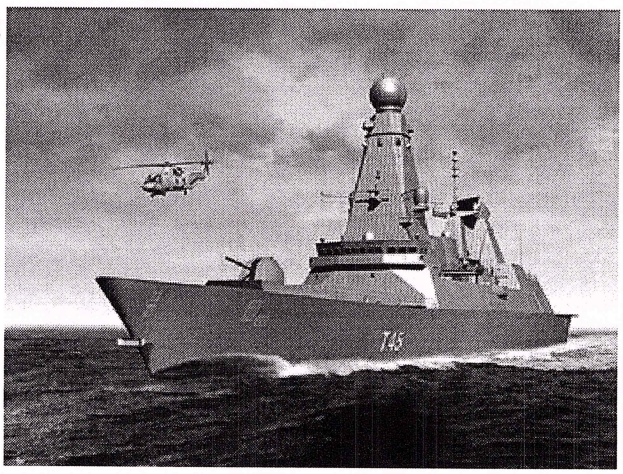
Those acquainted with the more foam-lipped Linux fanciers will also be familiar with the position that Windows use is morally corrupt, indicative of sexual perversion, and causes cancer.

A lot of customers keep buying from Microsoft, however. One may want to deploy a particular kind of hardware, perhaps used only by a few organisations. It may well be that you can only get the associated software from the hardware maker, and the vendor in question doesn't provide anything other than Windows-based machines.

One type of hardware where this is happening more and more is warships.

This shift has already been heavily criticised (http://www.theregister.co.uk/2004/11/05/mod_oks_win2k_warships/). Nonetheless, BAE Systems subsidiary Insyte, the UK's sole provider of warship command systems, has decided to standardise on Win2k (this was during the company's former incarnation as AMS).

The Type 45 destroyers now being launched



(http://thescotsman.scotsman.com/index.cfm?id=122192007) will run Windows for Warships: and that's not all. The attack submarine Torbay has been retrofitted with Microsoft-based

command systems, and as time goes by the rest of the British submarine fleet will get the same treatment, including the Vanguard class (V class). The V boats carry the UK's nuclear weapons and are armed with Trident ICBMs, tipped with multiple H-bomb warheads.

All this raises a number of worrying issues. First up is basic reliability and usability. Most of us have stared in helpless despair at the dreaded blue screen; how much worse would you feel if that wasn't just your desktop gone but your combat display, and it really was the screen of death?

Surely we can't have our jolly tars let down by possibly untrustworthy, difficult to use kit such as Windows? Especially when you reflect that cost is not an issue. When you're buying destroyers at £1bn per hull, the price difference between 26 PCs and the same number of Sun workstations barely shows up.

Big step forward

All that may be so. However, the sad fact is that Windows will probably be a big step forward for the Royal Navy (RN). Anyone who has spent time in an RN warship is entirely accustomed to seeing equipment on which he may depend for his life occasionally throw a double six for no good reason. Windows may be unreliable, but it's hard to imagine it being as failure-prone as the kit which is out there already.

Again, Windows platforms may be troublesome to maintain, but most civilian sysadmins simply wouldn't believe the resources the navy can throw at problems. A present-day Type 42 destroyer carries at least four people who have absolutely nothing else to do but care for the ship's command system. As of just a few years ago, this was still a pair of antique 24-bit, 1MHz machines each with about 25KB of RAM.

Two of the seagoing sysadmins will be senior technicians with at least five years' expensive general training and months of courses specifically tailored for the kit they are minding now. Their assistants will be less skilled, but still useful. They can take care of drudgery – minor bumf, safety checks, making tea – freeing the real techs for serious work. And the on-board team would seldom be expected to cope with anything as complex as a software update. That would be done in harbour by more advanced specialists, probably including vendor reps. Nor do the combat sysadmins get lumbered with general IT desktop support; there are other people to do that, also lavishly trained. If any organisation can keep Windows functional, it's Her Majesty's navy.

There may also be perfectly valid criticisms to be made regarding Windows useability. When triggering missile decoys with seconds to spare, one doesn't need a superfluous pop-up box saying "Do you want to use soft kill?" with "Confirm" and "Cancel" buttons. But this kind of thing isn't going to faze you if you're used to entering instruction sets such as "PE L5414.10N L00335.67E R6000 TMDA [INJECT]" from memory without backspace or delete. During combat, mind. The one group of users to whom Windows 2000 might look pretty marvellous are RN warfare operators.

