Trust Linux!

November 20 2009

(PhysOrg.com) -- A team of researchers has implemented support for 'trusted computing' in a commercially available version of the open source operating system Linux, breaking new ground in the global drive toward more secure computing environments.

The latest release of openSUSE, a Linux version sponsored by software maker Novell, comes packaged with software that allows users to set up a trusted computing (TC) environment on their computer, enhancing security beyond the antivirus programs and firewalls that frequently prove inadequate at keeping bugs, viruses and spyware at bay.

Promoted and developed by major chipmakers and software companies in the international Trusted Computing Group, trusted computing uses both hardware and software to create a trusted and secure environment, whether on a home PC, a web server, in a data centre or over a corporate

network. At the core of the technology is the trusted platform module (TPM), which is a chip that, among other security-boosting features, generates and manages cryptographic keys, verifies the identity of the computer on a network and protects software and data from malicious changes.

Awakening the dormant chip

Many new laptops and increasing numbers of desktop PCs and servers already have TPM chips as standard, while chipmakers such as Intel and AMD have started incorporating the technology directly into their latest generation of processors. However, most TPM chips are currently lying dormant, awaiting activation with the arrival of software that can make use of their enhanced security features.

“The hardware is there… what is needed are operating systems and software to exploit it,” says Herbert Petautschnig, a researcher at Austrian technology group Technikon.

Technikon led a consortium of 23 research and business partners, including AMD, IBM, HP, Infineon and Novell, in developing open source software and applications for TC environments as part of the EU-funded OpenTC project. The group’s implementation of TC support in openSUSE version 11.2 involved building a trusted software stack (TSS) for Linux, developing universal virtualisation layers (including improvements to the Xen hypervisor virtual machine monitor) and creating TC and TPM management software. It constitutes a pioneering implementation of TC technology.

“openSUSE is now the first operating system to offer full TC support,” Petautschnig notes. “Until now, TC had been implemented for specific applications, such as Microsoft’s BitLocker hard drive encryption in Windows Vista and Windows 7 or the fingerprint reader on some HP

laptops… With the OpenTC platform we are extending the TC environment to the full operating system and beyond," the project manager adds.

Unlike traditional security technology that operates only at the software level and only starts protecting a computer after it is loaded, TC technology provides security from the moment the power button is pressed. As the system boots and runs, the OpenTC platform continually monitors the computer for changes and ensures that only trusted, verified software is functioning. In a networked environment, it verifies the identity and integrity of the computer. And it allows different pieces of software and data to be "compartmentalised" so there is no exchange between them even as they share the same computing and/or network resources.

Safer online transactions, trusted corporate networking

OpenTC developed several proof-of-concept applications for the technology. In one, called private electronic transaction (PET), the team showed how it can verify and secure online transactions, such as accessing a bank account. In another, they showed how TC compartments can provide secure remote access to corporate networks, both keeping company information safe on an employee's home PC and ensuring that the employee's personal information, photos and games are not visible to their employer.

The ability of TC technology to keep data and processes safely isolated from each other can be extended to enable virtual data centres. As demonstrated by IBM in the OpenTC project, TC software could be used by data centre operators to provide virtualised resources to different clients while sharing the underlying physical infrastructure,

thereby ensuring different companies' data remain separate and secure.

The logical next step, which members of the OpenTC consortium plan to explore in a new project, is to extend TC to cloud computing to enhance the security of services and computational resources provided over the internet. Another project, TECOM, a follow-up initiative to OpenTC that has also received EU funding, will aim to develop TC solutions for embedded platforms, focusing particularly on smart phones and mobile computing applications.

Several of the project partners are commercially exploiting the results of the OpenTC project internally. Petautschnig says they are also open to investor interest to support further development of TC technology. Consortium members are also active in standardisation efforts, helping to extend trusted computing to mobile platforms and the Java programming language, for example.

Despite controversy, a bright future

In the past, TC technology has stirred controversy, not least over its potential for abuse by software and hardware makers to restrict what computer users can do and its applications for digital rights management. However, Petautschnig believes the future for trusted computing systems is bright as the technology starts to be seen as an essential tool in the fight against an intensifying onslaught of hack attacks, viruses and spyware bombarding the world's computer users.

"Most people will not know that TC components are running on their computers keeping them safe. Conversely, at present most do not know what information is being leaked and stolen by spyware and viruses running on their machines," Petautschnig notes.

More information: OpenTC project

Provided by ICT Results