Virus attack - how computer networks could heal themselves

The way the body defends itself against attack from micro-organisms is an area being examined by BT scientists looking at defence mechanisms against computer viruses.

People combat viruses such as the common cold by building up natural defences. Then a new strain comes along - and the immune system repeats the process.

The question being asked is: could those principles be applied to building an IT security infrastructure?

Complex networks

Leading a six-year research project into natural biological defence mechanisms - such as the human immune system - is principal engineer Dr Robert Ghanea-Hercock.

The project is being carried out in conjunction with the Ministry of Defence's defence technology centre.

Robert - who is based at BT's research and development centre Adastral Park - said: "Because there is increasing complexity in the networks that companies like BT operate, managing that complexity and making those new systems and networks as secure as possible inevitably demands a new approach.

"The ultimate aim is to create a network that heals itself and can recover autonomously from attack.

"Understanding IT security as though it were a complex adaptive system - like biological systems in the natural world - is key to protecting those networks."

Increasing attacks

Because the scale and value of commercial transactions taking place over the Internet are increasing daily, there are also an ever increasing number of malicious cyber-attacks.

These can be in various forms, including attacks to capture an individual's credit details or to damage a company by a denial-of-service attack, or through self-propagating worms and virus outbreaks.

The research conducted by Robert's team is aimed at increasing the resilience of network systems and applications based on biologically inspired models.

Emulating the human immune system

Using the human immune system as a model it is possible to emulate the behaviour of antibodies and our immune response. Hence when digital-pathogens and cyber-attacks occur, the network responds with autonomous software that mimics the defensive behaviour of human antibodies.

Related work is looking at how to enable an adaptive firewall capacity such that the firewall is extended into every single machine in a commercial network, without interfering with normal operations.

Robert explained: “The idea is to use software agents that monitor what’s taking place. They learn what’s normal behaviour and then anything that looks different to that pattern, i.e. someone trying to hack into the system, they detect and try to take action.

“It’s basically making the defence mechanism more pro-active. Most existing security tools simply block a known virus; but if something is not known, the system has a hard time and that’s why these viruses spread.

“But if you’ve got software that looks at behaviour, it can stop a virus even if it hasn’t seen it before.”

Resilience

Robert says it is now a case of persuading others that this can really work. He said: “Most of the group’s work is writing simulation software that shows that this idea could work.

“We then show this to BT lines of business and other companies to get them interested.

“It’s more to do with how you approach a problem. We are trying to move away from the mindset that you can just put a firewall around your network that stops things 100 per cent.

“The key word is ‘resilience’. We want to make the network robust so that it can sail through an attack rather than grind to a halt.

“The idea is the same as when a human gets a cold: it makes you ill but it doesn’t kill you because your immune system is resilient.”

He explained how important it is to make sure networks are given the best protection possible. “Viruses are getting worse all the time,” Robert said.

“A particular problem is that as more and more homes and small businesses are adopting broadband, this means their computers are always on and they are not as well protected as commercial networks.

“We therefore require more intelligent security applications that are able to autonomously defend all classes of network.”

“The ultimate aim is to create a network that heals itself and can recover autonomously from attack.”