

Crimebusters

Researchers are using advanced processing technology in a move to make the virtual and physical worlds safer. By **Graham Pitcher**.



The internet and email have transformed the way we communicate and source information. Today, it is hard to imagine life without almost instant access to resources around the world. But that facility has come at a price: cybercrime in its various guises.

Cybercrime started off at a low level with viruses. Generally harmless and sometimes entertaining, viruses were an inconvenience but demonstrated to those who were paying attention the importance of proper security procedures.

Since then, cybercrime has escalated to the point where it has become a serious threat to the integrity of the internet and those who rely upon it. Whether it's hacking into Pentagon computers, phishing for bank account information, identity theft or denial of service attacks, cybercrime is a now serious problem.

And it's a problem that isn't going away any time soon. The question now is how should the problem be addressed? A recently formed research institute at Queen's University Belfast (QUB) hopes it can come up with the answers.

The Centre of Secure Information Technologies (CSIT) has been established not only with the intention of keeping crime off the internet, but also to help in the fight against antisocial behaviour and street crime.

With funding of around £30million and a five year research programme in place, CSIT is bringing together research specialists from complementary fields such as data encryption, network security, wireless security systems and intelligent video analysis.

CSIT is one of the first Innovation and Knowledge Centres to be created in the UK. Amongst those funding the research are the Engineering and Physical Sciences Research Council and the Technology Strategy Board. This funding has been augmented by contributions from industrial partners such as BAe Systems and Thales, as well as local agencies and international research institutes.

It will also be no surprise to find out that CSIT is not alone in addressing burgeoning demand for security. Imperial College London has recently established the Institute for Security Science and Technology.

The reason, it claims, is that individuals, communities, businesses and governments are facing new security challenges in many aspects of everyday life, due to advances in technology, globalisation and living in a more interconnected world.

The Institute's mission is to improve security not only at the level of the individual, but also of whole populations. Its research includes ways to prevent identity theft and document fraud, as well as safeguarding transport infrastructure, energy supplies and communication networks.

Professor Chris Hankin has recently been appointed director of the Institute. He said: "Finding ways to harness the science and technology at Imperial to find ways of improving security is an exciting challenge. In particular, I hope to build up our strengths in cyber security, to help make networks less vulnerable."

Dr Sakir Sezer leads the SoC research effort at CSIT. He noted that while the institute was pursuing work in apparently different technology areas, the

work was being done in a coherent fashion. "The network is information," he noted. "What we're trying to do is tackle the need to move security off the network in order to make the internet safer. This means we will need to do more network processing, including deep packet inspection and traffic forensics."

On the face of it, this appears an easy task. But it's not; much of the traffic passing over the internet is encrypted. How do you then determine whether there is a threat or not? Dr Sezer said the approach will also require behavioural analysis, which will, in turn, require a new kind of processing technology. What the work is aiming to do is create a device that can inspect and analyse internet traffic in real time, allowing potential threats to be pinpointed and stopped before harm is done. According to CSIT, such a processor might operate up to 10,000 times more quickly than existing solutions.

The basis of the processor will be the RXP, or regular expression processor; a technology developed by Queen's University Belfast spin off Titan IC Systems. The RXP is said to have a unique approach to the problem by analysing all internet traffic in real time.

"Conventional technology can only deal with information on a character by character basis," said Dr Sezer, "which means it's too slow for real time

analysis. With parallel processors scaled to handle 32 characters at once, real time inspection of huge amounts of data becomes possible."

But Dr Sezer is keen to point out that the technology being developed will not eradicate threats. "Our goal is to minimise their effect and we believe this can only be done with real time analysis and real time response."

CSIT envisages devices such as the RXP being deployed in routers and gateways, moving the protection function from the firewall in the desktop pc into the network.

"And the RXP will provide the performance necessary for this to be performed in the network," Dr Sezer continued.

It's not surprising to find out that CSIT's work has attracted significant interest from industry and from government agencies. "That's because securing the communications infrastructure is important," he said. "A major issue from the governmental point of view has been breaches in their security in the past. Commitments have now been made to improve the communications infrastructure in the UK by including monitoring devices within networks; early detection and mitigation systems which can kick in in milliseconds, rather than days."

CSIT believes it has the right mix of technology and the right researchers to allow the problem to be solved in the next few years. "We have the core technology and partners who complement our work," Dr Sezer observed.

