Semantic security framework and context-aware role-based access control ontology for Smart Spaces

Semantic Big Data Workshop, ACM SIGMOD 2016 Conference 2016,
San Francisco, California, July 1st 2016

Shohreh Hosseinzadeh, **Natalia Díaz-Rodríguez**, Seppo Virtanen, Johan Lilius

University of Turku, Finland
Åbo Akademi University, Finland

Turun yliopisto
University of Turku

Introduction

- Smart Spaces
- Security, Privacy and Context Awareness in Smart Spaces

Contribution

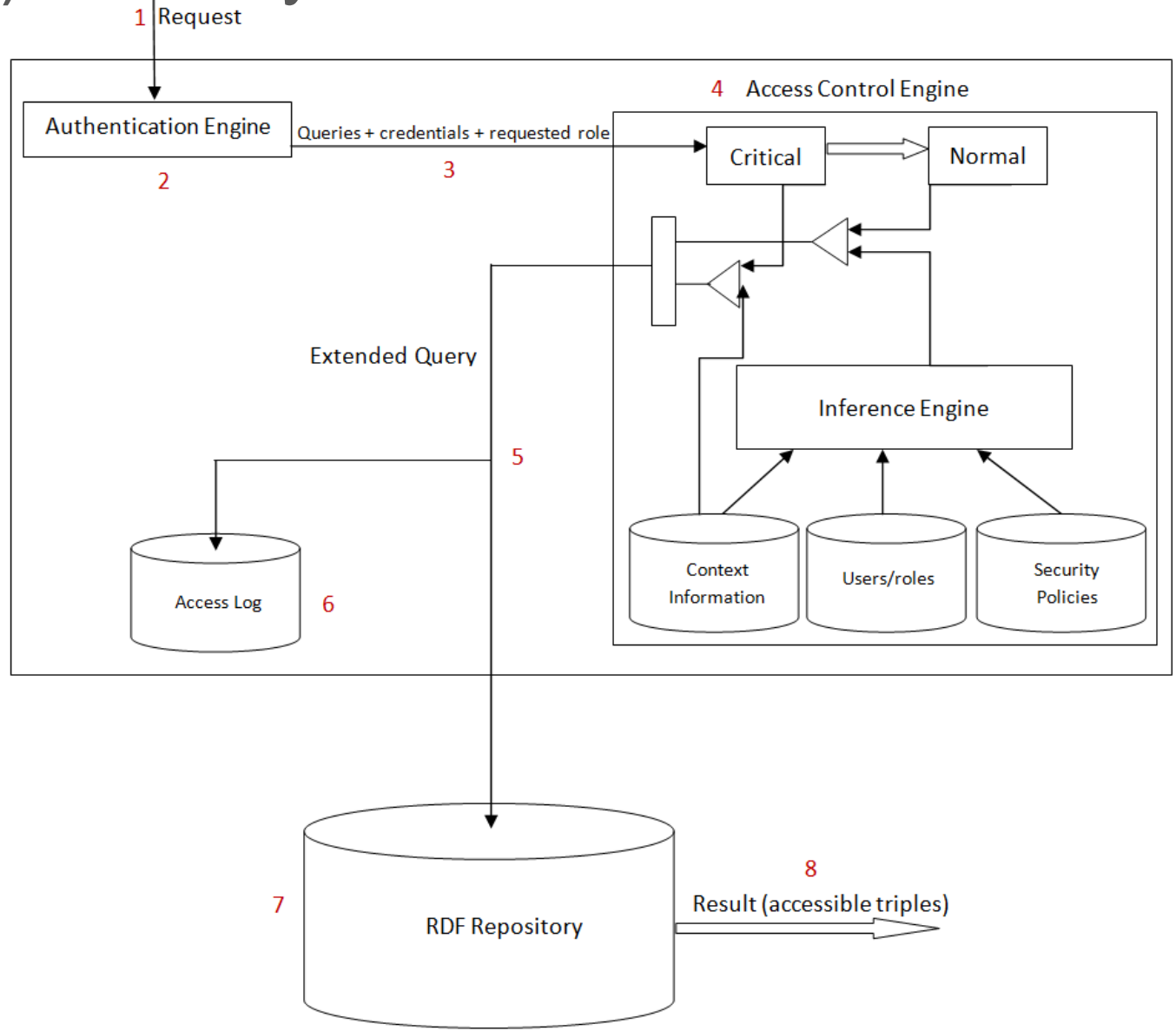
Granular triple-level mechanisms for security and privacy in Smart Spaces

