In networks we trust

February 24 2010

(PhysOrg.com) -- European researchers are proposing a paradigm-shifting solution to trusted computing that offers better security and authentication with none of the drawbacks that exist in the current state of the art.

Trusted computing (TC) is a hot topic in computer science. Major software and hardware providers are planning to include TC components in the next generation of computers, and the US army and the US Department of Defence reportedly require trusted platform modules on all their computers.

Trusted computing is a system comprising hardware and software modules that ensures that the software running on a computer has not been altered or maliciously modified after its initial installation, thus ensuring compliance with the original intended functionality. It is a way of enhancing security, preventing viruses and other malicious code, or malware, and protecting intellectual property.

For example, a TC system can verify that a malicious user has not altered the program of the music player on his computer in such a way as to ignore or bypass the checks on the permissions and restrictions of the songs being played.
Current systems work but are heavily dependent on hardware which limits their usefulness. A big problem facing computer science now is how to ensure a trusted computing environment on a remote, untrusted, machine.

This is an important problem. Trusted computing can reduce or even eliminate the risk of viruses and malware, and it can enormously enhance computer security - all major gains for consumers.

The module system can also be employed as a useful tool for digital rights management (DRM). It goes far beyond current validation methods - which often only authenticate the software during installation, leaving both the code and the computer vulnerable to later modification.

But lessons from the past show that hardware-dependent security systems are dogged by problems. They can fail to entrust valid software, or can fail to communicate with other elements in the system. This happened, notoriously, with some systems using new DRM techniques for high-definition TV.

Trusted security

Difficulties can arise, too, when components are updated. A far more robust solution would provide real-time 'entrusting' on remote, untrusted machines. It could enhance security and provide a universal solution to the trusted computing challenge.

The solution may not be far off, thanks to the work of the European RE-TRUST project. RE-TRUST sought to provide remote, real-time entrusting on an untrusted machine via the network.

"In many cases, computers are connected to the network at all times, and this trend is increasing," explains Yoram Ofek, coordinator of RE-TRUST.

"Initially, we started out with the assumption that nothing can be trusted, but on reflection, we realised that many network entities are trusted, like Google, Yahoo, Ebay or Microsoft," he explains. "So then we looked at

how we could create trustworthy entities on the network that could then ensure software was authenticated on untrustworthy machines."

RE-TRUST, which stands for Remote EnTrusting by RUn-time Software authentication, provides a novel methodology for both software-only and hardware-assisted remote entrusting (RE).

Whereas hardware-assisted entrusting requires a special chip either on the computer's motherboard or inserted into a USB drive, RE-TRUST uses logic components on an untrusted machine to enable a remote entrusting component to authenticate - via the network - the untrusted machine's operation during runtime. This means it ensures that the software is running properly and that the code integrity is maintained, thus almost completely guaranteeing security.

A big idea

It is a big idea. "All applications and solutions running over a network, such as the internet, can benefit from the RE-TRUST approach. RE-TRUST will have a major impact on all commercial applications and solutions where security or trust is a concern, independently of whether they are based on a client-server or a peer-to-peer paradigm," Prof. Ofek explains.

This will become even more vital as more and more services move online. Already, music is increasingly distributed online and TV is shifting in that direction. Software and data are mature online markets that could also benefit from the RE-TRUST approach.

Currently, digital rights holders stand opposed to peer-to-peer networks, mainly because of their association with piracy. But peer-to-peer still offers probably the most efficient distribution method for large files. The RE-TRUST solutions could entrust peer-to-peer networks so they

become a powerful new distribution channel.

Mutating code

The team developed a large number of novel solutions to persistent problems. Code mobility and reconfigurable computing for software protection use mobile hardware agents, essentially a ‘dongle’, that implement monitoring techniques for securely producing and delivering code integrity attestations for an application.

Orthogonal replacement, on the other hand, is a novel client code replacement strategy. The client code is periodically replaced by new code. That code, when combined with the code running on the server, delivers seamless functionality to the user and so remains invisible to the latter, while in fact the code is mutating in real time, thus preventing any malicious manipulation and frustrating any attempts to reverse engineer the original application.

Voice over IP (VOIP), too, came under the scrutiny of RE-TRUST. Project partner Gemalto provides a USB device that contains a smartcard. By taking advantage of the USB device, this integrity role is delegated to the smartcard. With this design, a monitor sends application properties to the local control service located on the smartcard which is able to check for the code integrity.

These are just a few of the results, and the project has already had a big impact. Some of the work, like Gemalto’s smartcard, has direct applications, with other work destined for future technologies or products.

Finally, the researchers will continue with some elements of their study. It all means that, in the very near future, our trust will reside in the network.

More information: RE-TRUST project - re-trust.dit.unitn.it/

Provided by ICT Results