

## Taking the Ubiquitous Administrator out of the Trust Chain

Alf Zugenmaier, Microsoft Research Cambridge, UK

Adolf Hohl, Institute for Social Studies and Computer Science, University Freiburg, Germany

**Abstract** – Ubiquitous computing can be thought of as consisting of two parts, firstly the devices that a user owns and may or may not carry around and secondly the devices that form a “ubiquitous infrastructure”, the smart environment. While the first part is usually considered to be under the administration of the user, the second part is not under his control. How can a user verify proper administration of the smart environment? One example where bad administration of the smart environment can not be recognized easily by the user is privacy. We examine the trust model for using smart environments for a hospital scenario and show how attestation techniques similar to the ones used in DRM can be introduced which may force device manufacturers to make their devices secure without relying on manual “hardening” by an administrator.

### Introduction

The project EMIKA [MuKrSt+2003] tries to enhance patient services in a hospital by making use of ubiquitous computing technology. Among other things, it provides public terminals, which patients can use to view their personal medical history which may be stored on their personal smartcard. Of course, this data is very sensitive and must be protected. To do this certain policies have to be defined and enforced. The policy that is used in this setting is very simple: The data has to be displayed correctly; and the terminal should not allow any data to leak, i.e. any trace of the information must be removed from the terminal after use. Of course, these policies may be much more complicated, as can be seen from the policies that are expressible by P3P [Ma2002].

The user has to have a certain level of trust that these policies are adhered to in order to be able to use the system. Similar to Beth et al [BeKlBo1994], we define trust in this paper to be the expectation that a certain attribute of a system is as desired, i.e. the policy adhered to.

For the moment we assume that the administrator of the terminal does not act maliciously. As the hospital terminal is a slimmed down version of a standard desktop workstation system, there are the same security threats (weak passwords, viruses, buffer overflows, etc). If the administrator configures the terminal correctly, the probability of loss of confidentiality of sensitive data is minimal.

### Today’s trust model

The trust relations which are necessary to trust the described system includes as actors: the manufacturer of the device, the administrator and at the top of the trust chain the user. Figure 1 demonstrates the trust relations. A bold arrow from A to B means A trusts B. A dashed arrow means that this trust is indirect. The administrator trusts the device to behave according to the policy and their manufacturers to produce these devices accordingly. The user trusts the administrator to select the right device, administer it correctly and load the policy onto the device. The user also takes the policy on a trust basis, even though it may be verifiable. Some of the trust relationships are indirect, i.e. the user’s trust in the device is mediated through trust in the administrator to choose device that the administrator chooses to trust.

### Introducing attestation techniques

There may potentially be as many administrators involved as there are devices in the environment. For the user it seems like an unnecessarily high burden to trust all these, and in addition trust all the policies set for these devices by the administrator. To reduce the number of entities the user has to trust in, a consumer protection organisation as well as an attestator is introduced. The consumer protection organisation is trusted by the user to define policies for certain devices and define which attestators are trustworthy with regard to their attestations.

The attestator doesn’t just trust the evaluated products, he has to verify them until he has the certainty that they behave as they claim.

### Trust model with attestation techniques

The introduction of a consumer protection organisation (CPO) and an attestator reduces the amount of direct trust relations of the user. The user has to trust that the CPO has selected a set of trusted attestators who had evaluated the devices of interest and that the CPO has properly verified the policies. During an interaction a user is confronted only with the consumer protection organisation's name as the root of trust. The policies are defined by the administrator and verified by the CPO or defined by the CPO and then chosen by the administrator to be appropriate for the task. A direct trust relation between the user and the administrator is no longer necessary, because the policy is verified by the CPO.