1. Security framework for Smart-M3 platform [13]
2. Context-aware role-based access control scheme

Smart-M3

- Smart-M3 is a functional platform that provides a cross domain search extent for triple based information. Smart-M3 enables smart cross domain applications that rely on information level interoperability.
- Multi Device, Multi Platform, Multi Part
- https://sourceforge.net/projects/smart-m3/

1) Security framework architecture

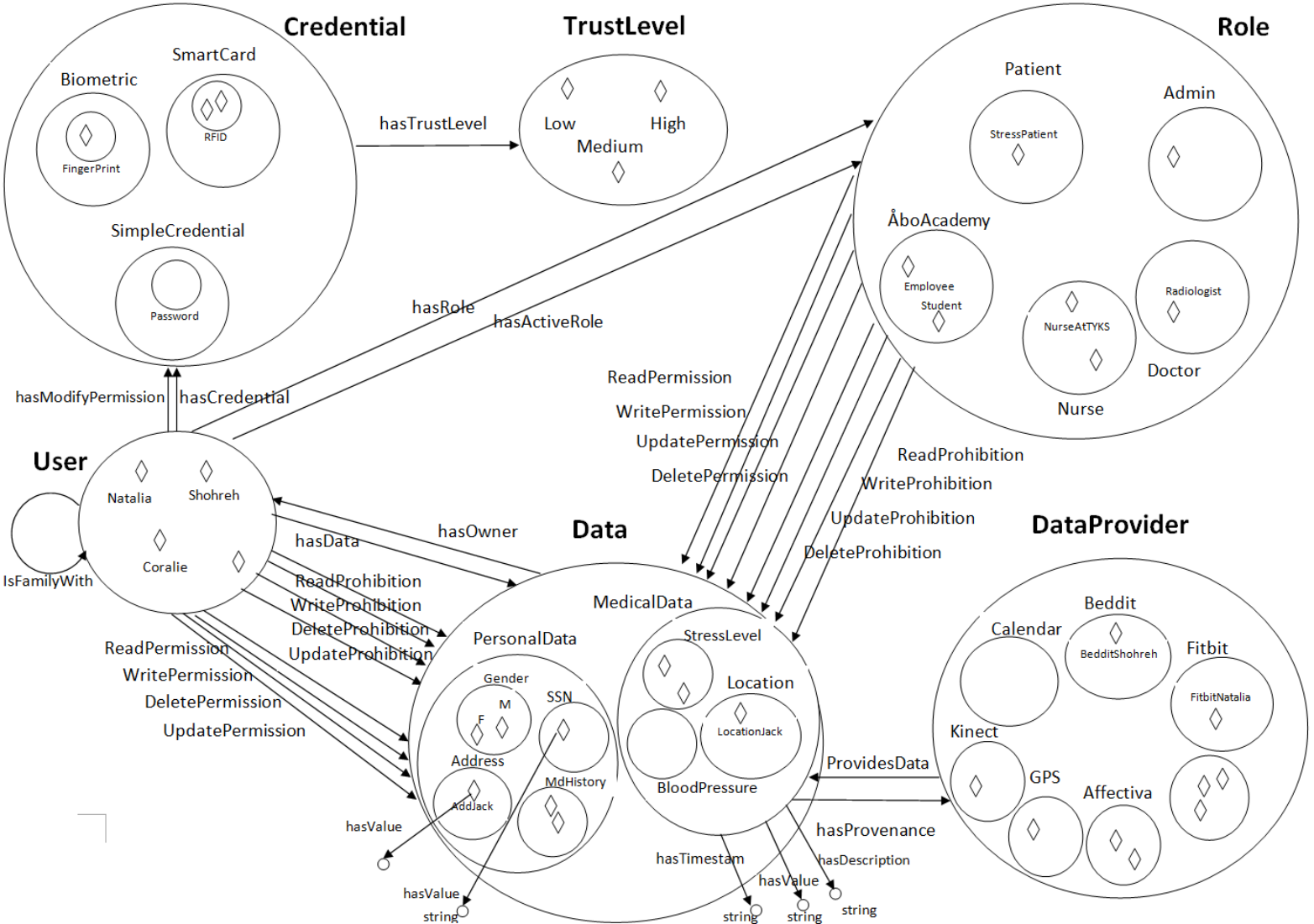


Security aspects supported:
Authentication, Authorization and Access control

Different steps:

