High Security for $100 Laptop

Bryan Hintz | 11:45 AM

SAN FRANCISCO – The One Laptop Per Child project, which proposes to give every child in the developing world a computer of his own, dangled fans with the promise of breaking down barriers of economic disparity.

Now it’s imposing hard-bitten security geeks with a plan to lock down the hundreds of millions of educational machines against spyware and computer intruders.

The laptop, officially called the XO, includes a swiveling LCD screen that can switch between low-resolution color and higher-resolution black-and-white. It also has a camera and microphone that enable clear video calls, three USB ports, a 2MB of RAM, 512 MB of flash storage, built-in Wi-Fi with extraordinary range, a long-lasting battery rechargeable by a cord or car battery, and a custom, Linux-based operating system that allows users to run programs on their XO laptops.

Millions of XO laptops are expected to be produced late this year, with Thailand, Brazil, Uruguay and Rwanda, among others, signed up for the rollout. Implementations of the XO’s virtual machine will be the first in the world.

Still, the XO laptop will have an anti-theft system designed to render stolen laptops useless. Each XO is assigned a “lease,” secured by a virtual sandbox. “Vista’s sandboxing is trying to impale sandboxing on something broken,” Krstic said.

Krstic’s no fan of Microsoft’s security, either -- despite Vista’s imposition of limited permissions on programs, and its isolation of Internet Explorer in a virtual machine. “Vista’s sandboxing is trying to impale sandboxing on something broken,” Krstic said.

Krstic’s objectives are to attack the problem of malware by removing the economic incentive to attack, and to make security usable. But it should come as no surprise -- given how thoroughly the project has rewritten the conventions of what a laptop should be -- that the XO’s security isn’t built on firewalls and antivirus software.

Instead, the XO will promise a security system that takes a radical approach to computer protection. For starters, it does away with the ubiquitous security prompts so familiar to users of Windows and antivirus software, said Ivan Krstic, a young security guru on break from Harvard who’s in charge of security for the XO.

"How can you expect a 6-year-old to make a sensible decision when 40-year-olds can’t?" Krstic asked in a session at the RSA Conference. Those boxes simply train users to check "yes," he argued.

Krstic’s system, known as the BitFrost platform, has only one user prompt (turning on the camera) and imposes limits on every program’s powers. Under BitFrost, every program runs in its own virtual machine with a limited set of permissions. Thus a picture viewer can’t access the web, so even if a hacker comes up with an exploit that lets him control the program, he couldn’t use it to grab all the photos on the laptop and upload them to the internet.

"Applications can no longer run rampant," Krstic said. "Spyware becomes very, very hard. It can’t spy on the keyboard. You can only spy on how a user uses their program."

Krstic contrasts this approach to Microsoft’s Windows XP where every program, including Solitaire, has the right to access the web, turn on the video camera, open spreadsheets and send e-mail.

Programs downloaded to the computer can’t "request a set of permissions that let them do bad things," Krstic said, unless that software has been certified by a trusted authority, which will be either One Laptop Per Child or one of the countries signed onto the project. Users can, however, manually assign more power to a particular program through the security control panel.

Krstic’s objectives are to attack the problem of malware by removing the economic incentive to attack, and to make security usable. While the idea of limiting permissions program by program dates back as far as 1990, according to Krstic, it’s not been adopted widely because it puts the burden on application writers to deal with security.

Other Linux/Unix-based systems -- including Apple’s Mac OS -- run programs with authority limited to a local user, but that’s not enough, said Krstic, because the program can still delete user files, even if it can’t touch the underlying system files. Krstic’s no fan of Microsoft’s security, either -- despite Vista’s imposition of limited permissions on programs, and its isolation of Internet Explorer in a virtual sandbox. "Vista’s sandboxing is trying to impale sandboxing on something broken," Krstic said.

Still, Krstic admits there’s a drawback to his system: It limits interactions between applications.

"This kind of model makes it more difficult for glue between applications to be built," Krstic said. "But 99 percent don’t need glue."

Beyond cyberthreats, the XO laptop will have an anti-theft system designed to render stolen laptops useless. Each XO is assigned a "lease," secured by a virtual sandbox.

Krstic, because the program can still delete user files, even if it can’t touch the underlying system files.

Krstic’s objectives are to attack the problem of malware by removing the economic incentive to attack, and to make security usable.

Still, Krstic admits there’s a drawback to his system: It limits interactions between applications.

"This kind of model makes it more difficult for glue between applications to be built," Krstic said. "But 99 percent don’t need glue."

Beyond cyberthreats, the XO laptop will have an anti-theft system designed to render stolen laptops useless. Each XO is assigned a "lease," secured by a virtual sandbox.

Krstic’s objectives are to attack the problem of malware by removing the economic incentive to attack, and to make security usable.

Still, Krstic admits there’s a drawback to his system: It limits interactions between applications.

"This kind of model makes it more difficult for glue between applications to be built," Krstic said. "But 99 percent don’t need glue."

Beyond cyberthreats, the XO laptop will have an anti-theft system designed to render stolen laptops useless. Each XO is assigned a "lease," secured by a virtual sandbox.

Krstic, because the program can still delete user files, even if it can’t touch the underlying system files.

Krstic’s objectives are to attack the problem of malware by removing the economic incentive to attack, and to make security usable.