Business Line

Date:21/08/2006 URL:
http://www.thehindubusinessline.com/bline/ew/2006/08/21/stories/2006082100090200.htm

Hackers show the way!

R.K. Raghavan

In a blow to anti-terrorism efforts, `hacktivists' demonstrate how easy it is to clone e-passports.

Two conferences held in Las Vegas over five days, earlier this month, brought to focus live security issues that should be of interest to everyone who surfs the cyberspace these days. The annual "corporate-driven" Black Hat meeting and the less organised and a more "anti-establishment" DefCon that follows the former continue to attract the `Who's Who' in the business of cyber security to the Sin City for an exchange of ideas and experiences. Both afford hackers and their ilk an opportunity to expose the chinks in the armour of those who produce gadgets or software and claim these are invulnerable.

While Black Hat is ten years old, the DefCon started three years earlier. The numbers present at the two venues have been growing each year. Compared to the 3,000 who gathered this year, I am told that a mere 100 came to the initial Black Hat conferences. The DefCon attracted nearly 6,000.

More than before, a wider spectrum of interests is now represented. And the conferences are no longer just an American show. They are being taken more and more seriously all over the globe. While the corporate world is present in the form of giants such as Microsoft and Cisco, the FBI also finds it useful to send its officers to get a glimpse of the new hacking tricks from a law enforcement perspective.

Talent of all kind

Interestingly, the occasion is also utilised by companies for talent hunting to embellish their workforce. In the final analysis, one can either learn from the many expert demonstrations, which are a star-attraction, or squander away valuable time in raucous parties that go with the two meetings.

A lighter touch to the events comes from pranksters among conference participants who enjoy themselves penetrating the Vegas hotel TV billing systems or wireless networks. These games, some of which can offend sensibilities, keep everyone on their toes! The organisers themselves are wary of being taken for a ride by those trying to barge in without tickets. The incentive for such dishonesty actually comes from high admission prices. For instance, entry to the DefCon conference this year cost as much as $100!

In view of the past experience of specially designed badges being counterfeited by skilful participants, this time the organisers got a circular badge prepared by an electronic hardware designer of San Diego. The badge depicted the DefCon logo of a skull and crossbones and a smiling face with two light-emitting diodes for the eyes. A tiny microprocessor inside made the eyes blink in four different ways. The general belief was that this was a secure badge that none duplicated this time. But the organisers would have to come up with something totally different at the next conference if they want to keep intruders away!

Absorbing `hacktivism'

Also absorbing is the tension usually generated at the conferences between `hacktivists' (active hackers) and big companies from attempts by the former to pick holes in new products. There was plenty of drama this year following Microsoft's bold decision to put to test its newly designed Operating System, `Vista', which was promoted as a very secure successor to Windows XP. Vista is slated for a January release. It seemed as if MS was trying to disprove the widely held belief that it did not care a great deal for security. Much to the amazement of the crowd Rutkowska, an unpretentious researcher from a Singapore-based firm, was quickly able to prove that it was possible to bypass a mechanism created by MS to block any unsigned driver software from running on the system. She also presented a rootkit — which she called Blue Pill — that could serve as a backdoor for intruders. MS officials were impressed by Rutkowska's presentation, and promised to make checks.

The point however is that Vista was vulnerable only when running in the administrator mode. A standard user cannot easily introduce or activate a malware, because there is protection in the form of a User Account Control (UAC), which is a Vista feature that disallows many user privileges available normally. Rutkowska herself admitted that her demonstration did not establish Vista to be totally insecure and that only some minor refinement was called for to make it more secure.

Passport clones

Perhaps the most sensational disclosure at the Black Hat conference was that e-passports, touted the world over as an effective anti-terrorism mechanism, were far from invulnerable to cloning attempts. Lukas Grunwald of DN-Systems, Hildesheim, Germany, told the gathering that passports equipped with radio frequency identification (RFID) tags could be easily copied with the help of a laptop, an RFID-reader and a smart card writer. He actually demonstrated the transfer of data from his passport to a smart card carrying an RFID chip. Such a copied chip could later be built into a forged passport. This revelation could be of great concern to all immigration officials in the world, but for US authorities especially it could be a cause for immediate worry, because RFID passports are scheduled for issue in that country from October this year. The only saving grace is that the data on such a passport could at best be cloned and not altered.

Many other subjects such as weaknesses in wireless networks and the vulnerabilities of the widely used Blackberry also figured at the two conferences. There was also a presentation on how Xerox machines could be subverted to breach data security. I was impressed by the FBI choosing to be present on the occasion. This highlighted the growing dimensions of cyber crime and the role played by those who gathered at Las Vegas in solving such crime. This should give some ideas to our own CBI's leadership. My next column will deal with these and other issues.

(The writer is a former CBI Director who is currently Adviser (Security) to TCS Ltd)