

Andreas Put and Bart De Decker

imec-DistriNet, KU Leuven

andreas.put@kuleuven.be

bart.dedecker@kuleuven.be

IoTSEAR: a System for Enforcing Access control Rules with the IoT

About

Andreas Put is a postdoctoral researcher in the imec-DistriNet research group at KU Leuven. During his PhD, his research focused on privacy-enhancing technologies, anonymous authentication, and e-Voting. However, his research in recent years centers around enhancing security and privacy specifically in IoT environments.



Outline

- › Introduction
- › Context Model
- › IoTSEAR
- › Conclusion

Introduction

Introduction

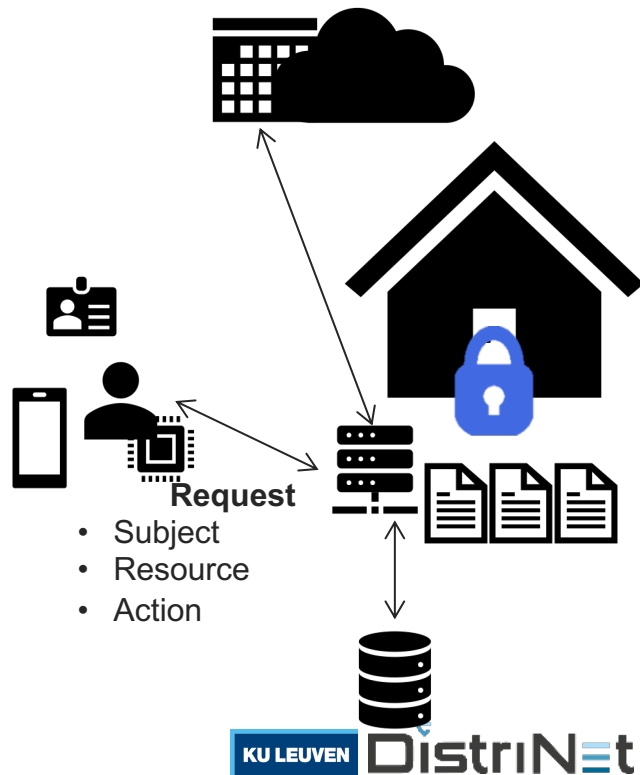
Context-aware access control

› Context types

- ›› System state
- ›› IoT Device context
- ›› 3rd party/Cloud service
 - ››› Incl. federated identity management

› Context security requirements!

- ›› Integrity, authenticity, ownership



Introduction

IoTSEAR scope

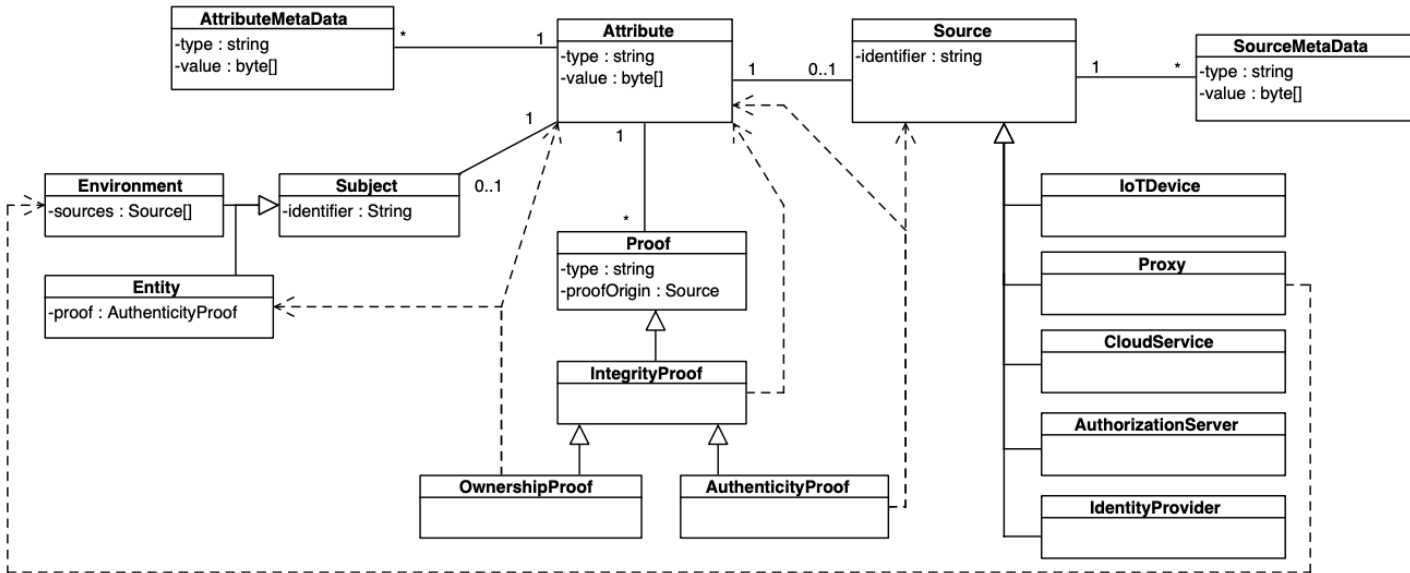
- › How to specify context security requirements?
 - **Generic model for context**
- › How to specify context aware access permissions?
 - **policy language [1]**
- › How to enforce access permissions & security requirements?
 - **IoTSEAR middleware**

