Information Security Now – 38

John Mitchell

Security threats come in three major forms: unauthorised access, unauthorised modification and denial of service. The UK's Computer Misuse Act (1990) dealt with the first two, but had nothing to say about the third, which is unfortunate, as this is the easiest of the threats to initiate and with today's internet of things, possibly the most damaging. America's FBI recently stated that up to 700 million devices had been subverted with a Trojan which could be remotely initiated for a distributed denial of service attack (DDos). Firewalls give some protection against this type of attack, but can be overwhelmed by the sheer number of pings being received. As no access is gained and nothing is modified it would appear that this type of cyber-attack slips through a crack in the legislation. Even if it did not, the UK legislation would be pretty toothless in bringing to account an attacker from another jurisdiction. This is one of the problems faced by a cyber-defender. The attack can be launched from anywhere: on-world, or even off-world via satellites. Brute force attacks may be crude, but they need very little skill and are difficult to defend against. If you control your electricity supply via the internet, then a DDos attack may prevent you from controlling it. The critical national infrastructure may be up and running, but without a controlling hand.

The way you walk may well be a more reliable authenticator that you are you, than many of the other available authentication methods. The growth of biosciences for authentication is one of the many innovations to counter cyber security threats. In simplistic terms, the cyber threat of impersonation relies on the fact that users have pre-defined privileges which are activated once the user is authenticated by the computer. So the sequence is: identification; authentication; privilege allocation. Traditionally, the authentication mechanism has been something known (password), something possessed (token), or something you are (finger print). A mix of all three can provide two, or three factor authentication. The downside being that the more complicated the mechanism, the more onerous it becomes for the user. So something unique and which is part of you may be the way to go.

However, there are several downsides to this approach. What if you do not carry the required attribute? I know a few people who have fingers, but no associated prints. And you may need a special piece of kit to take the necessary reading which raises the cost and needs to be available at all access points. Even the humble password requires a keypad. So the way you walk, you gait, may well be a good way of identifying you in a crowd and thus a great policing tool, but is not so useful if you want to log into your email account from a hotel room. Signatures are coming back into fashion, but only if you write on a device which can measure the pressure and velocity of your hand writing. Another additional piece of kit. In the recent science fiction series *Humans* the synths (robots) recognise another synth because they shared data when meeting each other. A type of cyber bioscience authentication process. But when they came across synths which did not share data they were lead to believe that the non-sharing synths were human, because a non-sharing synth

would simply say that they were human, and as synths could not lie, this was taken at face value even when all the signs of non-humanity were being broadcast. So a reasonably sophisticated authentication process is trumped by some in-built logic which has greater precedence than the huge amount of data screaming that 'this is a synth I see before me'.

Which leads me to the main challenge faced by cyber security. No matter how sophisticated the authentication mechanism it ultimately come down to a series of electronic pulses being matched against a similar pre-recorded sequence. Air traffic control systems rely on radar to pick-up a plane, but also on the plane identifying itself with a transponder transmission. Without the latter we simply have an unidentified flying object. However, if a plane sends a forged signature, then we have no authentication process to identify the forgery. Naval submarines are tracked around the world by their sound signatures. Each navy maintains an authentication database to identify both foe and friend alike and then spend millions trying to disguise the signatures of their own submarines, knowing that the other side are doing just the same. Keeping the signature database current is a continuous occupation with huge repercussions if it is not.

You will notice that all identification/authentication pairings rely on a simple matching test. So we can predict two types of potential mischief. In the first instance you forge the incoming data stream to match the filed exemplar. In the second instance we change the exemplar to match the incoming stream. So, returning to how you walk. A camera records your gait which is converted by an algorithm into an electronic signature. So, if at this stage we could replace your gait signature with another, the identification attribute is still you. So in the future, when that recorded gait is picked up in a crowd it will identify you, even though the recorded gait is that of another. Nicely framed. Which means that we must have a verifiable process to ensure that the exemplar used in any comparison can be relied on. The second issue of forging the data stream is where most cyber security effort has been directed. Multi-factor authentication makes it difficult to forge the data stream, but also tends to make it difficult for the user.

Despite the technological innovations the actual security battle is fought human to human. One designs and builds an attack mechanism while another does the same on the defence side. Each enhancement on the attack side has to be analysed, deconstructed and neutralised by the defence. The time lag between threat identification and neutralisation is the key to either success or failure. Even a few nano-seconds may be too long where cyber war is the prelude to, or a component of, a kinetic war. So human intelligence need to be supplemented by cyber. We really do need artificial intelligence security officers. But how much latitude should we give them? Should it be the authority to launch a counter attack, or even a pre-emptive strike, to neutralise a potential threat before it takes place? How do Asimov's laws of robotics work when we have cyber versus cyber activity, rather than cyber versus human? Security innovation needs to take account of its wider implications. The difference between a killer app and a killer, may be only a line of code away.