A Privacy-Centered System Model for Smart Connected Homes

Joseph Bugeja, Andreas Jacobsson and Paul Davidsson
Internet of Things and People Research Center, Department of Computer Science and Media Technology
Malmö University, Malmö, Sweden

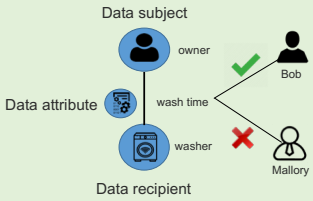
MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER
KK-stiftelsen

INTRODUCTION

- The home is the place where intimacy and reserve are expected.
- Internet-connected devices are resulting in potential for abuse, misuse, and appropriation of user data.
- This paper: **Proposes a model that can be used for the systematic identification and modeling of privacy threats affecting smart homes.**
- **Problems with existing works….**
  - **Narrow scope:** Challenging to apply to realistic use-cases.
  - **Model shortage:** Lack of a standard model that focuses on the home.
  - **Shallow analysis:** Privacy threats are identified without any formal basis.

BACKGROUND

- Privacy is defined as the appropriateness of information flows.*



- Leveraging the theory of Contextual Integrity* as an overarching framework.

* Nissenbaum, Helen. "Privacy as contextual integrity." *Wash. L. Rev.* 79 (2004): 119.

METHODS

- Blackbox modelling and abstract notation for describing the smart connected home.
- High-order logic and functions are created for the identification of privacy threats.
- The identification of threats is based on Ziegeldorf et al.+ work on information privacy.

+ Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges." *Security and Communication Networks* 7.12 (2014): 2728-2742.

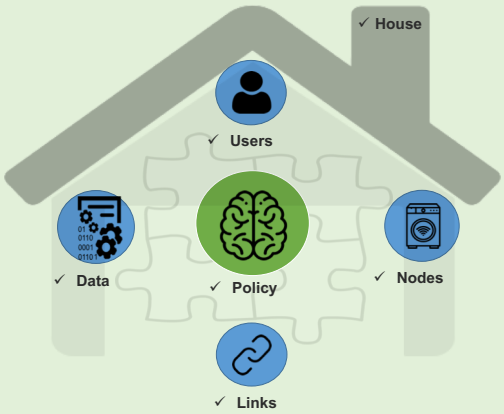
HOME AND PRIVACY THREATS

- The smart connected home is represented as a 6-tuple system:
  - *H*, House, is the physical building which the residents inhabit.
  - *N*, Nodes, is a set of physical components of the smart connected home space.
  - *U*, Users, is a set of human users interacting with the smart connected home.
  - *L*, Links, is a set of communication channels between the nodes and users.
  - *D*, Data, is a set of data being collected and processed by the smart connected home setup.
  - *P*, Policy, is a set of rules describing how data are transmitted between the different entities.
- For the privacy threats, we created 6 primitives and 7 logical formulas to support their identification, given a particular smart home configuration.

Primitives/ Formulas	$\Phi^{d_x}_{d_i}, \theta^{d_x}_{d_i}, \gamma^n, perms^u_{d_i}, read^l_{d_i}, write^l_{d_i}$
	$\stackrel{def}{=} \forall p \in P, \exists\ (dp_i <> \emptyset) \wedge (\Phi^{d_x}_{dp_i.d_i} = \texttt{true})$
	$\stackrel{def}{=} \exists\ (l \in L) \wedge (\Phi^{d_x}_{d_i} = \texttt{true}) \wedge write^l_{d_i}$
	$\stackrel{def}{=} \forall p \in P, \exists\ (dp_i <> \emptyset) \wedge (\theta^{d_x}_{dp_i.d_i} = \texttt{true})$
	$\stackrel{def}{=} \forall l_i, l_e \in L \wedge (l_i <> l_e) \wedge (read^l_{d_{i1}} \wedge read^l_{d_{i2}} \implies read^{l_e}_{d_{new}}) \wedge (read \notin perms^u_{d_{new}})$
	$\stackrel{def}{=} \exists\ (l \in L) \wedge (u \in U) \wedge read^l_{d_i} \wedge (read \notin perms^u_{d_i})$
	$\stackrel{def}{=} \exists\ (n \in N) \wedge (\gamma^n = \texttt{true})$
	$\stackrel{def}{=} \exists\ (l \in L) \wedge (u \in U) \wedge write^l_{d_i} \wedge (write \notin perms^u_{d_i})$

PRIVACY-CENTERED SYSTEM MODEL

- A graphical illustration of the proposed model alongside the privacy threats that it can identify.