[1] A. Put and B. De Decker, “Attribute-based privacy-friendly access control with context,” in International Conference on E-Business and Telecommunications. Springer, 2016, pp. 291–315

Context Model

Context Model

Overview



Context Model

Attribute & Proof

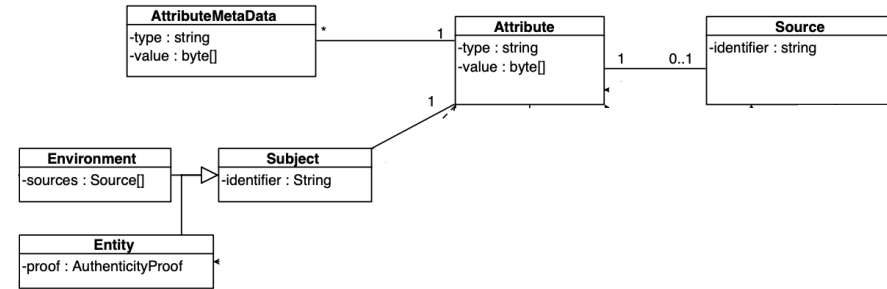
› Attribute:

- › Raw data
sensor output, identity/authorization token, ...
- › Metadata: timestamp, encoding, ...
- › Source
- › Subject

› Proof:

Universally verifiable object

- › IntegrityProof & AuthenticityProof
Verify attribute Integrity & source authenticity
- › OwnershipProof
Verify link between Subject & Attribute



