Information Security Now - 15

John Mitchell

"Who goes there?" is the classic challenge of the sentry guarding the perimeter of the camp. A typical physical security barrier, but what happens when we cannot see the potential threat, or even know if our perimeter has been compromised? Logical security is the obvious answer, but this itself requires us to have the ability of making the invisible visible. Conversely, if we want to keep something secret we need the ability to not only detect the invisible threat, but also to prevent our secrets from being "lit up" by the enemy. Keeping things secret is not only the domain of the military. We civilians are legally required to keep personal data secret and our organisation probably has things that are commercially sensitive that it would like to keep to itself. However, it is not only law abiding citizens that like to keep things secret; the criminals often have a greater desire that their activities are not made public due to the sanctions that may be applied if their secrets are revealed. So security is a two edged sword, with one side wanting to keep things secret and the other side wanting to find out what is being hidden. Interestingly, the Computer Misuse Act may be used against the good guys as well as the bad. If I legitimately want to see what you have electronically concealed, then I need to be certain that I am not opening myself to an accusation of "unauthorised access", or worse still "unauthorised modification". The criminals do not care anyway, so the Act is only a deterrent to the law abiding. Here comes an example. I was asked to check a hard drive for some compromising material. First, I had to be sure that the drive was owned by my client company and not the user of the device. Second, I had to check that the firm had a policy that the equipment should only be used for the firm's business and that they had warned staff that the firm reserved the right to read all the traffic and data. Finally, to be sure to be sure, I required a clear, written request and authority from the company to examine the data. Then it became interesting. The firm believed that the employee concerned was downloading pornography from the internet, but there no indication of pornographic images on the drive. The computer was not "locked down" so the user could load any software that they liked. A trawl of the programs on the machine revealed one called "*Invisible Secrets*". I knew that this software allowed the hiding of data inside image files so I had a good idea that there was some steganography involved in keeping things hidden. But where? The firm was in the graphic design business so there were upwards of ten thousand images on the hard drive, but which one(s), if any, held the invisible secret(s)? I had already found some password protected word-processed files which I had accessed quite easily with some commercially available software because the password was a dictionary word, but now it was find the needle in a haystack time. I tried writing a script to automatically open *Invisible Secrets*, access an image file to see if it asked for a passphrase (which would indicate something hidden) and If not, then cycle to the next file. This did not work because of the interrupts involved so it was back to a more prosaic approach. My assistant noticed that the suspect's cubicle contained numerous pictures of exotic cars so she suggested first searching images of that type. Bingo! The fifth file I opened using *Invisible Secrets* asked for the pass phrase. Fortunately, our suspect had been lazy and the pass phrase was the same password that we had previously unmasked from the word documents. The moral here is that the bad guys need to keep secrets too and they have very powerful tools available to them. Asymmetric encryption, as provided by PGP, is currently unbreakable without the secret key and the legislation embedded in the Regulation of Investigatory Powers Act (RIPA) for the disclosure of a key is a derisory two years in prison. Compare this with fifteen years for making a paedophilic image and 10 - 15 years for Money Laundering and breaching the Proceeds of Crime and the Terrorism Acts. I know which one I would rather confess to!

John is Managing Director of LHS Business Control, a corporate governance consultancy which he founded in 1988. He is currently a member of the BCS Specialist Groups Executive Committee and a former chair of the Information Risk Management and Audit (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454