Privacy-Preserving Access Control in IoT Scenarios through Incomplete Information

Dr. Savio Sciancalepore

Dr. Nicola Zannone

Presented by: Gelareh Hasel Mehri

April 2022

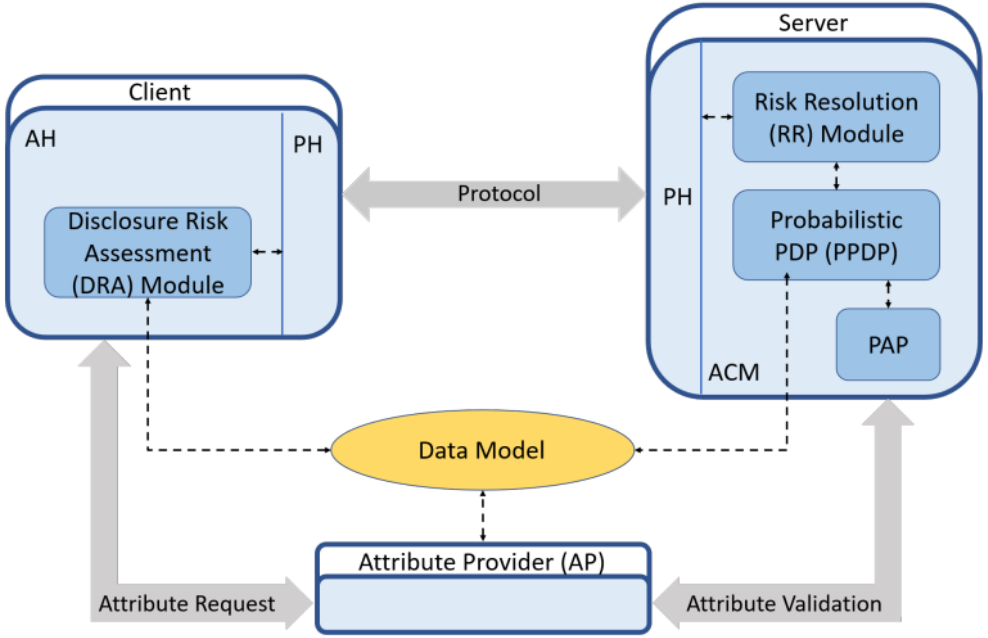
Problem Statement

- ❑ Fine-grained info are required for services and resources to be granted in IoT
- ❑ The user might have privacy preserving concerns regarding the granularity of sensitive information disclosure

PICO

- ❑ Provides an evaluation platform for users to assess its disclosure risk and to act based on privacy exchange and energy consumption tradeoff

- Attribute Provider (AP)
  - *Collects and certifies the client’s attribute values*
  - *Provides cryptography materials for server's attribute validation*
- Client
  - *Attribute Handler (AH)*
    - *Local storage and management of attributes*
    - *Decision Risk Assessment (DRA)*
  - *Protocol Handler (PH)*
    - *Supports interactions with the server*
- Server
  - *Access Control Manager (ACM)*
    - *Protection of sensitive resources and services*
    - *Probabilistic Policy Decision Point (PPDP)*
    - *Policy Administration Point (PAP)*
    - *Risk Resolution (RR)*
  - *Protocol Handler (PH)*
    - *Supports interactions with the server*
- Data Model
  - *Shared*
  - *Tree-based structure*
    - *Clients use it to determine the level of granularity*
    - *Servers use it for incorrect risk assessment*



PICO Architecture

Notation

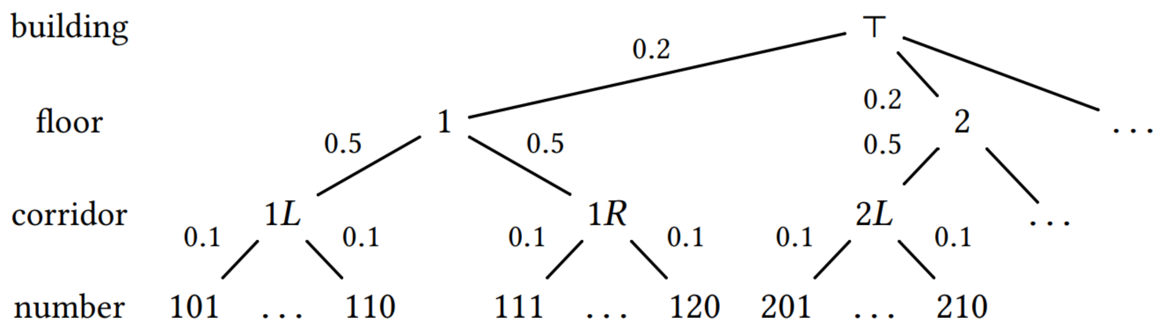
- $A = \{a_1, \dots, a_n\}$, a_i : attribute i
- V_{ai} : set of possible values for a_i
- $H_a = (N, S, \lambda)$: attribute hierarchy
- N : set of nodes
- $S \subseteq N \times N$: specialization relation on N
- (n_i, n_j) : path from i to j
- $\lambda : S \to [0,1]$: labeling function, shows closeness between two attribute values
- $(a, v_i) \subseteq (a, v_j)$: In attribute a, v_i is a specialization of v_j
- Specialization is:

  Reflexive

  Antisymmetric

  transitive

Hierarchy Tree



Degree of Similarity

- Base case: for adjacent n_i and n_j

$$\sigma(n_i, n_j) = \begin{cases} 1 & \text{if } n_i = n_j \\ 1 & \text{if } (n_i, n_j) \in S \\ \lambda(n_i, n_j) & \text{if } (n_j, n_i) \in S \end{cases}$$

Probability of inferring j when we know i

- Path: for a path from n_i to n_j

$$\sigma(n_i, n_j) = \prod_{k=1}^{m-1} \sigma(n_k, n_{k+1}) \qquad (\text{with } n_i = n_1 \text{ and } n_j = n_m)$$

Disclosure Risk Assessment (DRA) - Client Side

- Assesses the risk associated to the disclosure of attribute values and decides at which level of granularity information can be disclosed
- For an attribute value, the disclosure risk is the probability of inferring the most specialized value of a user

$$\delta_{H_a}(n') = \sigma(n', n)$$

n : exact attribute value

n' : generalization of n

i.e. (a , n) ⊂ (a , n')

- Attribute risk tolerance:
  - sensitive
  - non-sensitive

$$\delta_{H_a}(n) \geq \tau_a$$

$$\delta_{H_a}(v) < \tau_a$$

- All generalizations of a non-sensitive value are also non-sensitive
- Risk disclosure of a set of attribute values is equal to the highest disclosure risk.

$$\delta(V) = \max\{\delta_{H_{a_i}}(v_i) \mid v_i \in V\}$$

Probabilistic PDP – Server Side

- Represents the risks of incorrectly granting/denying access due to incomplete information
- Query : a set of attribute name-value pairs (a_i , v_i)
- Set of queries over A
- Using XACML policy language syntax
- t : policy targets
  1. Atomic : (a ,v)
  2. Composite : Boolean expression (¬, ∧, ∨) over atomic targets
- p : policy
  1. Atomic : singe decision, 1 or 0
  2. Target policy : (t , p)
  3. Composite : deny-override (△) or permit-override (▽) over {1 , 0, ⊥}
- Deny-override algorithm (△) : Deny decision has priority over a permit decision
- Permit-override algorithm (▽) : Permit decision has priority over a deny decision

$$q = \{(a_1, v_1), \ldots, (a_k, v_k)\}$$

$$Q_{\mathcal{A}} = \wp(\bigcup_{a_i \in \mathcal{A}} \bigcup_{v_j \in \mathcal{V}_{a_i}} (a_i, v_j))$$

Deny-override & Permit-override look-up tables

P_1	P_2	$P_1 \triangle P_2$
0	0	0
0	1	0
0	⊥	0
⊥	0	0
1	0	0
1	1	1
1	⊥	1
⊥	1	1
⊥	⊥	⊥

P_1	P_2	$P_1 \triangledown P_2$
1	1	1
1	0	1
1	⊥	1
⊥	1	1
0	1	1
0	0	0
0	⊥	0
⊥	0	0
⊥	⊥	⊥

Probabilistic PDP – Server Side

- Set of targets over A : T_A
- Set of policies over A : P_A

❑ Evaluation Function $[\![.]\!]_T$

- $T_A \times Q_A \rightarrow [0, 1]$
- $[\![t]\!]_T(q)$: likelihood that q matches t based on the degree of similarity between the attribute values in t & q

  1 : target certainly matches the query

  0 : target certainly doesn't match the query

❑ Valuation Function $[\![.]\!]_P$

- $P_A \times Q_A \rightarrow [0, 1]^3$
- $[\![p]\!]$ P(q) : likelihood that a certain decision is returned based on the degree of similarity between attributes
- $[\![p]\!]_P(q) = (\ell^1, \ell^0, \ell^\perp)$