Instances of the context model

Applied to a sensor reading

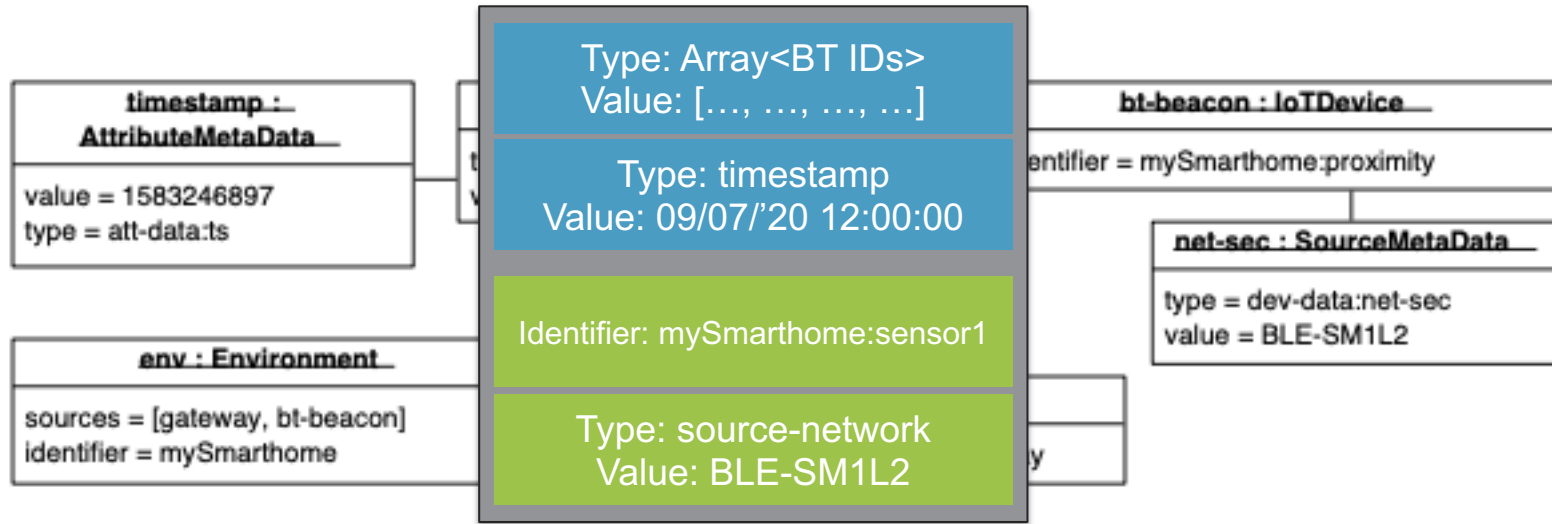
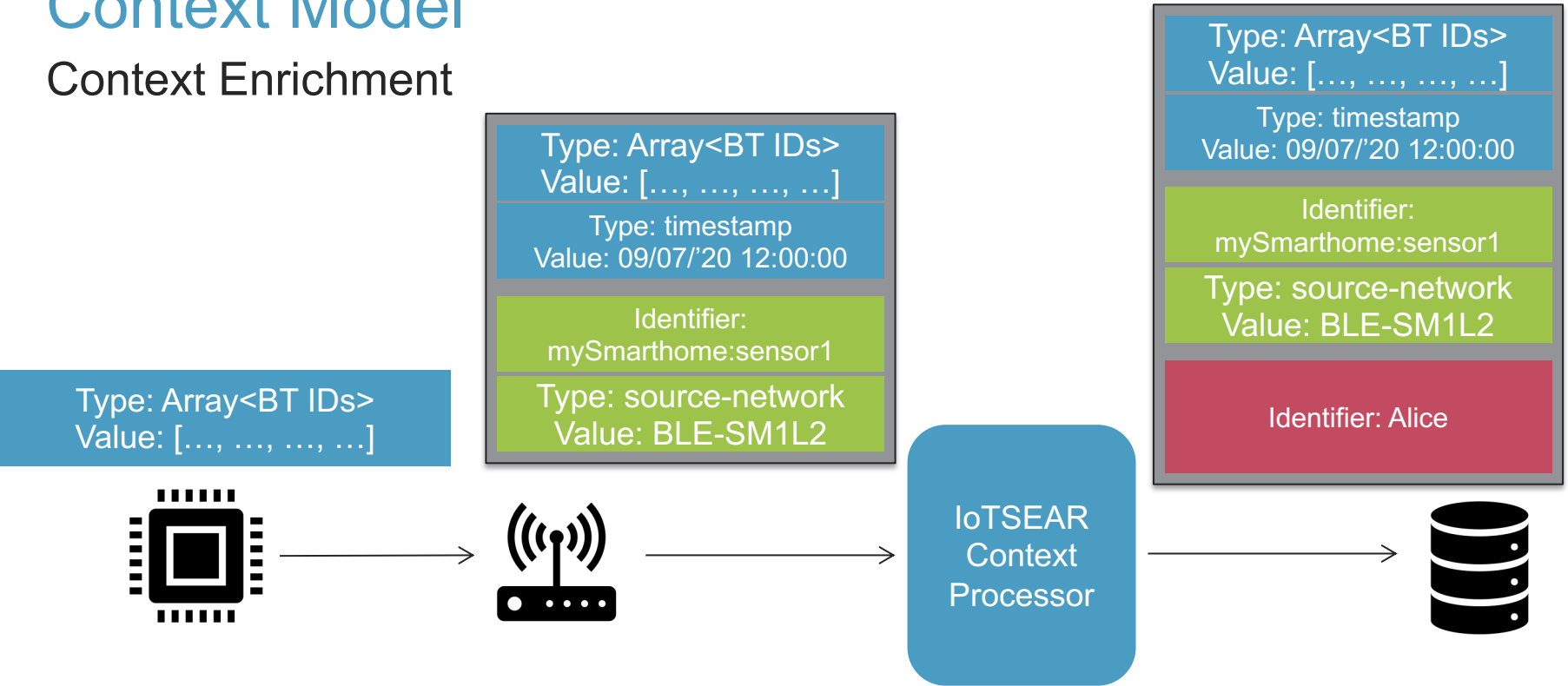