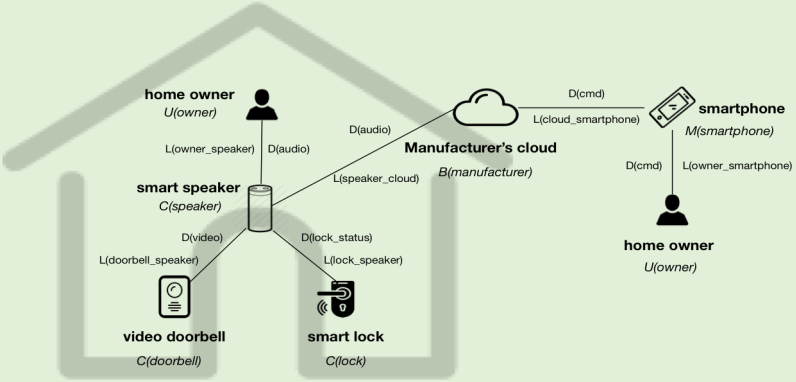
- ✓ Support for the automatic detection of privacy threats through logical formulas.
- ✓ Device and service agnostic.
- ✓ Model is scalable and extensible.

Threat does not exist | Threat is a potential future threat | Threat is present

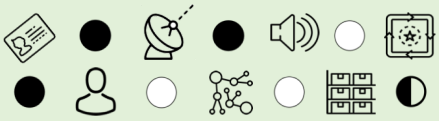
- Identification
- Profiling
- Localization and tracking
- Linkage
- Privacy-violating interaction and presentation
- Inventory attacks
- Lifecycle transitions

AMBIENT-ASSISTED LIVING USE-CASE

- An instantiation of the privacy-centered system model in a setup involving the home owner who can unlock a door using voice as input, and remotely through a smartphone.



- House, $H = \{house\}$
- Nodes, $N = \{doorbell, lock;\ speaker, manufacturer, smartphone\}$
  $C(speaker).capabilities = \{gateway, storage, processing, interaction\}$
  $B(manufacturer) = cloud$
- Users, $U = \{owner\}$
- Links, $L = \{doorbell\_speaker, lock\_speaker,\ speaker\_cloud,\ cloud\_smartphone,\ owner\_smartphone,\ owner\_speaker\}$
- Data, $D = \{(lock\_status,\ system,\ lock\ open/close,\ indefinite),\ (cmd, system, application\ command, purpose),\ (video, visitor, video\ of\ guest(s), purpose),\ (audio, owner, voice\ interaction, purpose)\}$
- Policy, $P =$ {(*doorbell_speaker*, {(*video*, {*read*})}, *doorbell, speaker*,∅),
  (*lock_speaker*, {(*lock_status*,{*read*})}, *lock, speaker*,∅),
  (*speaker_cloud*, {(*audio*, {*read*})}, *speaker, manufacturer,*
  Time = {8 :00 − 24:00} ∧ *Location* = {*house*}),
  (*cloud_smartphone*, {(*cmd*, {*read*})}, *smartphone, manufacturer*,∅),
  (*owner_smartphone*, {(*cmd*, {*read*})}, *owner, smartphone*,∅),
  (*owner_speaker*, {(*audio*, {*read*})}, *owner, speaker*,∅)}



CONCLUSIONS AND FUTURE WORK

- IoT technologies deployed inside the home challenge the long-held notion that the home is a private, protected, and intimate place.
- We contributed in adding more more transparency about risks emerging out of smart homes.
- Our privacy-centered system model helps in the identification and modelling of privacy threats.
- For future work:
  - Evaluate the completeness of the proposed model through empirical studies.
  - Express the system model using a formal specification language.
  - Leverage the model for performing quantitative risk analysis.

ACKNOWLEDGMENT

This work has been carried out within the research profile "Internet of Things and People," funded by the Knowledge Foundation and Malmö University in collaboration with 10 industrial partners.