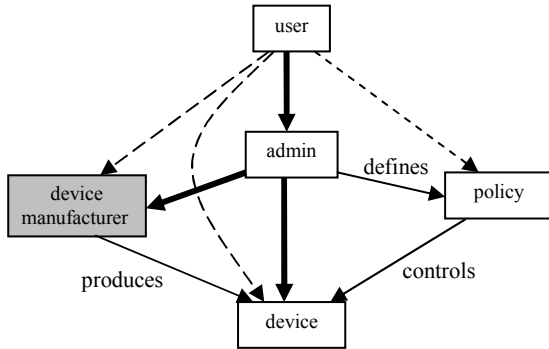


Figure 1: Today's trust model

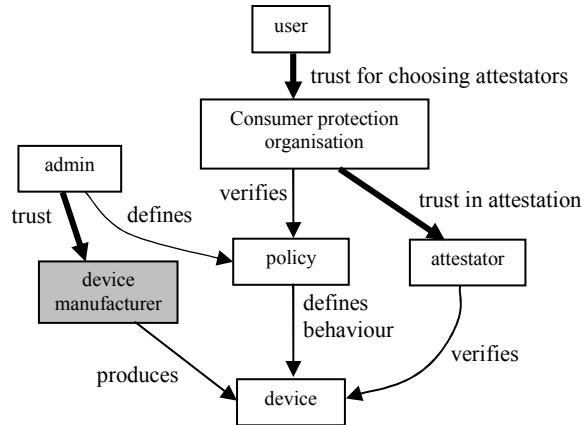


Figure 2: Trust model with attestation

### In the case of failure

We consider that a user is able to notice and has evidence that the used system has violated a given policy. In today's situation, a breach of trust will be noticed by only one or a few users. There is no mechanism by which other users are warned. In addition, when it comes to assigning the blame, the administrators will most likely try to blame the device manufacturer, who will return the accusations. However, with attestation, the administrator will be left out of the trust chain. The consumer protection organisation has the possibilities to revoke attestations and thus warn a large number of users at once.

### Conclusions

We are not the first to propose introducing DRM like techniques for privacy preservation. Similar approaches were proposed by Korba and Kenny [KoKe2002] and by Mont et al. [MoPeBr2003]. However, the underlying trust model has not been examined yet.

The user's trust in many, many administrators is replaced by trust in fewer customer protection organizations. Their sole task is to decide on which attestators to use and verify policies for use with different actions. Because there are only a few (larger) organizations, breach of their trust by attestators has more dire consequences. These attestators will push this responsibility to the device manufacturers, who then have a motivation to ensure the administrator cannot circumvent given policies. This would have the effect of creating an incentive for zero administration ubiquitous computing environments.

Of course there are a number of open issues, of which we only mention a few: Technically, there is still the question of how to support patch and version management in attestation. Organizationally, the question arises how to deal with a potentially vast number of single purpose policies. Socially, trust can not be prescribed by technical solutions. It has to develop over time. The success of branding shows that it is possible to build trust in a few brands, on the other hand, there are a significant number of failed attempts showing that trust building cannot be forced [EgMu2001].

## References

- [BeKIBo1994] T. Beth, M. Borchering, and B. Klein. Valuation of trust in open networks. In ESORICS 94. Brighton, UK, November 1994.
- [EgMu2001] Holger Eggs and Günter Müller. Sicherheit und Vertrauen: Mehrwert im E-Commerce. In: Sicherheitskonzepte für das Internet. Springer-Verlag Berlin, 2001.
- [KoKe2002] Korba, L., Kenny, S.: Towards Meeting the Privacy Challenge: Adapting DRM. ACM Workshop on Digital Rights Management, November 2002.
- [Ma2002] Massimo Marchiori (Ed.). The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Recommendation, 2002
- [MoPeBr2003] Mont, M., Pearson, S., Bramhall, P.: Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. Technical Report HPL-2003-49, 2003.
- [MuKrSt+2003] Müller, G., Kreutzer, M., Strasser, M., et al: Geduldige Technologie für ungeduldige Patienten, führt Ubiquitous Computing zu mehr Selbstbestimmung? In: Total vernetzt. Springer-Verlag Berlin, 2003.