  ℓ^1 : likelihood that the decision is permit

  ℓ^0 : likelihood that the decision is deny

  ℓ^1 : likelihood that the decision is NA

  $\ell^1 + \ell^0 + \ell^\perp = 1$

$$
\begin{array}{lcl}
[\![(a,v)]\!]_T(q) & = & \max\{\sigma(v_i, v) \mid (a, v_i) \in q\} \\
[\![\neg t]\!]_T(q) & = & 1 - [\![t]\!]_T(q) \\
[\![t_1 \vee t_2]\!]_T(q) & = & [\![t_1]\!]_T(q) + [\![t_2]\!]_T(q) - [\![t_1]\!]_T(q)[\![t_2]\!]_T(q) \\
[\![t_1 \wedge t_2]\!]_T(q) & = & [\![t_1]\!]_T(q)[\![t_2]\!]_T(q) \\
\hline
[\![1]\!]_P(q) & = & (1, 0, 0) \\
[\![0]\!]_P(q) & = & (0, 1, 0) \\
[\![(t, p)]\!]_P(q) & = & [\![t]\!]_T(q) \cdot [\![p]\!]_P(q) + (1 - [\![t]\!]_T(q)) \cdot (0, 0, 1) \\
[\![p_1 \triangledown p_2]\!]_P(q) & = & (\ell_1^1 + \ell_2^1 - \ell_1^1\ell_2^1, \ell_1^0\ell_2^0 + \ell_1^0\ell_2^\perp + \ell_1^\perp\ell_2^0, \ell_1^\perp\ell_2^\perp) \\
[\![p_1 \vartriangle p_2]\!]_P(q) & = & (\ell_1^1\ell_2^1 + \ell_1^1\ell_2^\perp + \ell_1^\perp\ell_2^1, \ell_1^0 + \ell_2^0 - \ell_1^0\ell_2^0, \ell_1^\perp\ell_2^\perp)
\end{array}
$$

Risk Resolution – Server side

- Responsible for policy enforcement, similar to the Policy Enforcement Point (PEP) in the XACML
- Decision needs to be made conclusively and not by likelihood
- The uncertainty in likelihood estimations needs to be quantified
- "Not-applicable" decisions need to be translated into either "permit" or "deny"
- Conservatively deciding, NAs are considered "deny"