(1) Access request from user
(2) Authentication engine assures authenticity
(3) If positive, request forwarded to Access Control Engine
(4) Execute access control rules: check if requester has rights to perform the requested action
(5) If positive the request is forwarded to the repository and access log
(6) The access log keeps record of the recent accesses.
(7) The result (accessible triple) is retrieved from the repository
(8) The result is sent to the user

2) Context Aware Role Based Access Control (CARBAC) ontology



Turun yliopisto
University of Turku

Comparison of access control ontologies and their Smart Space domains

Reference & Access control model	Context aware	Rule-based	Domain	Privacy control	Triple level control
[22] Context-based	✓	✓	Pervasive Computing Environments	×	×
[14] Privacy-centric	×	✓	Heterogeneous administrative medical domains	✓	✓
[7] CoBrA, No access control ontologies	✓	✓	Context-aware systems and SS	✓	×
OWL-S Services[1] Ontology-based	×	✓	Semantic Web services	✓	×
[20] OPO Access Control List (ACL)	×	✓	Linked Data	✓	✓
[16] User Behavior and Capability Based Control Access	✓	✓	Smart Spaces	✓	×
[4] Credential-based	✓	✓	XACML and SAML-based systems	✓	×
[19] SitBAC	✓	✓	Smart Spaces	✓	×
[23] Proteus, Context-centric	✓	✓	Pervasive Environments	×	×
[10] ROWLBACK	×	✓	Dynamic Environments	×	×
This work: CARBAC	✓	✓	Health and well-being SS	✓	✓

Turun yliopisto
University of Turku

Access Control Policies

- Expressed via rules
- At run-time, rules are executed, and decisions made on permission/prohibition of performing an action.
- For writing the access control rules, we used C Language Integrated Production System (CLIPS) v6.24
- 2 kinds of Access Control rules, defined by:
    a) Admin
    b) User for privacy protection purposes.

Example 1: Rules defined by the admin

(triple (Jack, *hasRole*, Doctor))

(triple (Maria, *hasRole*, Patient))

(triple (Maria, *hasMedicalHistory*, ?h)))

➔

(assert (triple (Jack, *roleHasReadPermissionOverData*, ?h)))

(assert (triple (Jack, *roleHasWritePermissionOverData*, ?h)))

(assert (triple (Jack, *roleHasUpdatePermissionOverData*, ?h)))

(assert (triple (Jack, *roleHasDeletePermissionOverData*, ?h)))

Turun yliopisto
University of Turku

Example 2: Rules defined by the user (highest priority)

(assert (triple (Jack, *userHasReadPermissionOverData*, ?h)))

(assert (triple (Jack, *userHasUpdatePermissioOverData*, ?h)))

(assert (triple (Jack, *userHasDeletePermissionOverData*, ?h)))

(assert (triple (Jack, *userHasWritePermissionOverData*, ?h)))

(assert (triple (Jack, *userHasUpdateProhibitionOverData*, ?h)))

(assert (triple (Jack, *userHasDeleteProhibitionOverData*, ?h)))

(assert (triple (Jack, *userHasWriteProhibitionOverData*, ?h)))

➔

(assert (triple (Jack, *roleHasReadPermissionOverData*, ?h)))

Turun yliopisto
University of Turku

Example 3:
Context aware access control rules

Doctor: restricted to only read the medical history of the patients outside the hospital, but cannot update/delete/write:

(triple (Jack, *hasRole*, Doctor))

(triple (Maria, *hasRole*, Patient))

(triple (Maria, *hasMedicalHistory*, ?h)))

(triple (LocationJack, *hasValue*, TrainStation))

