A Privacy-Centered System Model for Smart Connected Homes

Authors: Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson

Presenter: Joseph Bugeja
How can we capture the properties and requirements for modeling privacy in smart connected homes?
The Privacy-Centered System Model

- The smart connected home system model
- Leveraging the theory of *Contextual Integrity*\(^*\) as a definition of privacy

\[\text{Data subject} \quad \text{owner} \]
\[\text{Data attribute} \quad \text{wash time} \]
\[\text{Data recipient} \quad \text{washer} \]

Privacy threat identification in action

- Privacy-centered model of the smart connected home

Policy, \( P = \)
\[ \{(\text{doorbell\_speaker}, \{(\text{video}, \{\text{read}\})\}), \text{doorbell, speaker}, 0\}, \]
\[ \{(\text{lock\_speaker}, \{(\text{lock\_status}, \{\text{read}\})\}), \text{lock, speaker}, 0\}, \]
\[ \{(\text{speaker\_cloud}, \{(\text{audio}, \{\text{read}\})\}), \text{speaker, manufacturer,} \]
\[ \text{Time} = \{8:00 \text{ } - \text{ } 24:00\} \land \text{Location} = \{\text{house}\}, \]
\[ \{(\text{cloud\_smartphone}, \{(\text{cmd}, \{\text{read}\})\}), \text{smartphone,} \]
\[ \text{manufacturer}, 0\}, \]
\[ \{(\text{owner\_smartphone}, \{(\text{cmd}, \{\text{read}\})\}), \text{owner, smartphone}, 0\}, \]
\[ \{(\text{owner\_speaker}, \{(\text{audio}, \{\text{read}\})\}), \text{owner, speaker}, 0\}\}

✓ Using high-order logic formulas to identify threats

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

Joseph Bugeja
NEXT STEPS

✓ Evaluate the **completeness** of the proposed model

✓ Express the system model using a **formal specification** language

✓ Leverage the model for performing **quantitative risk analysis**
Thank you for your attention!

joseph.bugeja@mau.se
bugejajoseph.com