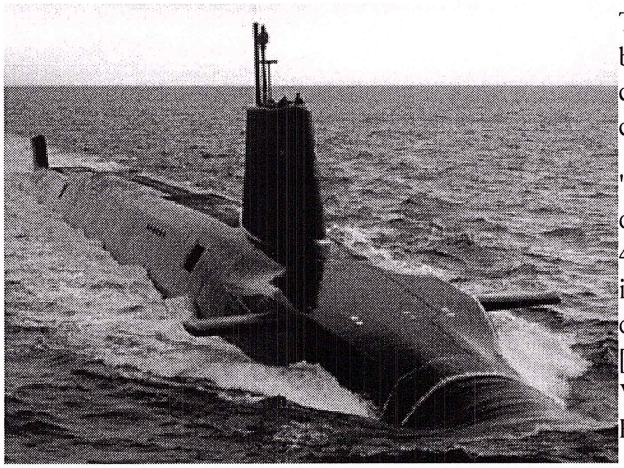
In fact, the navy is easily impressed by almost any modern technology. As another example, the RN is only today getting used to the avant-garde notion of display screens which can be read with the lights on. Her Majesty's warships still have a lot of crazy old circular-sweep CRTs – essentially, modified 1940s-style radar scopes – whose image is so dim they can only be used in darkness. On the bridge during daylight you often need a hood or blackout curtains just to check the radar.

Many of these aged displays have refresh rates measured in deciseconds, not milliseconds. To this very day, RN navigators typically have to track the ship's position in pencil on a paper chart. There is normally no moving-map display of the sort found in

every merchant ship – or even minicab. The results of this luddism are often expensive (http://news.bbc.co.uk/1/hi/england/hampshire/dorset/3051451.stm) and embarrassing (http://news.bbc.co.uk/1/hi/uk/920457.stm).

Customers like this aren't going to be very critical of even the most unimpressive kit. The RN will likely be very chuffed with its huge leap forward to Win2k, though many of Microsoft's civilian customers will be three operating systems down the road by the time the Type 45s join the fleet.

So reliability, usability and maintainability may not be an issue, at least not for these benighted end-users. But what about security? An enemy will find it difficult to exploit a brief, random system crash aboard a warship, as he won't be able to predict it. But downtime caused by malware could well be predictable and/or persistent, giving all sorts of openings to the opposition. Worse, malware can do more than knock systems down. It can extract information and potentially send it elsewhere. It can insert spoof data. Worst of all, it could potentially take control of hardware directly, raising the spectre of weapons being fired to the direction of an evilly-disposed black hat.



The nuclear-armed Vanguard-class boats, perhaps naturally, tend to cause the most worry in this context:

"Of more concern to Windows detractors than the fitting of Type 45s was the news from AMS [that] it was conducting early development work for retrofitting [Win2k] to the Royal Navy's Vanguard-class submarines," Richard Smedley said in LXF(pdf) (http://www.linuxformat.co.uk/pdfs/LXF64.pro_war.pdf).

Paradoxically, perhaps, this is not true. The V-boats are actually one of the less bothersome cases. To be sure, bot-controlled nukes would be bad news, but it isn't really possible. Submarine warfare in general and deterrent patrols in particular aren't a worrying environment for network security. Nuclear-propelled submarines – especially Trident ones – spend almost all their sea time underwater.

The standard UK means of communication with a submerged boat is VLF radio from a single massively secure shore transmitter (http://www.visitcumbria.com/car/anthorn.htm). It is shore-to-ship only, and extremely low bandwidth (say 300 baud). Even this vanishingly thin, one-way, inaccessible pipe isn't always there, and it isn't directly connected to the sub's command system anyhow.

Of course, there are other ways than networks for malware to arrive, but the command system of a V-boat isn't going to have USB slots or optical drives. Furthermore, nobody has ever gained unauthorised access to the interior of an ICBM sub. Peaceniks with time on their hands have reached the outer casing (http://www.tridentploughshares.org/article378), though the boat in question was unarmed and de-fuelled at the time. People more dangerous than the disarmament hippies (http://weblog.greenpeace.org/makingwaves/archives/2006/05/brian.html) have never yet bothered with such capers, perhaps because one can't achieve much once inside.

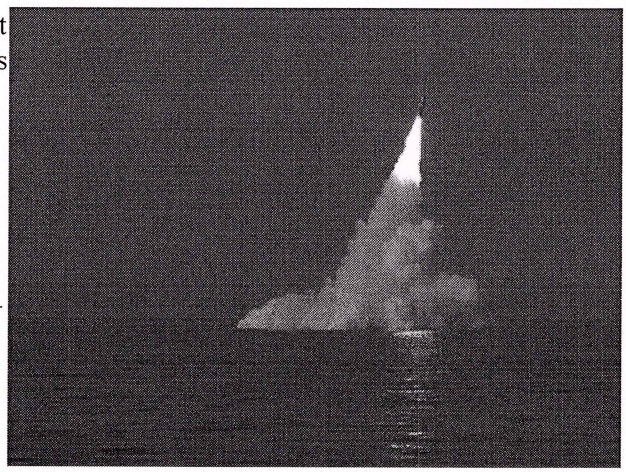
Even bearing all this in mind, it is still possible that a V-boat might one day suffer from

malware in its command system. However, the command system never gets any control over the nukes unless the prime minister has decided to launch them. One-time-pad messages have to be sent and read by live people, physical keys have to be turned by human hands. There are many chances to abort. There isn't any rush or hurry - that's the whole point of sub-launched nukes, after all. You don't need to sweat about an incoming counter-force strike, you don't need to get your shot off first. Submarine strategic weapons are not a time-critical application.

