Protecting the critical infrastructure in the face of cyber–warfare

Posted on Wednesday 17th November 2010

‘One of the highest priority national security risks to the UK.’ This is how cyber–security is regarded in the recently presented National Security Strategy. The document, which outlines the main security concerns of Britain and how the government intends to deal with them, further observes that cyber attacks can have ‘potentially devastating real–world effects’ on government, military, industrial, and economic targets.

So why do cyber attacks pose the same level of risk as terrorism, international military crises, and major accidents or natural hazards?

In June 2010, a Belarusian security company reported the discovery of a new, complex piece of malware – ‘Stuxnet’. What distinguished Stuxnet from the thousands of pieces of malware discovered around the same time was its targets and its likely inventors. Stuxnet was designed to ultimately attack SCADA (Supervisory Control And Data Acquisition) systems; that is, the systems used to control and monitor industrial processes, such as gas pipelines, power plants, and water treatment facilities.

The sophistication of Stuxnet and the level of resource needed to develop it have convinced many that Stuxnet is the product of a state-sponsored cyber–warfare program and much speculation has also circulated about its actual targets.
Several lessons can be taken from the Stuxnet story. First, Stuxnet marks a shift from ‘traditional’ cyber attacks, which are deployed for financial gain, to attacks that attempt to control critical factory operations. While attacks on virtual assets, such as credit card numbers or online banking accounts, are bad enough, attacks that could cripple a nation´s critical infrastructure would clearly have terrible consequences. Second, cyber attacks are no longer the realm of cyber criminals – they can be carried out by resourceful, government level agencies, and be used as part of a cyber–warfare effort. Finally, future attacks will be increasingly targeted, focusing on a specific computer system, whose inner workings, and weaknesses, have been studied in detail by the attackers.

This new sophistication of cyber attacks and their critical targets carry several implications for the security community, both in industry and academia. In particular, we need to focus our efforts on developing better tools and techniques to assess the security and integrity of our critical infrastructure; better methodologies to design and implement reliable secure software for these components; and better approaches to protect them from attacks.

The Formal Verification and Security Group in the School of Computer Science has considerable experience in devising techniques to analyse complex designs and to ensure the safe execution of software. Its members have also investigated the security of critical systems, such as the e-passport technology, online banking, and electronic voting machines.

Marco Cova
Lecturer in Computer Security at the University of Birmingham

For more Birmingham briefs please visit **www.birmingham.ac.uk/news/thebirminghambrief (http://www.birmingham.ac.uk/news/thebirminghambrief)**