An Airbag for the Operating System – A Pipedream?

Markus Linnemann
markus.linnemann@internet-sicherheit.de
Prof. Dr. Norbert Pohlmann
norbert.pohlmann@informatik.fh-gelsenkirchen.de

Institute for Internet Security
University of Applied Sciences Gelsenkirchen
Neidenburger Str. 43, 45877 Gelsenkirchen, Germany
www.internet-sicherheit.de

We have all become accustomed to fastening our seatbelt in the car, moving the seat to the right position and adjusting the mirrors correctly, but the most important safety features are the small technical refinements installed in the car: the anti-lock braking system (ABS), ESP and the airbags. As soon as the situation becomes dangerous these safety systems are activated and protect us against serious damage or injury. Why are there no such safety mechanisms for computer operating systems which we also use on a daily basis?

IT Safety versus Safety in the Car

There are many security tools which help us to detect and protect ourselves against harmful software. However, virus scanners and firewalls have to be properly configured and maintained. They do not therefore offer automated security. While it is rare for motorists to be attacked directly or intentionally put into dangerous situations, repeated attacks in the IT world on all computer systems that are connected to the Internet are an everyday occurrence. Currently it takes an average of approximately six minutes until an unprotected computer system is infested with malware.

Developments in the IT field occur several times faster than in the automobile industry, for example. The complexity of established operating systems is increasing continually in order to meet the rising demands of the information and knowledge society. However, the proneness to errors also increases disproportionately with this complexity. This fact is underlined daily by the large number of patches and safety updates.

It is always easy to recognize one's own car by its colour, make, shape and number plate, with the key being the ultimate means of authentication of the driver with respect to the vehicle. In the IT world we use passwords or security tokens for our authentication with respect to a computer system, but a computer system does not provide any authentication of itself with respect to us.
By the same analogy, we are not able to determine whether we are sitting in the right car and whether the car will also brake when we press the brake pedal.

The Trusted Computing Idea

Trusted Computing is a security technology being developed by an industrial consortium with more than 160 international members. The results of this consortium are open specifications whose fundamental aim is to make IT more trustworthy. Here the intention is to improve the security of distributed applications in a manner that is economically viable, i.e. there should be no massive changes to existing hardware or software. The main idea is the use of a hardware component (Trusted Platform Module) that cannot be manipulated and with which software-based attacks can be counteracted.

The specification of the Trusted Platform Module (TPM) has been implemented by many manufacturers and is currently integrated into over 60 million computer systems. At the end of 2008 it is hoped that more than 200 million of these chips will have been supplied.

This security module acts as a trusted anchor in a computer system (root of trust). Starting with the booting process of a computer system, all hardware elements and software programs (BIOS, operating system, application programs …) are measured with the help of hash functions and their statuses stored in the Platform Configuration Register of the TPM. The system configuration of the computer system can consequently be measured in full and is therefore also verifiable. In the car analogy this is comparable with an inspector who records the entire assembly process of a car and subsequently is able to show the "integrity" of the vehicle on the basis of a certified list of control numbers (e.g. chassis number) for all the parts. If a car part is replaced, the car is no longer in its original condition and is no longer trustworthy in comparison to the list. This only monitors the state of a system in relation to a reference. It doesn't mean in general that the new state of the system is unsecure, but its possible. This is precisely the method of system configuration verification offered by the TPM. Using these security functions it is possible for computer systems to authenticate the status of their system configuration to a user or other computer systems. This procedure is known as "attestation".

Moreover, the TPM offers the opportunity of sealing data and storing them confidentially. In this process the data are tied cryptographically to the system configuration during encryption. This procedure is known as "sealing". In this manner it is ensured that sealed data can only be accessed if the computer system is in a known state (system configuration). In the figurative sense it is therefore possible to determine precisely whether, for example, the braking system has been tampered with or not and therefore whether it is fully functional.

Security Platform as Part of the Trusted Computing Idea

Up to now Trusted Computing functions have only been tools which can be used to generate more trustworthiness in computer systems. However, the term Trusted Computing stands not only for security chips, such as the TPM. It is an umbrella term for all functions which can generate security using new methods. A TPM module alone does not bring greater security. This is a passive security module that offers security services. In order to be able to use this in a confidential manner, a security platform is required which guarantees just this property. In the analogy of the car it is the employee who monitors the construction of the car together with the test engineers who check the authenticity and functional efficiency. In technology it is an operating system-type security platform.

