

TPM-based Access Control for the Future Internet

Future Internet Fachgespräch - June 09, 2010 - Stuttgart

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

`lastname@net.in.tum.de`

Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München
<http://www.net.in.tum.de>



- ❑ Motivation: Future Home Networks
- ❑ Candidates for Access Control Technologies
- ❑ The Trusted Platform Module as an ID Safeguard
- ❑ Conclusion
- ❑ Questions?



The Future Internet needs Access Control

- ❑ Nobody knows what the Future Internet will look like
 - ❑ Many proposals submitted
 - ❑ No contender for the first prize is in sight

- ❑ All proposals for the Future Internet have one thing in common:
They need network access control mechanisms

- ❑ Requirements:
 - ❑ Easy to use and user friendly
 - ❑ Possible from different geographic locations (“roaming”)
 - ❑ Possible from different devices (“versatility”)
 - ❑ Only legitimate users should be able to access the network (“safety”)

- ➔ We see a chance to design new access control mechanisms today



The Importance of Future Home Networks will grow

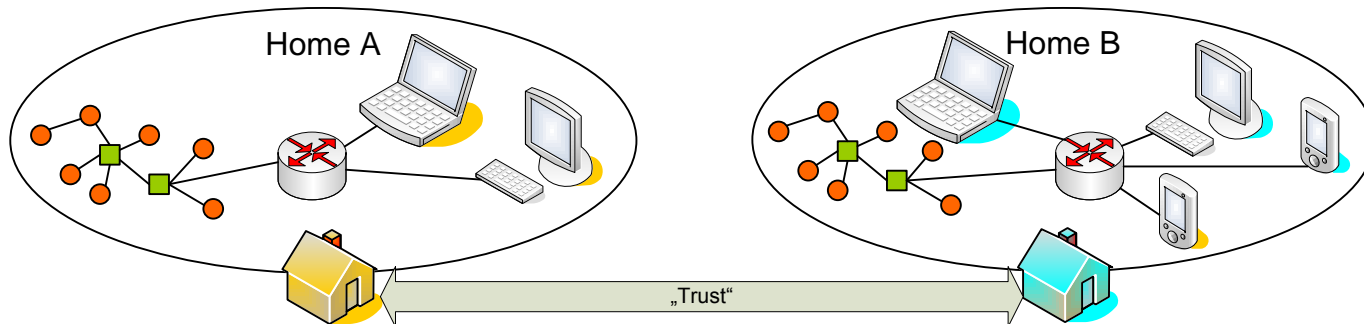
- The importance of Home Networks (HN) will grow in future!

- The AuthoNe Project researches Future HN
- One focus: access control and security for HN



- Possible use cases for a Future Home Network

- Control of home appliances
- Universal storage and backup medium for users' data
- Social networking-like features and interaction between HN



- ➔ Future Home Networks require access control mechanisms
- ➔ Idea: Use those Access Control Mechanisms for the FI, too



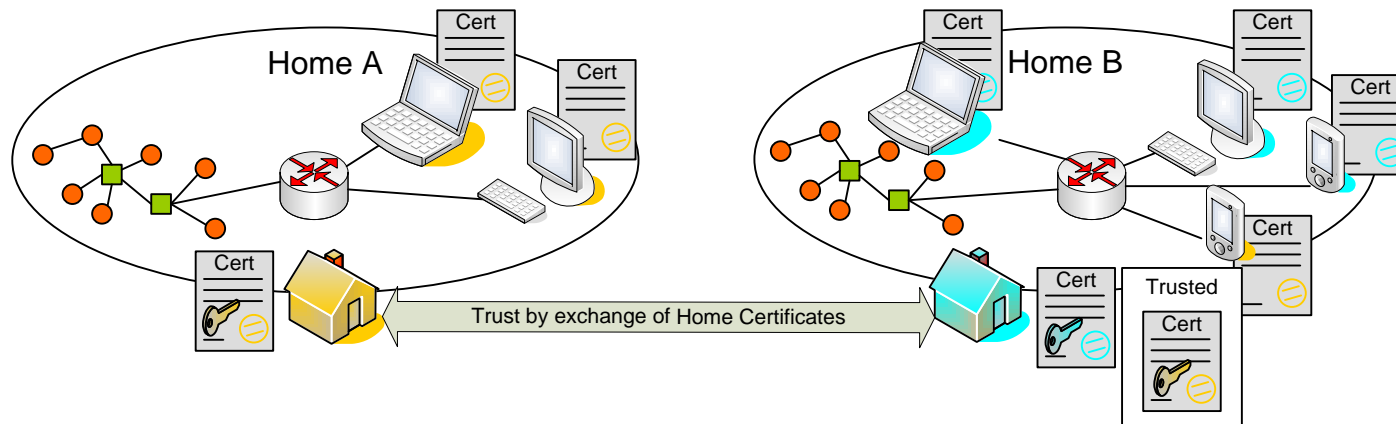
- ❑ Username and Password
 - ❑ Predominant scheme
 - ❑ Simple, actually nothing is required besides the user's memory
 - ❑ (Weak) passwords can be guessed and stolen
 - ❑ Passwords are cumbersome to manage
 - ➔ Not the best solution