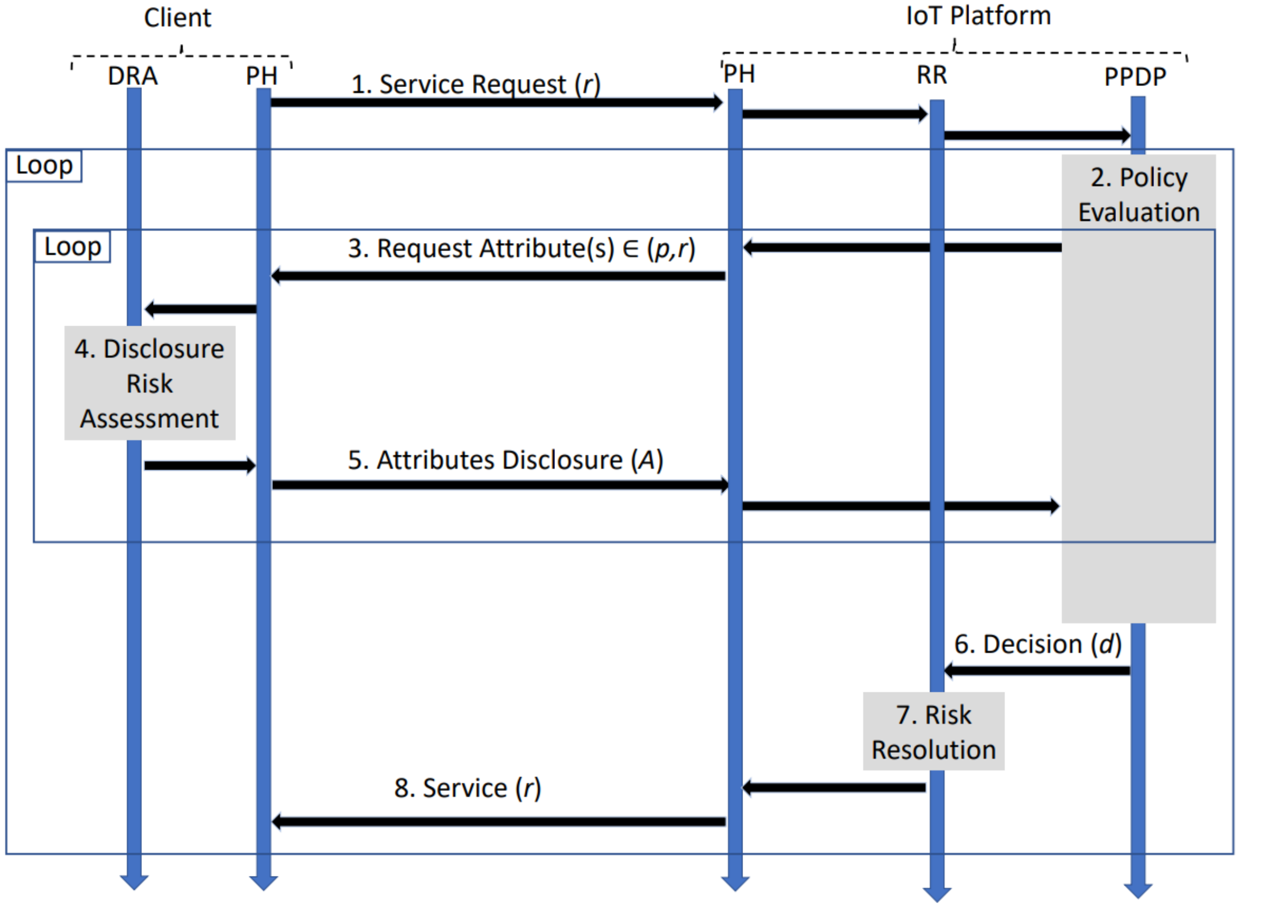
❑ Risk Tolerance

$$\ell^1 \geq \alpha\,(\ell^0 + \ell^\perp)$$

α : risk factor (showing criticality of resources)

$\alpha\,(\ell^0 + \ell^\perp)$: permission lower band

Protocol



- **Sequence diagram of the protocol used by the client to access services provided by the server IoT platform**

Notes

- **Client can decide to disclose her attributes in different levels of granularity.**
- **The protocol can be continued until:**
  - **The resource is granted**
  - **The client refuses to reveal more info**
- **Information disclosure increases the disclosure risk, and refusal to expose coarse-grained information is time and energy consuming**
- **A trade-off between disclosure risk and time/energy consumption is applied in client's behavior.**

Implementation

- ❑ Each disclosed attribute value is embedded into a CWT

❑ CWT

- CBOR Web Token
- A compact means of representing claims to be transferred between two parties
- Optimized for IoT use-cases
- Consisting of 3 parts:
  1. Header (for correct decoding)
  2. Claims (standardized or private)
  3. Signature (for integrity and authenticity verification)

❑ Claims

- A piece of information asserted about a subject
- represented as a name/value pair consisting of a Claim Name and a Claim Value
- Claims in a CWT are encoded using CBOR

- Standardized claims are used for the: *issuer (iss), unique identifier (cti), subject (sub), and expiration date (exp)*
- Ad-hoc private claim is used for *attribute values* (*atv*)
- HMAC-SHA-256 is used to generate CWT signature
- A single CWT is 233 bytes

❑ Delivering CWT over IoT wireless networks

  - CoAP message (adding 4 bytes header)
  - UDP (adding 8 bytes header)
  - 6LoWPAN (adding 40 bytes header)
  - IEEE 802.15.4 (21 bytes header and 4 bytes trailer)
  - Sum: 76 bytes
- MTU of IEEE 802.15.4 is 127 bytes
- Available payload for application-layer information: 50 bytes
- Number of MAC-layer messages needed to deliver a single CWT: five IEEE 802.15.4 messages

❑ Energy Consumption Estimations

  - Openmote-b IoT device, same protocol stack, same MAC-layer message
  - 802.65 mJ for a transmission slot
  - 778.51 mJ for a reception slot

