

TPM-based Access Control for the Future Internet

Holger Kinkel, Heiko Niedermayer, Ralph Holz, and Georg Carle

Network Architectures and Services
Technische Universität München
e-mail: `lastname@net.in.tum.de`

May 9, 2010

1 Introduction

It is still an open question what the network of the future will look like. Although a plethora of proposals have already been submitted and discussed, there is no clear contender for the first prize. Some proposals even call for thousands of future networks in parallel. However, one of the issues that all future networks have to address is access control to the network. It is fair to say that the general consensus is that access must

- be easy, i. e. user-friendly
- possible from different geographic locations (roaming)
- possible with different devices (versatility)
- be controlled, i. e. only legitimate users can access the network

In this contribution, we discuss access control for a Future Internet. Controlling such access will become an ever greater issue in future as a multitude of devices will be connected to the Future Internet via different access technologies. We see a chance here to design new access control mechanisms for the network that, unlike today, fulfill all the requirements listed above.

2 The Home As The Center of Reference

A secure scheme for access control needs a point of reference that participants trust. We argue that a user's home network is a natural point of reference, with useful properties in the context of future networks.

Such a home network is more than the mere collection of connected devices that can be found in today's homes. In future, the home network will offer its users advanced services like the control of home appliances, act as a universal and secure storage and backup medium and provide services to share the data with others. A future home network will be at the center of a user's digital

universe. Such networks are, e. g., investigated in the AuthoNe project [1]. In the following, we show how we can move from today's password-based access to more advanced and versatile mechanisms for access control.

2.1 Username and Password

The simplest way to control access is to start with authentication on the basis of a username and a password. This is the predominant scheme today, but it comes with major drawbacks as passwords are usually weak and can be guessed or stolen. It is also cumbersome to remember them and store them on a variety of devices.

2.2 Provider Independence: Self-Certifying Identities and Homes

One can replace the password scheme with a solution that remains independent of Internet Server or Identity Providers. Homes and users may have self-certifying identifiers. This means that their identity is really their public key. It enables homes to act as an authority for users, their accounts, and their access rights. As identities are related to public keys, they cannot be memorized like passwords and need thus to be transported on the devices that a user carries. Roaming is more readily solved by establishing a connection and trust relation between two homes and checking the corresponding identities. To address a case that would commonly occur, we have developed an approach in previous work[2, 4], aimed at scenarios where two homes have no relation between them and access in the foreign network may at first be blocked for the user. Such a solution fits already better with the challenges we have identified above. Arguably, however, it may lack some user-friendliness.

2.3 Provider-Based Access: Home CAs with TPM

Another secure approach for an access control mechanism for a Future Internet can be based upon Trusted Computing Technology, namely the Trusted Platform Module (TPM) in combination with the automated distribution of identities. In previous work, we have designed and implemented a Certification Authority (CA) for home networks whose private signing key is safely stored inside the machine's TPM. The TPM acts as a hardware safeguard and guarantees the security of the home CA's private signing key. The usage of TPM technology effectively prevents the theft of a home CA's identity. We integrated the TPM-based CA with a service that semi-automatically issues valid certificates to devices within the home network [3]. Devices equipped with a certificate signed by the local Home CA later can access the home network using techniques like WPA2 and gain access to the Internet. This approach still lacks flexibility as it only allows for the authentication towards the access control mechanism of the own home network as certificates are only valid within the own home. For a solution that allows roaming between networks, certificates that can be validated outside the own home network are needed. For this purpose, we propose that the home network's ISP acts as an Identity Provider. Upon closure of the contract with the ISP, the home network obtains a valid certificate signed by the ISP's CA for the home's CA. Certificates issued by the home CA to own devices

can now 1) be attributed to a certain home network and 2) be attributed to a certain ISP. In case a device with a certificate signed by its own home network wants to connect to a foreign home network, a roaming service running in the foreign home network is able to identify the device and relate it to its own home network and ISP. The device now automatically obtains access to its own home network, as the roaming service dynamically creates a virtual private network from the foreign to the own home network. TPM technology on devices will provide extra security as device identities cannot be stolen. More advanced TPM based techniques like attestation can be used if device integrity must be guaranteed for accessing the network. The difference between this approach and the one above is two-fold: first, external entities are used to certify a home and second, a homes or device's identity is protected against theft.

3 Summary

In this paper, we have argued that home networks may play an important role for access control in Future Internets. We have described how one can turn a home into an anchor point for security to achieve the goals of user-friendliness, roaming, versatility and security.

References

- [1] Georg Carle, Holger Kinkelin, Andreas Müller, Heiko Niedermayer, Marc-Oliver Pahl, Alexander König, Thomas Luckenbach, Klaus Scholl, Mario Schuster, Lasse Thiem, Leo Petrak, Markus Steinmetz, Christoph Niedermeier, and Jürgen Reichmann. Autonomic Home Networks in the BMBF project AutHoNe. In *8th Würzburg Workshop on IP (EuroView 2008)*, July 2008.
- [2] Ralph Holz, Heiko Niedermayer, Peter Hauck, and Georg Carle. Trust-rated authentication for domain-structured distributed systems. In *Proc. 5th European PKI Workshop: Theory and Practice (EuroPKI 2008)*, Trondheim, Norway, 2008.
- [3] A. Müller, H. Kinkelin, S.K. Ghai, and G. Carle. An Assisted Device Registration and Service Access System for future Home Networks. IEEE IFIP Wireless Days 2009, Paris, December 2009.
- [4] Heiko Niedermayer, Ralph Holz, Marc-Oliver Pahl, and Georg Carle. On Using Home Networks and Cloud Computing for a Future Internet of Things. In *Proc. Future Internet Symposium 2009 (FIS 2009)*, Berlin, Germany, September 2009.