Current operating systems cannot be used as a security platform, as they are simply compromised and can use viruses and Trojan horses to simulate trustworthy statuses which do not correspond to the actual statuses. A security platform therefore positions itself above the hardware and below the conventional operating system. Its task is to be as immune as possible to attacks and to check safety-critical processes from this situation.
In order to be able to fulfil these specifications, a security platform should consist of a very small code base and therefore be far less complex than established operating systems. As a result of minimalisation the error probability is considerably smaller and the trustworthiness higher. By means of virtualisation techniques a security platform is in a position to execute several applications and/or operating systems in parallel. It is therefore possible to execute individual secure applications in parallel in so-called compartments completely isolated from the established operating system. The trustworthiness of the secure applications can be verified by the measurement opportunities offered by the TPM. It is therefore no problem if the established operating system has been compromised by malware, as all security-critical processes can be executed outside the operating system by secure applications. The compartments can contain either exclusively secure applications that have been adapted for the security platform, or lean operating systems with standard applications. In the latter case the operating system is then measured together with the application in order to be able to demonstrate the intactness, i.e. the integrity, at all times (illustration 1).

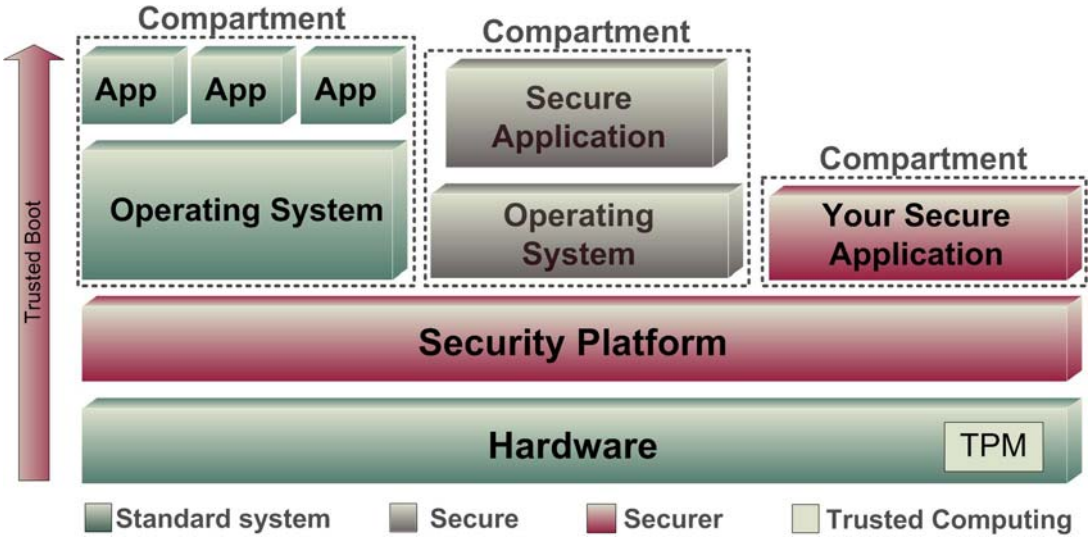

Fig. 1: Example: System architecture with the Turaya security platform

A security platform in combination with Trusted Computing technology offers a broad spectrum of design possibilities for trusted applications. This makes possible end-user systems which can safely administer and store data. Harmful software such as Trojan horses and viruses are simply isolated from security-relevant data. Server and client systems can be reliably authenticated - for example during online banking the bank's computer can be identified at all times and the bank data processed confidentially.

The Airbag for Operating Systems for More Trustworthiness

With Turaya, the EMSCB (European Multilateral Secure Computing Base), in which several universities and IT security firms are involved, provides a trustworthy, fair and open security platform based on Trusted Computing technology. It also offers the opportunity to enforce rules and regulations (policy enforcement), thus providing new and trustworthy possibilities in enterprise rights management. The processing of classified documents on different computer systems with different policies becomes possible. For example, documents can be viewed and printed on certain computer systems, while on others they can only be viewed.
The aim of the project is to create a security platform with an open architecture and interfaces that serve as a basis for trustworthy IT systems. New and innovative business models are made possible by the provision of the security platform for PCs, PDAs, cell phones and embedded systems.

For our project we are looking for further partners who wish to build on the Turaya security platform in order to provide new inspiration from Europe in the field of IT security. Further information on the project is available on www.emscb.org.

The airbag for the operating system is therefore no pipedream. It enables a large leap to more security in IT, as in the analogy of the airbag for the car. This is being permanently refined and today offers side protection, head protection and protection for motorcyclists. We believe that Trusted Computing technology in combination with a security platform based on an open architecture and open interfaces also has the potential to solve a number of today's security problems as simply as an airbag.