OPINION

Battle-hardened systems needed for cyber warfare


Spirent Communications; 1363581

While secure systems stop information from falling to the wrong hands, they need to be tested exhaustively to stop users turning to faster, yet insecure, public networks, says Daryl Cornelius

Cyber warfare makes for strong headlines, but the term itself is a dangerously emotive phrase that is running ahead of legal and political clarification and restraint.

There is no doubt about the need to be prepared and able to defend against such an attack. The real doubt concerns how best to do it in view of the complexity of the systems being defended and the human fallibility encapsulated in the myth of the Trojan Horse.

The ultimate line of defence has always been the 'citadel'. As long as highly sensitive data is quarantined into tightly controlled networks with no link to any public service, it is relatively safe.

Just as a prime minister's hotline is isolated from the public phone network, NATO's Incident Management Section (IMS) ensures that any material classified as 'secret' is transmitted only internally, by secure intranet, rather than over the internet. IMS staff constantly monitor internet traffic for keywords that could indicate NATO secrets.

Generally, it is an uncomfortable fact that today's armies communicate by mobile phone – rather than the officially designated encrypted phone system – more often than their governments would like to admit. So the first question must be: why do trusted people leave the safety of the citadel?

The answer is that the public service is probably better. The commercial imperative rates performance, speed and user friendliness higher than security and the resulting user experience is so good that it becomes the preferred option. So, if our staff are to remain in the safe communications citadel, we need to provide a service that is as fast, efficient and reliable as any public service.

The only way to be sure that the intranet remains fast and efficient under all loads and circumstances is to test it exhaustively under simulated real-life and extreme loads.

It is the difference between a battle-hardened soldier and a merely well-trained soldier. Today's encryption with high-speed processors is designed to suffer minimal latency, but how well does that promise hold up under exceptional stress conditions? These are just the circumstances when any sluggishness in the system will tempt the user to risk a speedier route – and an enemy knows that the best time to attack is when there are plenty of distractions.

Direct attacks on encryption systems are not the main issue, however. As Alan Way, International Business Development Manager of Spirent Communications, explained in a recent UK Government Communications Headquarters (GCHQ) IP Security Seminar: "Today's network security needs a holistic approach in which endpoint or perimeter security could be potentially the weakest link. Attacking encryption head-on can be extremely complex and time consuming so, from the attackers point of view, the end points could well be the low-hanging fruit. By implanting a keyboard logger, using a Trojan, the attacker can effectively lift the data before or after the encryption process.

"This is why network detection intrusion devices and network prevention devices should also be rigorously tested under all types of load."

So the first rule must be to have a well-defended communications citadel, while the second rule is to make sure the citadel maintains not only high performance but also high quality of experience for the user in order to keep him or her within that citadel.

However well designed the defences, the very complexity of communications networks means they must be exhaustively tested against every known type of attack and also under a whole range of usage conditions and loads. An attacker knows that it is when the network is under stress that it becomes most vulnerable.

Having fortified the citadel – and done our best to keep operatives within it – we must face the fact that the greatest vulnerabilities lie outside that safe zone.

> **The greatest threat of cyber warfare is the least dramatic: subtle manipulation of data and people**

Just as 20th century warfare turned its sights on the civilian population to defeat a nation, so will the cyber attacker know that, however strong the military, it will struggle to operate in the context of a collapsing economy and civilian chaos.

One of the biggest shifts currently happening – and wherever there's a shift there's a loophole – is in virtualisation and cloud computing.

The internet becomes the glue that not only links organisations to their stakeholders, but increasingly holds the whole organisation together. The hacker that accesses a soft switch can re-route traffic at will and virtualisation leads to potential severe vulnerability across the whole business and social infrastructure. Again, the growth in virtualisation demands a corresponding increase in prior and routine testing.

Above all there is human fallibility. The US Army put the gullibility of its servicemen to the test by sending an email from the bogus Army Family and Morale, Welfare and Recreation Command. The email directed users to a website to receive free tickets to theme parks and asked them to give personal contact information.

Of course, no information was collected and such data would not be of much use to a foreign power launching a major attack, but think of the demoralising effect on a soldier from a terrorist organisation that "knows your family and where they live".

So the greatest threat of cyber warfare is the least dramatic: subtle manipulation of data and people so as to destabilise society without anyone realising it is happening.

Manipulating data to re-shape reality was once called 'the propaganda war'; it is now called cyber war.

Daryl Cornelius *is Director of Enterprise for EMEA at Spirent Communications*