In order to maximise the value of this work, Dr Sezer's team is also looking to optimise the rule sets that enable processing hardware to decide which bit and word sequences indicate threatening behaviour, which traffic may be generated by malicious software and which emails may be carrying viruses, worms and trojans.

"The combination of next generation content processor technology and



"WITH PARALLEL PROCESSORS SCALED TO HANDLE 32 CHARACTERS AT ONCE, REAL TIME INSPECTION OF HUGE AMOUNTS OF DATA BECOMES POSSIBLE."
DR SAKIR SEZER



more sophisticated rule sets will improve internet security beyond recognition," he claimed. "This could mean not only fewer viruses, but also less internet bullying, less identity theft and less internet misuse in general."

One of the techniques being developed at CSIT is traffic mining; the study of internet traffic to uncover anomalies or activities that would prefer to pass unseen – akin to detecting the undetectable.

Traffic mining activities may range from monitoring encrypted channels for unwanted behaviour to uncovering processes that are designed specifically to bring harm to a computer or network system.

The network security work is one of four broadly similar research efforts underway at CSIT. The other three are looking at data security, wireless security and surveillance systems.

Leading work on surveillance systems is Dr Paul Miller, a 20 year veteran in the field. Although this work may not appear to be related to Dr Sezer's network security research, both projects draw on a similar approach; content analysis.

"Our main area of research is video content analysis," Dr Miller explained. "Today's CCTV cameras are passive and only accumulate huge volumes of data. That's ineffective in terms of reducing crime. We want to develop active systems that can generate real time alerts. These can then be examined and a response determined."

These systems will be built on QUB's Integrated Sensor Information System, or ISIS. This will be developed in two ways: by improving the sophistication of the data analysis techniques which the system brings to bear; and providing the necessary intelligence to allow information to be prioritised.

Paralleling the network security research, one of the focuses will be on behaviour analysis. "There has been a lot of work in this area," Dr Miller said, "profiling people and tracking them. From that, we can infer their threat level."

This approach is being developed for a public transport application. "We're working on a major CCTV system for buses," Dr Miller continued. "Passengers could be profiled when they get on the bus and, using crime statistics, produce a degree of threat. If it's high, that video would be pushed to the top of a queue. If the threat level is high enough to suggest an assault maybe about to happen, the video feed can be sent back to the bus, with a warning that they are being watched or that a police car is on its way."



In Dr Miller's opinion, people profiling is key to the system's success. "A lot of work has been done on event detection, but we're looking at event management. But to accomplish this, we will need wireless technology and this will need to be more secure."

Not surprisingly, Dr Sezer observed: "There's a lot of commonality between our research projects in terms of algorithms."

Dr Miller says around 30% of his work will be based around the RXP processor. "But the rest will be algorithms."

Security is not immune from the need to reduce power consumption and the amount of data captured. "This work will result in a new generation of silicon processing at the video camera," Dr Miller believed. "This could be an ASIC with a power consumption of, say, 5W." The benefit of processing at the camera is the reduction in data load. "One of the big issues is if processing has to be done at a server. You may have a lot of compressed data to handle and dealing with 64 channels in real time is not a trivial task."

"THERE HAS BEEN A LOT OF WORK [ON] PROFILING PEOPLE AND TRACKING THEM. FROM THAT, WE CAN INFER THEIR THREAT LEVEL."

DR PAUL MILLER

One of the aims of Dr Miller's work is to make public transport safer and easier to use. And this is one of the 'grand challenges' which CSIT is addressing. Called security convergence for transport corridors, this project aims to bring convergence between information and physical security

technologies. Such technology will, it is hoped, enable secure transport 'corridors' that facilitate the rapid transit of people in the transport sector – including airports. And recent events make it likely that such systems will be in demand.

Like CSIT, the Institute is pursuing interdisciplinary research, encouraging collaboration between engineers, scientists and medical researchers to tackle major security challenges. Its research themes have been chosen for their likely impact on personal security, the protection of public places and the national infrastructure. A number of key security enablers have been identified, including sensors and sensor fusion, image analysis, data analysis and data mining, biomedical imaging and network sciences.

Despite the apparent size of the problems CSIT is addressing, Dr Sezer remains optimistic that the challenges will be solved. "We will have delivered IP within the first three years," he concluded, "and we'll see companies commercialising our work within five years."