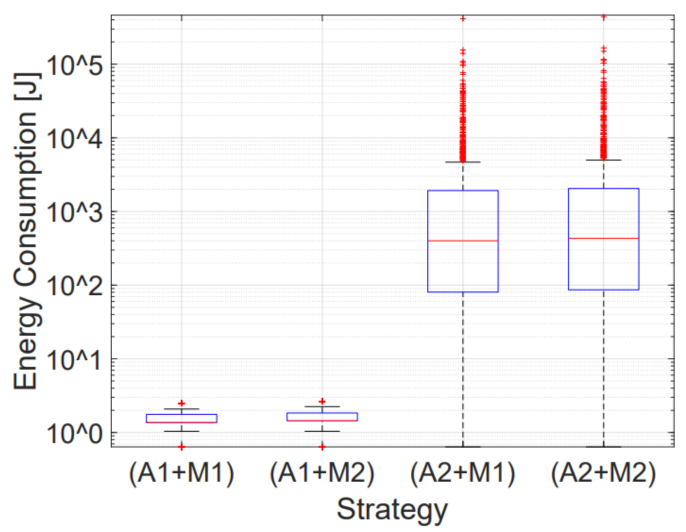
Experiment

- **Attribute disclosure approaches:**
  1. Direct disclosure of non-sensitive attribute values with the highest disclosure risk (*A1*)
  2. Incremental disclosure of non-sensitive attribute values, from low risk to high (*A2*)
- **Attribute delivery modes:**
  1. All CWTs delivered together in a single stream (*M1*)
  2. CWTs delivered one-by-one in different streams (*M2*)
- **Operational strategies:**

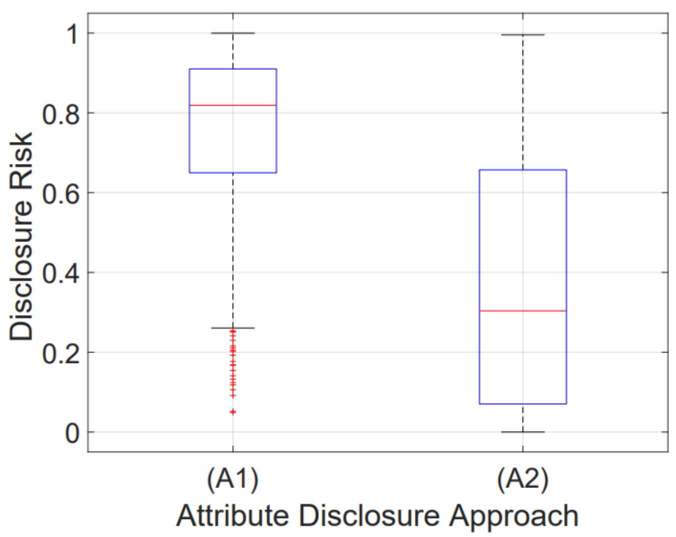
  (A1+M1), (A1+M2), (A2+M1), (A2+M2)

❑ **Considerations:**

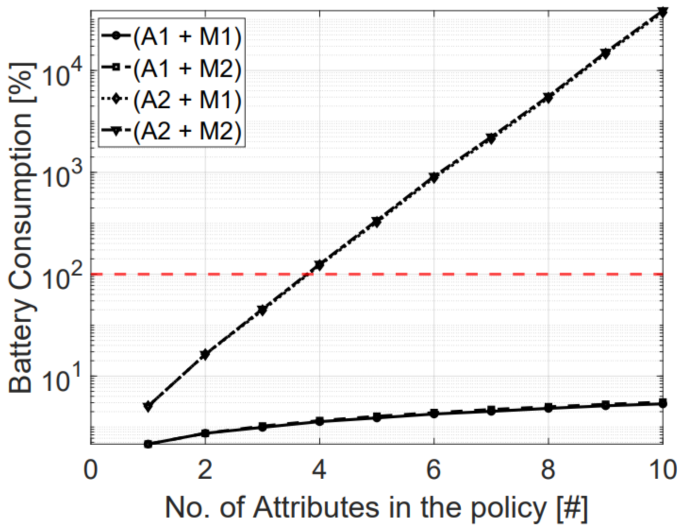
- Number of attributes: 6 (fixed in first experiment, ranging from 1 to 10 in second experiment)
- Attribute hierarchies: Static, Height-balanced binary trees, predefined depth (9, 10, or 11)
- Random semantic closeness values (siblings' semantic closeness values with the parent node sum up to 1)
- Random policies on the server side : Random combination of attributes (from 1 to 6) + Random risk factor



Energy Consumption [J]
10^0
10^1
10^2
10^3
10^4
10^5
(A1+M1)
(A1+M2)
(A2+M1)
(A2+M2)
Strategy



Disclosure Risk
0
0.2
0.4
0.6
0.8
1
(A1)
(A2)
Attribute Disclosure Approach



Battery Consumption [%]
10^1
10^2
10^3
10^4
(A1 + M1)
(A1 + M2)
(A2 + M1)
(A2 + M2)
0
2
4
6
8
10
No. of Attributes in the policy [#]

Results

Ref:

Sciancalepore, Savio & Zannone, Nicola. (2022). PICO: Privacy-Preserving Access Control in IoT Scenarios through Incomplete Information. 10.1145/3477314.3508379.