tNAC – trusted Network Access Control meets security platform

Marian Jungbauer, Norbert Pohlmann

{jungbauer | pohlmann}@internet-sicherheit.de

1 Introduction

Current and future networks must be flexible and open in terms of their expansion. At the same time these networks should enable trusted communication. The flexibility and inexpensive use of the Internet brings along a lack of security which only allows a limited usage of the available possibilities. Field workers use their computer systems in many different environments with varying security requirements and conditions. Home workers use their PCs for private purposes and regular employees take their notebooks home. Due to the temporary or permanent removal of computer systems from the company network - and therefore also from its protective measures - these computer systems are exposed to significant dangers. If a computer is compromised by malware outside a company network, the company's security mechanisms will be bypassed upon its reintegration into the company network (either directly or via the Internet).

Even today there are possibilities in existence for expanding networks in a flexible manner and equipping them with security services - for example via VPNs which offers encryption and user authentication. However, there is a lack of security mechanisms which guarantee the trustworthiness and the identity of the used computer systems.

The Network Access Control (NAC) concept is part of a fairly new group of security concepts which makes the trustworthiness of computer systems verifiable and therefore helps to establish trustworthy and secure network connections. In a NAC enabled network the configuration of any connecting computer system is preventively checked before the network access. Only if the security policies, as defined by the network operator, are fulfilled, a computer system will be considered to be trustworthy and then allowed to access the network and the connected services. Computer systems with a faulty or undesirable system configuration cannot enter the network which is therefore protected from damage.

With the Trusted Network Connect (TNC) [Trus08] specification the Trusted Computing Group is developing its own NAC approach. The development is taking place through the Trusted Network Connect Subgroup [Trus06] with over 85 firms represented and is currently available (May 2008) in version 1.3 [Tru+08]. The aim is the development of an open, producer-independent specification for verifying endpoint integrity.

Besides TNC there are further NAC approaches in existence. The most prominent representatives are Cisco Network Admission Control (Cisco NAC) [Cisc04] as part of the "Self-Defending Network" strategy and Microsoft Network Access Protection (Microsoft NAP) [Micr08] released along with Windows Sever 2008. In addition to these three "major" solutions, there are many further approaches from firms such as Check Point, Juniper Networks, StillSecure, Symantec and Vernier Networks.

2 Limitations of today's NAC Solutions

All current NAC concepts – including the given above – have limitations; for example the complex management and a barely existing interoperability.

But the core limitation is the lack of trustworthiness caused by the use of common operating systems. The trustworthiness created by any NAC solution depends on the trustworthiness of the client's measurement readings representing the client state. These readings must be correctly measured and transmitted in a trustworthy manner without modification to the NAC network. With common operating systems there is no possibility to guarantee the correctness of the measured values. If the operating system of a computer has been compromised, the measurement readings can be influenced by the malware at any time which leads into a paradox. Because of the permanent risk of unnoticed falsification, any collected data must be considered as being compromised and therefore not trustworthy. This was demonstrated at the Black Hat Conference 2007 using Cisco NAC. By means of a modified Cisco Trust Agent (CTA) it was possible at all times - irrespective of the computer status - to gain access to a NAC-protected network [Heis07].

In order to get around this paradox, TNC offers a certain level of protection against manipulation of the hardware and the possibility of signing and therefore securing the transmission of the measured values through its optional and direct support for the Trusted Platform Module (TPM). However, while still using common operating systems the possible level of trust reached by using a TPM is still limited, because malware can still manipulate the measurement readings directly at the measured components.

3 Solution: Integration of NAC into Security Platforms

The limitation mentioned above can only be solved by an integration of NAC into a security platform. This chapter gives an example of such integration on the basis of TNC and the security platform Turaya.

The security platform Turaya has been developed by the former EMSCB research and developing project [Emsc07]. Turaya does not replace common operating systems. It's a new security layer positioned between the hardware and the operating system. It can control security relevant processes and gives the ability to securely use Trusted Computing functions [LiPo07].

One of the core functions is the ability to securely isolate processes and applications. Any process or application can run in parallel but strictly isolated environments so called "Compartments". A security relevant application – e.g. an online banking application – runs isolated from a common operating system. Any access by the operating system or any other compartment to data, which is stored in this compartment, is prevented. These way even compromised compartments cannot be used by an attacker to access the isolated data.

3.1 "Easy" integration of TNC into the Turaya security kernel

The potential to securely separate compartments with running applications of the Turaya security platform is also a great advantage for NAC. The applications that need to be measured and the TNC components can securely be isolated by the means of the security platform (Figure 1). A simultaneous compromising of the application as well as the TNC components is made a lot more difficult to

accomplish for a possible attacker. Faulty integrity measures of the applications are therefore prevented.

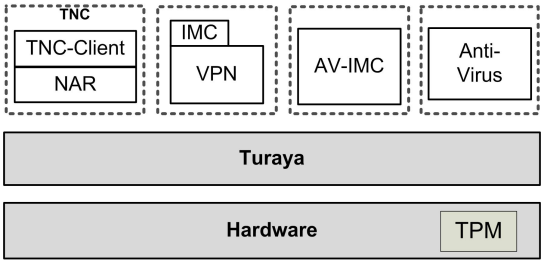

Figure 1: Integration von TNC in Turaya

However, new challenges evolve from the “easy integration”. As applications of the security kernel the TNC components have to rely on the integrity of the kernel itself. This cannot be determined securely by TNC, due to the fact that a possible compromise of the security kernel would cause the measurement values, collected by this kernel, not to be trustworthy. At this point a paradox is exchanged by another.

