Taking the Ubiquitous Administrator out of the Trust Chain

Adolf Hohl
University Freiburg, Germany
Alf Zugenmaier
Microsoft Research Cambridge, UK

Workshop UK Ubinet; 6 May 2004
Agenda

- Problem
- Trust Model
- Attestation
- Evaluation
- Conclusion
Problem Statement

smart environment

What happens to personal data? Adherence to policies? In presence of an attacker? A question of trust?
Trust – Definition

the expectation about an entity to behave as desired (in respect of one specific aspect)
Trust Model – Today

- Direct trust
- Indirect trust

user

admin

defines

device manufacturer

produces

device

controls

policy
Introducing Attestation

- attestator vouches for the device adhering to defined policy
- attestation certificate verified by personal device
- policies evaluated/stated by consumer protection organization
- specific policy chosen by user of personal device
Trust Model – with Attestation

- **user**
- **admin**
- **device manufacturer**
- **consumer protection organisation**
- **attestator**
- **device**

Relationships:
- **admin** defines **policy**
- **policy** controls **device**
- **device** produces **attestator**
- **attestator** evaluates **device**
- **user** interacts with **consumer protection organisation**
Evaluation – Trust Chain

- user
- admin
- device
- many
- few
- consumer protection organisation
- attestator
- device

Many-to-many connections are indicated with dotted lines.
Evaluation

- reduced number of policies
- translation of machine policies into human readable policies by trusted CPO
- attestator may be cut out of the loop if CPO is capable of verifying each technical implementation
- Are trust mechanisms sufficient to enforce correct behaviour of CPO and attestator?
- More issues: configuration management, patches, timeliness, services spanning multiple devices, unforeseen usage, …
Conclusion

• Ubicomp can provide “easy” ground for attestation – single purpose devices

• Trust building complex process – cannot be forced

• Attestation weaker than self protection