Against all odds

And remember, this is already a highly disastrous, very statistically rare event we're discussing. Somebody's getting nuked here by UK weapons designed and intended for second-strike use, which suggests that a lot of *Reg* readers are already dead. Frankly, a slim chance of technical delays to the retribution doesn't seem worth losing sleep over. If somebody needs nuking, they'll get nuked sooner or later.

Even supposing there's a noticeable risk of the submarine's weapons being permanently disabled, it still doesn't matter. If the UK is launching its nukes at all, they've already failed to achieve their purpose. Far from needing five-nines reliability, a strategic deterrent only really requires, say, 90 per cent assurance that it will function. That's quite enough to deter anyone who can be deterred. You'd need to be a very odd enemy to say: "What's that? The UK's nukes have only 90 per cent reliability due to running on Windows? Well let's attack Blighty then. A one-in-ten chance of not being vapourised by the response sounds good to me."



In theory, an unbelievably puissant black hat in the pay of Dark Forces might manage to write specialist malware that could reliably direct or sabotage the weapons rather than just crash the system. This code could perhaps fire our Tridents at the UK, or an ally, or relatively harmlessly into the sea – without the sub's crew noticing and aborting the launch. Somehow, this uber-malware might be introduced into a V-boat command system and survive undetected until the government decided to nuke someone and the weapons releases were unlocked. A nuclear-armed enemy might be so entirely confident of all this that he might seize the chance to wipe out Britain, happy in the knowledge that there would be no response.

We're starting to search really hard for things to panic about here. It would make more sense to worry about a rogue sub crew – or, likelier, a rogue prime minister. Anyway, an agency with the resources for such an attack would be equally capable of doing it to a Linux box.

So the presence of Windows in the Trident boats isn't of great concern. However – again for hardware reasons – it is reasonable to be worried about the Type 45 destroyers, despite the lesser power of their weapons.

This is because the Type 45s are air-defence ships. They are intended to shoot down incoming ship-killer missiles such as the Russian Moskit (http://www.globalsecurity.org/military/world/russia/moskit.htm), known to NATO as

"Sunburn". A Sunburn flies low above the waves, so it doesn't appear over the horizon until it's quite near the defending destroyer. The entire design of the Type 45 is devoted to getting its fire-control radar as high above the waterline as possible in order to see the missiles further off, but even so it is only 30 metres up.

A radar is a heavy object, and putting heavy stuff high up in a ship tends to make it capsize. Thus, a Type 45 can't expect to acquire a sea-skimmer at ranges much greater than 20 miles. The Sunburn is better than Mach 2, and can hit the destroyer perhaps 30 seconds after appearing on radar – and that's game over for 200 British sailors.

This means the Type 45's combat system needs to go from acquisition to kill in well under 30 seconds – we don't want supersonic debris pelting the ship. During that time an Aster counter-missile must launch vertically from its silo, tip over, accelerate to Mach 3-plus, and bullseye the Sunburn head-on at a closing speed in excess of Mach 5. There is no margin whatsoever for a bored human being to spill his tea, assess what's happening, and decide whether or not to approve weapons launch. This really is a time-critical application.

One might say at this point "why on earth doesn't the navy just use radar aircraft, 30,000 feet up? Then they could detect sea-skimmers hundreds of miles out, and fighters could nail them easily from behind. They could probably spot the planes or ships bringing the pesky things, and take them out from above before the shipkillers were even launched. Why would you ever spend £6bn trying to shoot these things down in the most difficult imaginable way, at the very last possible moment?"

To which the honest answer might be "we in the Royal Navy find that when we buy planes nobody gets a promotion out of it and the kit may get taken over by the RAF (http://www.airsceneuk.org.uk/hangar/2000/jf2000/jf2000.htm). If we buy a ship, however, someone gets to be captain and the slug-balancers leave us alone. Anyway, it's our £6bn, we'll do what we like with it. What do you mean you're a UK taxpayer and it's actually your money? That's crazy talk".

