

# To monitor schools better

**Runa Mukherjee**

**N**EW DELHI - Along with the tremendous educational benefits brought about by the Internet, have come increasingly difficult network security threats and challenges.

To begin with, network threats have changed from identity-based threats to content-based ones, putting enormous pressure on network security assets to try to adapt.

Compounding matters is the growing emphasis on "real time" communication and access to information, which forces these network security assets to work even faster to find malicious content before it can do its harm.

Conventional network security systems—which are just a collection of mostly software-based point solutions cobbled together into an ad hoc "system"—have not been able to keep up with the need for "real time" protection. Vishak Raman, country manager, Fortinet India, said: "Students are the real



*Vishak Raman, Country Manager, Fortinet*

hackers today. They are better than the professionals as the resources are available to them in plenty. Also, they can do a lot of trial and error and become perfect with practice."

He explained that it is the students who have the time and skills to make use of the freely available root kits on the Internet to their

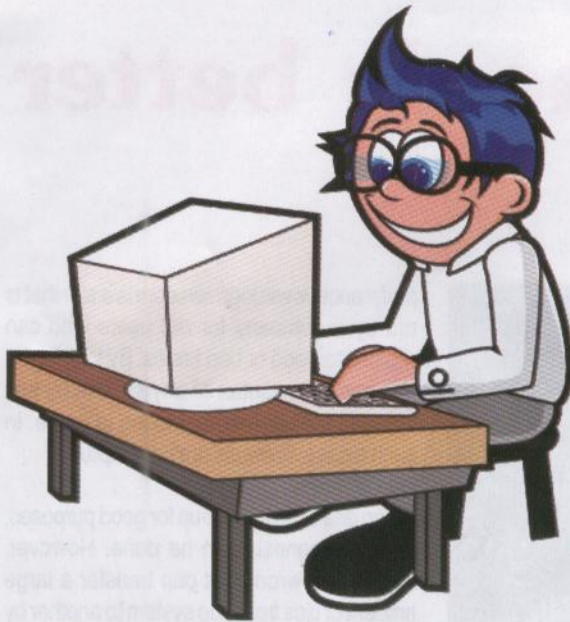
preference. [www.logmein.com](http://www.logmein.com) is a site that is run by a company for net users who can utilise it to good or bad tastes. By logging in, one can take control of any system by just entering the username and log in name. In such a case, firewalls are not helpful.

When one uses this set-up for good purposes, remote diagnosis can be done. However, when used wrongly, it can transfer a large amount of files from one system to another by just knowing the required password.

"Bot Networks are tools for spamming. For instance, if you need to send information or data about a new product to a large number of people, other's mail servers are illegally used to mail in bulk. As a consequence, the genuine company from whose server the content is being wrongfully mailed, becomes blacklisted," he said, emphasising on another tool that is easily available on the Internet and is causing a lot of harm lately.

When talking about the latest security

*The Internet has increased students' exposure to many valuable and useful sources of information; unfortunately, however, it has also made it easy to access inappropriate or illegal content, distribute malware and utilise campus networks for non-educational pursuits. Key issues like malware infection and distribution and access to inappropriate content by young students have placed an enormous strain on all resources that are associated with the health, maintenance or support of campus computing systems and networks. While numerous products are available today that can be used to filter inappropriate content, eliminate viruses and worms, detect network intrusions and prevent access to critical computing assets, the cost of procuring and managing these systems stretches the personnel and budget limitations of most educational institutions. What is needed is a new, architecturally different approach to network protection for educational environments that is effective, inexpensive, easy to install and maintain, and consistent with applicable government requirements.*



*Students get to see secure content on school computers*

applications, Vishak Raman said that normal firewalls are not enough in today's security scene. Even second-generation firewalls that do deep packet inspection are not enough.

"They are like the airport inspection one goes through, the baggage are checked. But, fragmented pieces of any object may go unnoticed.

"Thus, it is easy to reassemble that object once inside the plane and then use it for harmful purposes," said Raman.

Fortinet's products do complete packet reassembling, which means it first fragments all the parts of the content/data coming in, inspects and discards accordingly, and then reassembles them.

Security is important at every level, though it is preferable to

prevent illegal data at the gateway level itself. When asked how expensive a complete system would be, he emphasised on the fact that for a sound security system, one needs to invest a good amount of money on installing and maintaining.

Talking about the problems that the Indian security market is facing, Raman said: "People buy free, uncertified products that are mostly fake as they don't want to spend too much. New products are being offered in the market (like anti-virus, etc) with no credentials. Uncertified products do more harm than good."

Amity University and BITS Pilani are some of the esteemed institutions that have applied Fortinet's Antivirus Firewalls and Fortinet's ASIC-powered Antivirus Firewalls (that can scan email and web content) for their institution campuses.

Thus, it's important for schools and big educational institutions to strengthen their security in a time when all types of content, both good and bad, are flowing freely via the Internet.

These institutions must primarily use certified security products so that the detection rate capability is very high and students, who are the best hackers, as Raman calls them, should gradually understand what is of use to them and what's definitely out of bounds. **CP**

## Reveleus futureproofs governance structure

**UNITED STATES** - Reveleus, a business of i-flex solutions and a leading global provider of analytical applications for the financial services industry, recently announced the availability of the Reveleus Governance, Risk and Compliance (GRC) framework, a comprehensive approach to implement a governance structure, manage enterprise risk, and enable regulatory compliance.

This framework brings together a direct measurement and surveillance capability unique to the financial services industry.

However, it will have a more traditional Risk and Control Self Assessment approach.

With the Reveleus GRC framework in place, financial institutions will gain a higher degree of operational insight and improve business performance by avoiding the traditional 'band-aid' approach.

A comprehensive GRC framework solves two pressing risk and compliance challenges faced by financial institutions worldwide - 'hidden costs' of multiple systems and the duplication of processes that are not only expensive to maintain, but also hinder the ability to holistically manage the impact of external and internal risk and compliance events.

"With a financial services industry focus, our GRC Framework and GRC

Solutions Experts fill an important gap in the current market.

It empowers executive management with a process oriented approach that ensures compliance with multiple regulations and better measurement of risk," said S. Ramakrishnan, CEO of Reveleus and Mantas.

Reveleus' leadership in Enterprise Risk Management and Compliance combined with Mantas' industry-leading behavior detection platform offers the ideal framework to 'future-proof' financial institutions.

It allowing them to address governance, risk and compliance through a single platform.