➔

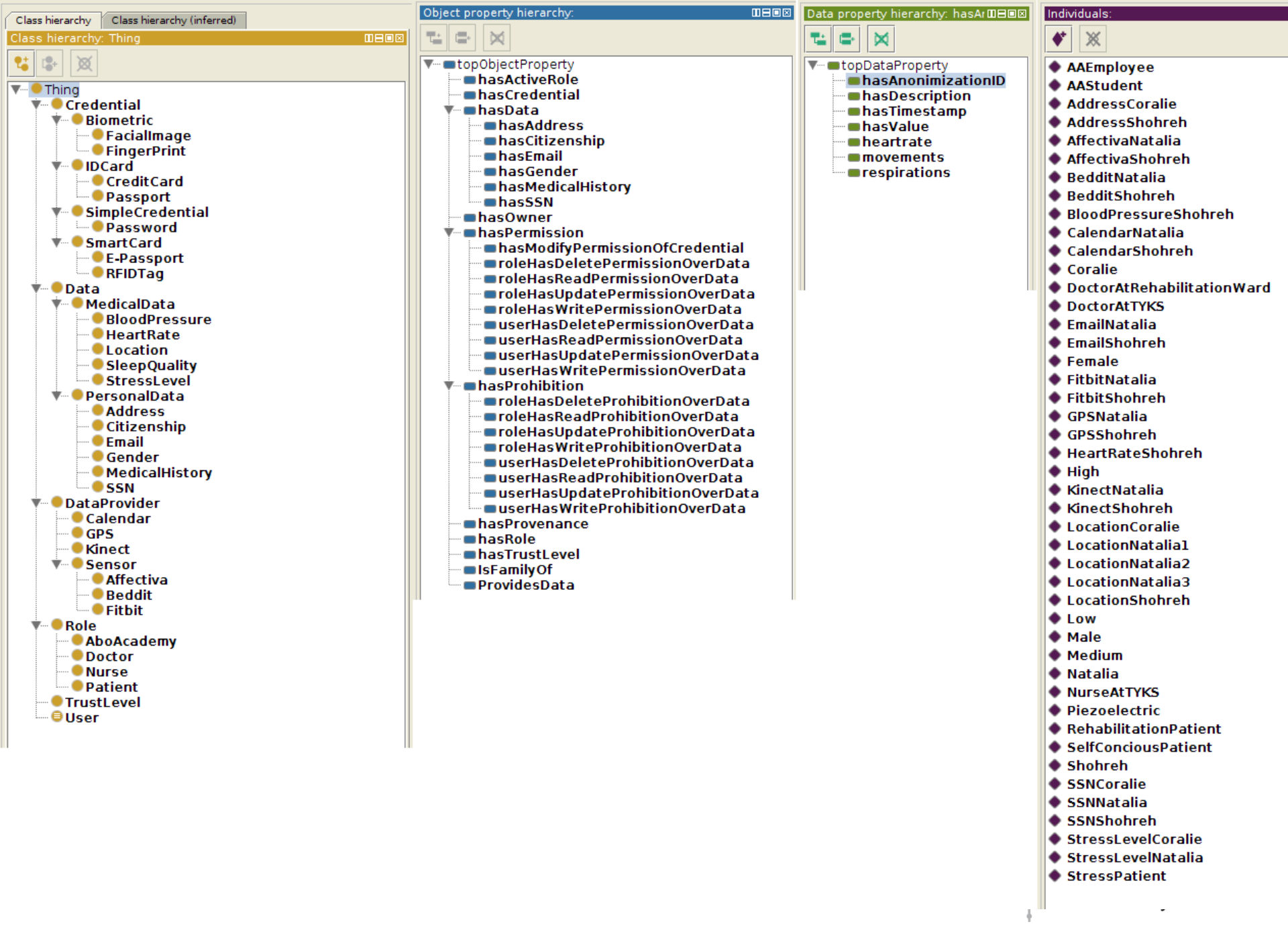
(assert (triple (Jack, *roleHasReadPermissionOverData*, ?h)))

(assert (triple (Jack, *roleHasWriteProhibitionOverData*, ?h)))