The logical consequence of all this is that whenever a sea-skimmer threat is deemed to be present – and if there isn't any such threat, why are we there in a Type 45 destroyer? – the weapon lockout keys will have to be turned and left turned until the threat has gone away.

As a matter of routine, then, a Windows computer in a destroyer will be enabled to launch weapons autonomously, perhaps for days at a time. Quite a lot of weapons, actually: the sea-skimmers can be expected to come in groups, so the destroyer's computer must be allowed to ripple off a fair number of Asters without asking. It can control at least 10 simultaneously.

Even without considering malware or other Windows-related issues, combat-ready air defence ships always present a severe risk of terrible, deadly accidents because there is seldom any chance to positively identify targets. The US Navy's existing Aegis ships have already demonstrated this (http://news.bbc.co.uk/onthisday/hi/dates/stories/july/3/newsid_4678000/4678707.stm).

It gets worse. This Windows box, unlike the one in the Trident sub, is by necessity heavily networked. A destroyer command system has to constantly communicate with other ships, aircraft, satellites, various organisations in the UK – lots of different computers. Naval surface task groups used crude automated data links before the internet was ever heard of, and nowadays the bandwidth is substantial and varied. A Type 45 will be plugged into many different networks. There will be NATO or other foreign units on some of these nets, which is to say that the authentication protocols and probably codes too will be available to anyone who wants them. Other pipes will connect, perhaps at one

or two removes, to the wild and woolly internet itself.

Hacking Destroyers

It still won't be easy to hack a destroyer, but it will be distinctly possible. If you can't do it over a network, physically infiltrating a surface warship is a trivial task compared to getting aboard a Trident sub. Surface vessels have dozens of upper-deck doors and hatches, compared to a submarine's handful. Destroyers routinely tie up at berths without shoreside security, guarded by no more than a pair of gangway sentries. A surface warship's crew can and often do bring guests and visitors aboard. Security cockups have been known even in naval bases (http://news.bbc.co.uk/1/hi/england/devon/5032516.stm).

So a malware-infected Type 45 is actually achievable, and the destroyer computer will routinely have autonomous weapons authority. Furthermore, even in the absence of malware, opacity and unreliability are key criticisms levelled at Win2k. That just isn't acceptable in this case. For a Type 45 to be even vaguely worth having, you really do need five-nines, rock-solid dependability. A 90 per cent punt won't do here. Against just six sea-skimmers, that would equate to only a 40 per cent chance of survival.

Then there's predictability. Aboard your destroyer in, let's say the Persian/Arabian Gulf, you may need to set up the condition "fire automatically on any unidentified supersonic object", and then unlock weapons to computer control. This, despite the fact there may be half a dozen airliners in the sky above you right then, all moving at high-subsonic speeds. If you can't do this and leave the system ready to rumble for days or even weeks, it isn't going to have the slightest chance of stopping a sheaf of Sunburns when they come smoking in over the horizon.

But you also need to be absolutely certain that Windows won't have a little hiccup, malware-related or not. Let's suppose that the GPS throws a wobbly, for instance, such that the entire plot appears to instantly jump 10 miles sideways. You need to be sure your command system won't decide as a result that the innocent airliner passing overhead has gone supersonic. And so on, and so on. The Insyte engineers will have to include big wads of Windows code which they don't properly understand in the Type 45: they can't realistically guarantee what the ships will do.

When asked to comment on these issues, Microsoft reps rather elliptically replied that "we'll have to decline this one", and BAE/Insyte didn't respond at all. A Navy source with an extensive background in destroyer warfare confirmed that it would sometimes be necessary to trust the Type 45's command system implicitly, but declined to comment on software or engineering issues.

In the final analysis, a working air-defence destroyer with its weapon systems live is by necessity a disaster waiting to happen, far more so than a Trident submarine. It's questionable whether the UK needs this sort of hardware at all, especially at this price. But if we're going to have it – and it seems we are – the kit needs to be controlled by the very best, safest and most predictable software architecture available. It's hard to see Windows as fitting the bill. ®

Lewis Page spent 11 years in the navy, mostly as a specialist in underwater bomb disposal. Highlights of his service included commando training with the Royal Marines, and the opportunity to render safe bona-fide "weapons of mass destruction". Disappointingly, these WMDs were discovered in Wales rather than any sunnier clime. On leaving the service he wrote a book, *Lions, Donkeys and Dinosaurs: Waste and Blundering in the British Armed Forces* (http://www.amazon.co.uk/exec/obidos/ASIN/0434013897/202-9705542-8989460), which was so successful that it is now almost impossible to obtain, though a paperback is forthcoming. Page can be found on the web at www.lewispage.co.uk.

Windows for Warships safe for Royal Navy, says MoD (5 November 2004)
http://www.theregister.co.uk/2004/11/05/mod_oks_win2k_warships/