3.2 Use of Remote Attestation

As shown, an integration of NAC into Turaya the “easy way” cannot extend the trustworthiness to a full trusted level. A promising approach preventing a new paradox is the combination of TNC with another Trusted Computing concept – the Remote Attestation.

Like NAC concepts, the Remote Attestation allows integrity checks of remote computer systems to verify that the system is at a trustworthy state. If a computer system's configuration has changed, the attestation would fail allowing the communication partner to abort the network connection. There are three entities participating in a Remote Attestation. Besides the computer system, which state has to be checked, and the computer system, that demands the attestation, a presence of a Third Party (or Trusted Party) is required. The Third Party is a trustworthy entity, which performs the certification of a computer system’s state. Without the process of certification there is no possibility to perform a Remote Attestation, except to the so called Direct Anonymous Attestation (DAA). The DAA was introduced in the TPM-Specification 1.2 and allows an attestation which does not require a Third Party.

On the downside every change of the computer systems state – even caused by a new antivirus signature – results in a re-certification. This re-certification has to be executed in a trustworthy (and complex) process – e.g. by a trustworthy person. In case of a present antivirus scanner, which can be updated up to multiple times a day, this procedure is not practical. Therefore, it is more practical to exclude frequently changing applications from a Remote Attestation.

A combination of TNC/NAC and Remote Attestation should raise a trusted and manageable verification of computer systems to a higher level but avoids the identified limitations occurring by a non combined use. As a computer system's integrity has to be checked, the security platform and the TNC components are measured by Remote Attestation, while applications like a firewall or an antivirus application are tested by TNC. As long as the configuration of the security platform remains relatively static (stable) the number of re-certification are minimized. However, it is possible to check

compartments and applications with often changing configuration – for example caused by an antivirus application – by a trustworthy use of TNC (Figure 2).

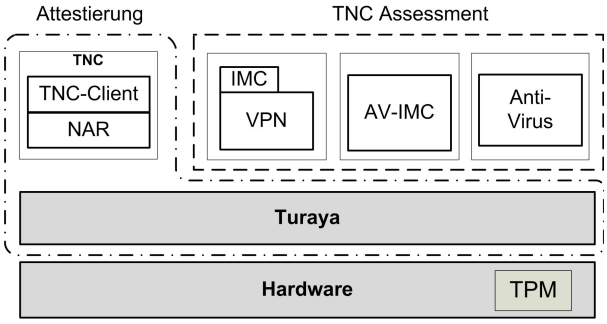

Figure 2: Combination of Attestation and TNC

4 Realisation: The tNAC Project

The tNAC (Trusted Network Access Control) project started in July of 2008. The main goal is the realisation of a complete Open Source NAC solution based on the TNC specifications including an integration of TNC into a security platform (Turaya) to achieve a higher level of trust.

The project is sponsored by the Federal Ministry of Education and Research. The consortium is consisting of the German Universities of Applied Sciences in Gelsenkirchen (Institute for Internet Security) and Hanover and a number of companies namely Datus AG, Sirrix AG and Steria Mummert Consulting. It combines two existing Trusted Computing Open Source projects – TNC@FHH, an Open Source TNC solution developed by the FH Hannover and the Turaya security platform, developed by the former EMSCB project in which the Institute for Internet Security was participating.

5 Conclusion

As a result of an increasingly stronger networking within and between companies over unsecured networks, an increase in the trustworthiness of network communication is essential. The NAC concept provides the opportunity to analyse end points with respect to their integrity, and therefore contributes to an increase in trustworthiness. Today's NAC solutions cannot provide the level of trust promised by the theoretical concept. This level can only be reached by the integration of NAC into a security platform, like Turaya, which is one of the main goals of the upcoming tNAC project. This integration is not trivial and has to be done in a trustworthy way. One possible solution is the combination of TNC and the Remote Attestation.

6 References

[Cisc04] Cisco Systems GmbH, Die Evolution des Self-Defending Network, 2004 http://www.cisco.com/global/AT/pdfs/prospekte/Securtiy_CNAC_032004.pdf

[Emsc07] EMSCB Project, www.emscb.de, www.internet-sicherheit.de

[Heis07] News: Ciscos Netzwerkzugangskontrolle NAC ausgetrickst – März 2007 http://www.heise.de/newsticker/meldung/mail/87663

[Jung07] M. Jungbauer: „Bewertung der Vertrauenswürdigkeit und Integrität entfernter Rechnersysteme“, Diploma Thesis, University of Applied Sciences Gelsenkirchen , 2007

[Micr08] Microsoft Corporation, Network Access Protection - Homepage 2008 http://www.microsoft.com/technet/network/nap/default.mspx

[Trus06] Trusted Computing Group: Trusted Network connect Subgroup, 2008 https://www.trustedcomputinggroup.org/groups/network

[Tru+06] Trusted Computing Group, TCG Trusted Network Connect TNC Architecture for Interoperability, 2008 https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_3_r6.pdf

[LiPo07] M. Linnemann, N. Pohlmann: “An Airbag for the Operating System – A Pipedream?”, ENISA Quarterly Vol. 3, No. 3, July-Sept 2007