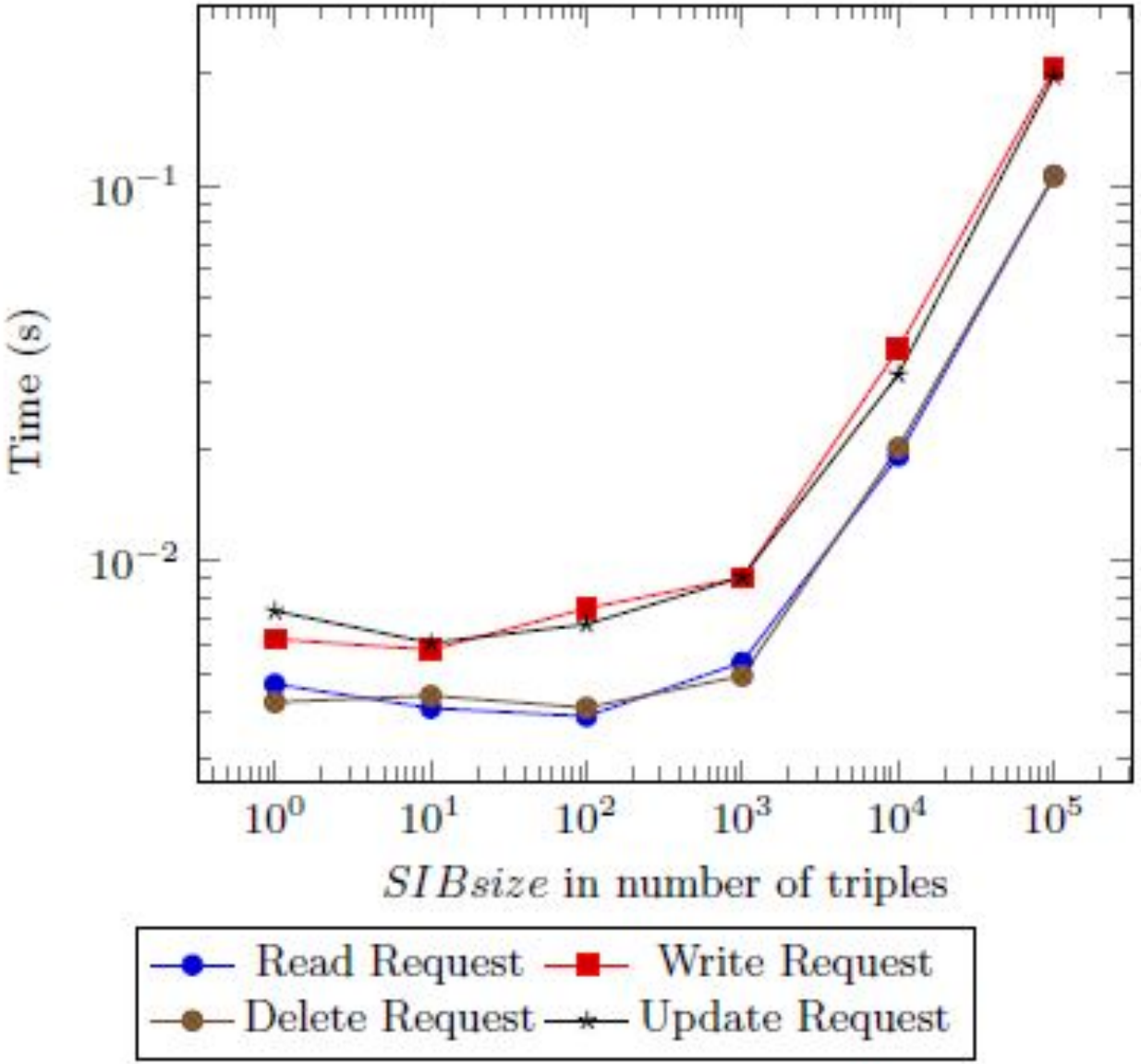
(assert (triple (Jack, *roleHasUpdateProhibitionOverData*, ?h)))

(assert (triple (Jack, *roleHasDeleteProhibitionOverData*, ?h)))