- ❑ Access Control technologies rooted in a Future Home Network:
 - ❑ Self-certified Home CA (provider-independent)
 - ❑ Provider-certified Home CA (provider-dependent)



Self-Signed Home CA (Provider-Independent)

- ❑ Home Certification Authorities („Home CA“) have self-signed certificates
 - ❑ Home CA issues certificates to devices
 - ❑ Creation of keys, certificates and trust level settings can be automated
 - ❑ Exchange of Home Certificates between HN enables roaming



- ❑ User's device is needed to carry the keys and certificate:
Device ~ ID
 - ➔ Simple and decentralized scheme
 - ➔ Required exchange of Home Certs is maybe not user-friendly



Provider-certified Home CA (Provider-Dependent)

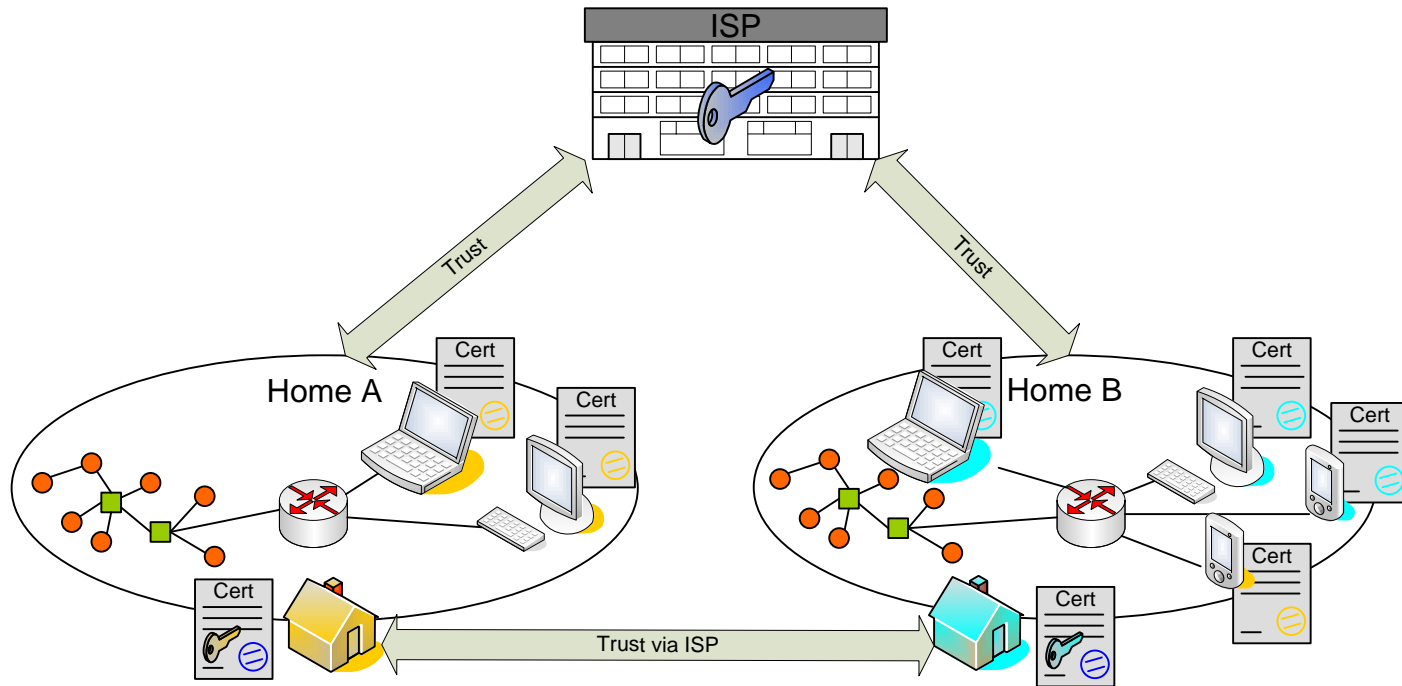
- ❑ Provider runs a Certification Authority for HNs and signs Home Certs
 - ❑ User certificates are signed by the Home CA
 - ❑ Users inside their own Home Network can be authenticated just like before

