$100 Laptop May Be at Security Forefront

October 9 2006

(AP) -- The $100 laptops planned for children around the world might turn out to be as revolutionary for their security measures as for their low-cost economics.

The One Laptop Per Child project, a nonprofit begun at the Massachusetts Institute of Technology, aims to improve education by giving children bright-colored, hand-cranked, wireless-enabled portable computers. Governments are to buy the laptops - beginning in 2007 with up to 7 million machines in Thailand, Nigeria, Brazil and Argentina - and hand them to kids for them to own.

The machines have garnered the most attention - and some skepticism -

for the design elements helping to keep their price low. Among other things, the computers will employ the free Linux operating system, flash memory instead of a hard drive and a microprocessor that is slow by today's standards but requires minimal power.

But programmers also have been taking advantage of the start-from-scratch nature of the project to design security protocols that they hope will greatly surpass those found in mass-market computers today.

The designers are still testing their approach with outside security experts - which is widely considered wiser than keeping such matters secret. But already they believe the security setup could make it unnecessary for the laptops to have anti-virus software.

Standard computer design generally lets most any program access any file stored anywhere on the machine. That is one reason why flaws in programs can be exploited by outsiders to steal or erase private information.

By contrast, the $100 laptops will force any application to run in "a walled garden" and limit the files it can access, said Ivan Krstic, a software architect at One Laptop Per Child focused on security.

Even if the security were to fail, Krstic believes a specialized encryption technology will prevent the BIOS - the software that runs a computer when it is initially turned on - from being overwritten. That means the PC could not be rendered unable to boot up.

"It's essentially unbelievably difficult to do anything to the machine that would cause permanent hardware failure," Krstic said.

Extensive security measures are necessary because so many of the machines are expected to be built, making them a large target for

mischief.

One particularly thorny potential problem is that the laptops can communicate with one another in a "mesh" network, sharing data and programming code. A computing Web site reported this week that Krstic had described that setup to the ToorCon security conference as "very scary."

But he contended to The Associated Press that the comment was taken out of context.

"We have code-sharing in the machines, which is really scary if we were not paying attention to it," he said. "But we think we have solutions to all of these problems."

One of the principal organizers of ToorCon, George Spillman, said Krstic's presentation was "very well received" because the $100-laptop designers have thought a great deal about security but "they're not arrogant enough to believe they have everything locked down."

Spillman believes at least some of the measures Krstic described are likely to be successful, though he cautioned: "There's always going to be some kind of a hole somewhere."

Walter Bender, a co-founder of MIT's Media Lab who is overseeing software and content on the $100 laptops, said children should be able to tinker with the laptops and learn how they work. To that end, these security measures can be turned off by the PCs' owners.

To protect against that leading to disaster, the laptops will automatically back up their data up on a server whenever the machines get in wireless range of the children's school. If a child loses data, the files can be restored by bringing the laptop within wireless range of the server.

On the Net: laptop.org

By BRIAN BERGSTEIN, AP Technology Writer
© 2006 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: $100 Laptop May Be at Security Forefront (2006, October 9) retrieved 10 April 2024 from https://phys.org/news/2006-10-laptop-forefront.html