Turun yliopisto
University of Turku


Class hierarchy
Class hierarchy (inferred)
Class hierarchy: Thing
Thing
Credential
Biometric
FacialImage
FingerPrint
IDCard
CreditCard
Passport
SimpleCredential
Password
SmartCard
E-Passport
RFIDTag
Data
MedicalData
BloodPressure
HeartRate
Location
SleepQuality
StressLevel
PersonalData
Address
Citizenship
Email
Gender
MedicalHistory
SSN
DataProvider
Calendar
GPS
Kinect
Sensor
Affectiva
Beddit
Fitbit
Role
AboAcademy
Doctor
Nurse
Patient
TrustLevel
User
Object property hierarchy:
topObjectProperty
hasActiveRole
hasCredential
hasData
hasAddress
hasCitizenship
hasEmail
hasGender
hasMedicalHistory
hasSSN
hasOwner
hasPermission
hasModifyPermissionOfCredential
roleHasDeletePermissionOverData
roleHasReadPermissionOverData
roleHasUpdatePermissionOverData
roleHasWritePermissionOverData
userHasDeletePermissionOverData
userHasReadPermissionOverData
userHasUpdatePermissionOverData
userHasWritePermissionOverData
hasProhibition
roleHasDeleteProhibitionOverData
roleHasReadProhibitionOverData
roleHasUpdateProhibitionOverData
roleHasWriteProhibitionOverData
userHasDeleteProhibitionOverData
userHasReadProhibitionOverData
userHasUpdateProhibitionOverData
userHasWriteProhibitionOverData
hasProvenance
hasRole
hasTrustLevel
IsFamilyOf
ProvidesData
Data property hierarchy: hasAr
topDataProperty
hasAnonimizationID
hasDescription
hasTimestamp
hasValue
heartrate
movements
respirations
Individuals:
AAEmployee
AAStudent
AddressCoralie
AddressShohreh
AffectivaNatalia
AffectivaShohreh
BedditNatalia
BedditShohreh
BloodPressureShohreh
CalendarNatalia
CalendarShohreh
Coralie
DoctorAtRehabilitationWard
DoctorAtTYKS
EmailNatalia
EmailShohreh
Female
FitbitNatalia
FitbitShohreh
GPSNatalia
GPSShohreh
HeartRateShohreh
High
KinectNatalia
KinectShohreh
LocationCoralie
LocationNatalia1
LocationNatalia2
LocationNatalia3
LocationShohreh
Low
Male
Medium
Natalia
NurseAtTYKS
Piezoelectric
RehabilitationPatient
SelfConciousPatient
Shohreh
SSNCoralie
SSNNatalia
SSNShohreh
StressLevelCoralie
StressLevelNatalia
StressPatient

Avg exec. time for access control requests to the semantic information broker (M3 SIB)



Smart Space Application Protocol (SSAP) operations:

- Read
- Write
- Delete
- Update a triple

Turun yliopisto
University of Turku

Conclusion

We proposed

- Flexible security framework
  - fine and coarse grained information level
  - Smart Space security and privacy ontology available: https://github.com/NataliaDiaz/AccessControlOntology
- Access control scheme for Smart-M3 based spaces
  - http://sourceforge.net/projects/smart-m3/

Turun yliopisto
University of Turku

Future Work

- Security alert implementation with M3 pub/sub mechanism,
- Large scale deployment
- Micro-managing of personal data
- Data as a currency
- Integration into wearable camera & **Egoshots** dataset https://github.com/NataliaDiaz/Egoshots

Turun yliopisto
University of Turku

Thank you for your attention!

Shohreh Hosseinzadeh
shohos@utu.fi University of Turku, Finland

Natalia Díaz-Rodríguez
ndiaz@decsai.ugr.es
https://about.me/NataliaDiazRodriguez

University of Granada, Spain and Åbo Akademi University, Finland
(currently data scientist intern at Stitch Fix)

Turun yliopisto
University of Turku

References

[1] OWL for Services: http://www.ai.sri.com/daml/services/owls/security.html.

[2] F. Abel, J. L. De Coi, N. Henze, A. W. Koesling, D. Krause, and D. Olmedilla. Enabling advanced and context-dependent access control in RDF stores. volume 4825 of Lecture Notes in Computer Science, pages 1-14. Springer, 2007.

[3] S. Al-Rabiaah and J. Al-Muhtadi. ConSec: Context-Aware Security Framework for Smart Spaces. In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Sixth International Conference on, pages 580-584, Palermo, 2012. IEEE.

[4] C. A. Ardagna, S. De Capitani di Vimercati, G. Neven, S. Paraboschi, F.-S. Preiss, P. Samarati, and M. Verdicchio. Enabling privacy-preserving credential-based access control with XACML and SAML. In Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, pages 1090-1095, Bradford, United Kingdom, 2010.

[5] M. Baldauf, S. Dustdar, and F. Rosenberg. A survey on context-aware systems. International Journal of Ad Hoc and Ubiquitous Computing, 2(4):263-277, 2007.

[6] T. Berners-Lee, J. Hendler, O. Lassila, et al. The semantic web. Scientific American, 284(5):28-37, 2001.

[7] H. Chen, T. Finin, and A. Joshi. An ontology for context-aware pervasive computing environments. The Knowledge Engineering Review, 18(03):197-207, 2003.