Figure 2. The context model applied to a proximity sensor reading

IoTSEAR

Context Model

Context Enrichment



Context Model

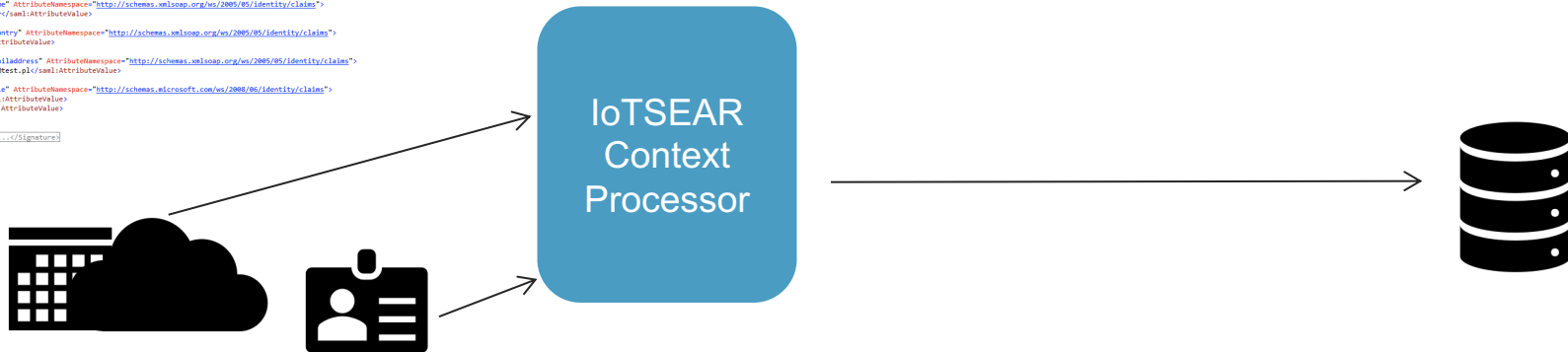
Context Enrichment

Type: samlAttribute:role Value: caretaker	Type: not-after Value: 09/07/'20 18:00:00
Type: timestamp Value: 09/07/'20 12:00:00	Type: authnContext Value: NFCBadge
Identifier: healthcare-IDP	proof: saml-signature Identifier: Alice
	Type: xmldsig#rsa-sha1 ProofOrigin: healthcare-IDP

```

1 <?xml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="f814e3d-5f65-4368-ae6c-029d6d94f23"
2 Issuer="ActAsSits" IssueInstant="2015-02-22T16:03:09.968Z" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
3 <saml:Conditions NotBefore="2015-02-22T16:03:09.955Z" NotOnOrAfter="2015-02-22T16:33:09.955Z">
4   <saml:AudienceRestrictionCondition>
5     <saml:AudienceRestrictionCondition>
6       <saml:AudienceRestrictionCondition>
7         <saml:AudienceRestrictionCondition>
8         </saml:AudienceRestrictionCondition>
9       </saml:AudienceRestrictionCondition>
10      </saml:AudienceRestrictionCondition>
11     </saml:AudienceRestrictionCondition>
12   </saml:AudienceRestrictionCondition>
13   <saml:SubjectConfirmation>
14     <saml:SubjectConfirmation>
15       <saml:SubjectConfirmation>
16       </saml:SubjectConfirmation>
17     </saml:SubjectConfirmation>
18   </saml:SubjectConfirmation>
19   <saml:AttributeStatement>
20     <saml:AttributeStatement>
21       <saml:AttributeStatement>
22       </saml:AttributeStatement>
23     </saml:AttributeStatement>
24   </saml:AttributeStatement>
25   <saml:AttributeStatement>
26     <saml:AttributeStatement>
27       <saml:AttributeStatement>
28       </saml:AttributeStatement>
29     </saml:AttributeStatement>
30   </saml:AttributeStatement>
31 </saml:Conditions>
32 </saml:Assertion>

