



search  technology

Lessons from America

If you ask computer studies students at the University of Malta or at Mcast to give an example of a breach in computer security, they might come up with the following story.

A major corporation sought the services of a computer security firm for vulnerability assessment. A week later, the contract was finalised and the security firm came back with a detailed and lengthy report on the client's computer security vulnerabilities.

The corporation's chief IT guy was confounded on how the security firm discovered all those security holes without setting foot in the corporate grounds. Here is what has transpired: The security firm purchased a number of low-cost USB jump drives. In each drive, the autorun feature was enabled and a root kit programme was installed. The drives were then randomly scattered in the company parking lot.

The following day the jump drives were maliciously disseminated, several of the root kit programmes were automatically activated and started relaying company information to the security firm. The employees were victims of their curiosity. The moment the jump drive was inserted into the USB port, the autorun feature installed the root kit into the hard disk and wiped itself out of existence from the jump drive to prevent detection.

If you insist to know from where the students got this story, they will tell you that they heard it from Guillermo A. Francia, a professor in the Department of Mathematics, Computing and Information Sciences at Jacksonville State University, Alabama. Over the past few months he has been lecturing at the University of Malta and Mcast as a Fulbright Scholar.

"Computer networks are made of hardware and software that, in theory, can never be completely verified. Theoretically, proving that a computer network is 100 per cent secure is an unsolvable problem," Dr Francia told i-Tech in between his lectures in computer security and forensics.

"This does not mean that providing a secure computing environment is hopeless. One should always bear in mind that information security is a process and not a goal. The process entails the creation and implementation of sound policies, standards, and practices in order to be able to maintain an acceptable level of confidence in the security of the system infrastructure."

Dr Francia echoes what many security experts are saying when pinpointing the real cause of trouble.

"The weakest link in security is the user," he insists. "Part of the problem can be attributed to lack of training. The propensity of users to give way to curiosity is another contributing factor. Yet another is the demand of most users for convenience and ease of use. Most users do not want to be hampered by complicated password requirements, firewall rules, e-mail filters, and browsing restrictions. Human behaviour is so complex and unpredictable. It is imperative that computer systems and protocols need to be designed around this limitation."

Therefore, he advocates the "great and urgent" need for security awareness training that is designed, not only for home computer users, but also for all computer users in general.

Forensic experts in IT have the right tools but it is a continuous struggle where there is no room for complacency.

"Presently, there is a proliferation of digital forensics tools that are available and can be used to track and prosecute the culprits of security attacks. Perhaps most troubling is that the bad guys on the internet are always on the prowl and seem to be maintaining a well-organised communication channel. Newly discovered hacking and penetration techniques spread like wild fire through these channels. The challenge for digital forensic researchers and experts is to maintain vigilance on the constantly evolving sophistication of cyber crimes and to expedite the research and development of systems to neutralise the anti-forensic tools."

Asked about his experience in Malta, Dr Francia revealed that he found Maltese students to be not so different from students in the US when given the opportunity to study computer security.

He believes that with the imminent establishment of SmartCity Malta, our country is on the verge of becoming a very huge venue in IT globalisation.



Guillermo A. Francia (third from left) with some of his students at MCAST.

"Offshore companies will start demanding IT workers who are trained in secure coding, secure network administrations, database security, digital forensics analysis, and security compliance and auditing. These are areas that, I believe, Malta should concentrate on. The question at hand is what can Malta provide that will make her stand above or preferably over, the other global IT hubs such as India, China, Romania, Ireland, and the Philippines?" concluded the American professor.

- ◀ **Global mobile phone use to pass three billion**
- ▶ **Microsoft rolls out web storage and photo gallery**