[8] N. D íaz Rodríguez, M. Cuellar, J. Lilius, and M. Delgado Calvo-Flores. A survey on ontologies for human behavior recognition. ACM Computing Surveys (CSUR), 46(4):43, 2014.

[9] N. Díaz-Rodríguez, R. Wikstr□om, J. Lilius, M. P. Cuellar, and M. D. C. Flores. Understanding Movement and Interaction: An Ontology for Kinect-Based 3D Depth Sensors. In Ubiquitous Computing and Ambient Intelligence. Context Awareness and Context-Driven Interaction, pages 254-261. Springer International Publishing, 2013.

[10] T. Finin, A. Joshi, L. Kagal, J. Niu, R. Sandhu, W. Winsborough, and B. Thuraisingham. Rowlbac: Representing role based access control in owl. In Proceedings of the 13th ACM Symposium on Access Control Models and Technologies, SACMAT '08, pages 73-82, New York, NY, USA, 2008. ACM.

[11] S. Haibo and H. Fan. A context-aware role-based access control model for web services. In IEEE ICEBE, pages 220-223, 2005.

[12] J. Hebeler, M. Fisher, R. Blace, and A. Perez-Lopez. Semantic web programming. Wiley, J. & Sons, Indianapolis, Indiana, 2011.

Turun yliopisto
University of Turku

[13] A. Kashevnik and N. Teslya. Context-Aware Access Control Model for Smart-M3 Platform. 2013.

[14] A. Khan and I. McKillop. Privacy-centric access control for distributed heterogeneous medical information systems. In Healthcare Informatics (ICHI), 2013 IEEE International Conference on, pages 297-306, Philadelphia, PA, 2013. IEEE.

[15] D. G. Korzun, S. I. Balandin, and A. V. Gurtov. Deployment of Smart Spaces in Internet of Things: Overview of the Design Challenges. In Lecture Notes in Computer Science 8121: 48-59, 2013.

[16] A. Mhamed, M. Zerkouk, A. Husseini, B. Messabih, and B. Hassan. Towards a context aware modeling of trust and access control based on the user behavior and capabilities. In J. Biswas, H. Kobayashi, L. Wong, B. Abdulrazak, and M. Mokhtari, editors, Inclusive Society: Health and Wellbeing in the Community, and Care at Home, volume 7910 of Lecture Notes in Computer Science, pages 69-76. Springer Berlin Heidelberg, 2013.

[17] S. P. Miller, B. C. Neuman, J. I. Schiller, and S. J. H. Kerberos authentication and authorization system. In Project Athena Technical Plan, Cambridge, USA, 1987. Massachusetts Institute of Technology (MIT).

[18] M. Mohsin Saleemi, N. Daz Rodrguez, J. Lilius, and I. Porres. A Framework for Context-Aware Applications for Smart Spaces. In Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on, Munich, Bavaria.

[19] M. Peleg, D. Beimel, D. Dori, and Y. Denekamp. Situation-based access control: Privacy management via modeling of patient data access scenarios. Journal of Biomedical Informatics, 41(6):1028-1040, 2008.

[20] O. Sacco and A. Passant. A privacy preference ontology for linked data. In Linked Data on the Web Workshop at the World Wide Web Conference, 2011.

[21] J. Suomalainen. Flexible security deployment in smart spaces. In Lecture Notes in Computer Science, volume 7096, pages 34-43. Springer, 2012.

[22] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila. A semantic context-aware access control framework for secure collaborations in pervasive computing environments. In I. Cruz, S. Decker, D. Allemang,

C. Preist, D. Schwabe, P. Mika, M. Uschold, and L. Aroyo, editors, The Semantic Web - ISWC 2006, volume 4273 of Lecture Notes in Computer Science, pages 473-486. Springer Berlin Heidelberg, 2006.

[23] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila. Proteus: A semantic context-aware adaptive policy model. In Policies for Distributed Systems and Networks. POLICY '07. Eighth IEEE International Workshop on, pages 129{140, Bologna, Italy, 2007.

[24] C. D. Wang, T. Li, and L. C. Feng. Context-aware environment-role-based access control model for web services. In Multimedia and Ubiquitous Engineering. International Conference on, pages 288-293, 2008.

Turun yliopisto
University of Turku