```



IoTSEAR

Policy representation

- Su
- Re
- Ac

```
{
  "identifier": "smartlock-actuate-normal",
  "priority": 1,
  "target": {
    "subject": "AnySubject",
    "resource": "smartlock-1",
    "action": "actuate"
  },
  "effect": "allow",
  "condition": {
    "darc:condition:and": [
      {
        "source": "presence",
        "operation": "darc:condition:operation>equals",
        "value": "1",
        "verifiers": [
          "darc:condition:verifier:freshness:15s"
        ]
      },
      {
        "source": "identity",
        "operation": "demo:operations:is-scheduled",
        "value": "./calendar.json",
        "verifiers": [
          "darc:condition:verifier:freshness:15s",
          "demo:condition:security:trusted-device"
        ]
      }
    ]
  }
}
```

Effect
/Notify/...

Priority

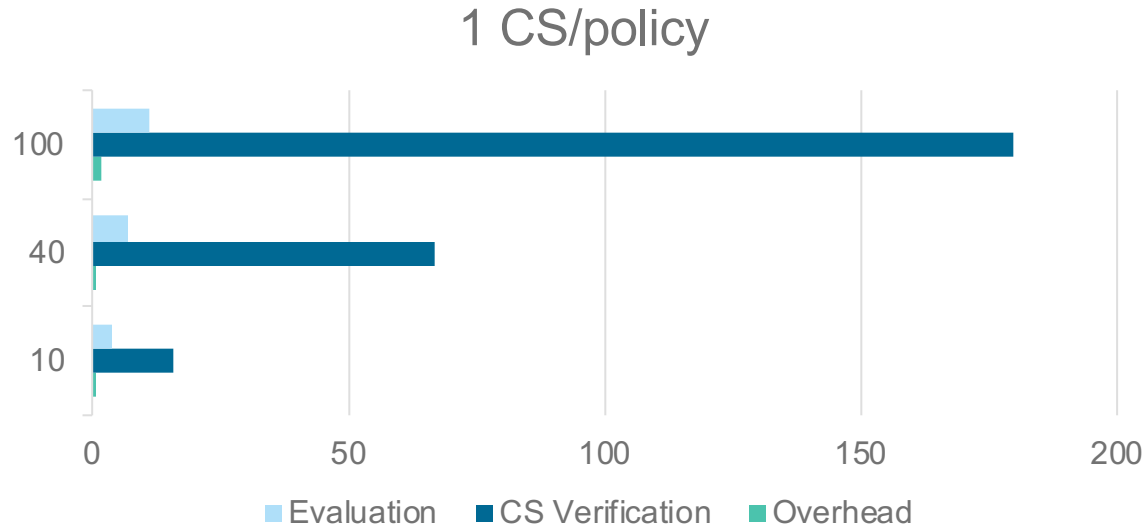
Value

IoTSEAR

Context verifiers

- › Middleware component
 - › Selected through identifiers in policy
 - › Used to filter useable context objects
 - ›› Input: Context object
 - ›› Output: Boolean
- › E.g. Freshness, known-devices, basic/substantial/high, ...
 - › Often application dependent

IoTSEAR performance



Conclusion

Conclusion

- › Generic model for context
 - › Allows (third parties) to verify custom security requirements
- › IoTSEAR middleware
 - › Policy enforcement & context management
 - › Application specific security requirements
 - › Acceptable performance overhead

DistriNet

Thank you!

andreas.put@kuleuven.be

bart.dedecker@kuleuven.be