- ❑ Chain of trust established: ISP → HomeCA → Device
 - ❑ Users now can be authenticated when roaming is needed in foreign Home Networks

- ➔ User friendly, as no exchange of Home Certificates is required
- ➔ But less user control over security as TTP is needed:
ID is bound to ISP



Provider-certified Home CA (Provider-Dependent) II



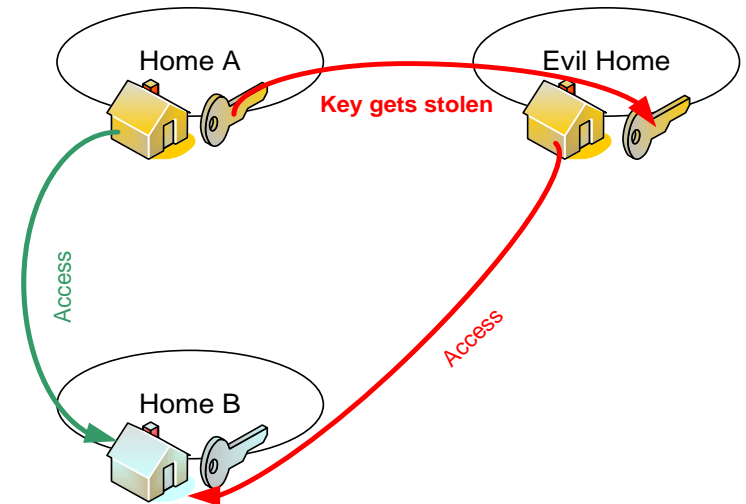


Security concerns – Identity Theft

- ❑ Private networks and devices are not highly secured
- ❑ Possible threat: private signing key of a Home CA or user gets stolen
 - ❑ Adversary is able to issue valid certificates to illegitimate users
 - ❑ Adversary is able to use valid certificate

➔ ID theft of Home Network or user

- ❑ Major question:
How to secure a private signing key?
- ❑ Approach:
Use a Trusted Platform Module (TPM)





The Trusted Platform Module as an ID Safeguard

- ❑ Standardized by Trusted Computing Group (Intel, Infineon, Lenovo...)
- ❑ TPM is a shielded cryptographic microcontroller
 - ❑ Integrated in computers' main boards
 - ❑ RSA keys can be generated and used inside the TPM
 - ❑ Private keys have properties like, e.g., non-migratability
 - ❑ Non-migratable keys cannot be extracted from the TPM
- ❑ Trusted Computing Technology provides...
 - ❑ mechanisms that prove properties of keys to other entities
 - ❑ mechanisms that prove properties of the system to other entities
- ➔ TPM can guarantee that a private key never is exposed, i.e. that the private key never leaves the Home CA or a user's device



Conclusion

- ❑ Whatever the Future Internet will look like – it will require easy to use, versatile and roaming-capable access control mechanisms

- ❑ Home Networks will gain importance in future
 - ❑ We need to solve the access control problem here, too
 - ❑ We can reuse those mechanism for the Future Internet

- ❑ Self-Certified Home CA
 - ❑ Provider-independent
 - ❑ Exchange of trusted IDs is required for roaming
 - ❑ Some limitations in user friendliness

- ❑ Provider-Certified Home CA
 - ❑ Provider-dependent
 - ❑ Roaming is easy

- ❑ The TPM increases security of keying material



Questions?

- Thank you for listening