New Approaches to Privacy and Security

Bernd Blobel, PhD, FACMI, FACHI, FHL7
Professor, University of Regensburg, Germany
Former Head, eHealth Competence Center, University Hospital
Regensburg, Germany
Co-Chair, HL7 Security WG
Objectives

• This presentation introduces into new standards for privilege management and access control communication and cooperation in healthcare.

• It refers to NIST RBAC, HL7 RBAC Healthcare Permission Catalog, HL7 Healthcare Privacy and Security Classification System (HCS) – Release 1 as well as policy-driven RBAC using explicit ontology-based policies according ISO 22600.
New Approaches to Security and Privacy

The Interoperability Challenge

Knowledge

Information cycle
(after van Bemmel et al., changed)

HP or HCE
Action
Patient

Observation

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge

HP or HCE
Action
Patient

Observation

Knowledge

Information cycle
(after van Bemmel et al., changed)

Diagnosis

Therapy

Observation

Data

Interpretation

Patient

The Interoperability Challenge
The Interoperability Challenge

- Interoperability describes motivation, willingness, abilities and skills to meet common interests or business objectives.
- Interoperability in such systems requires shared appropriate knowledge, abilities and skills for establishing an adequately cooperating combined system.
- When the corresponding knowledge, abilities and skills is not present on the communicating and cooperating sites, they must be provided dynamically.
- The different realization of the interoperability prerequisites results in different interoperability levels required for providing comprehensive interoperability.
Role-Based Access Control

Role_Hierarchy

Principal 0..* Structural_Role

User_Assignment

User_Session 0..* 0..* Session 1..*

Functional_Role

User_Section 0..* 1..* 1..* Session_Role

Permission_Assignment

Target_Component
HL7 RBAC Healthcare Permission Catalog
Policy

- Policies are rules governing the choices in behavior of a system (Sloman)
- A policy is a collection of general principles specifying the desired behavior of a system (Bell Labs)
- A policy is a set of legal, political, organisational, functional and technical obligations for communication and cooperation (ISO 22600)
Policy

Policies rule administered aggregations (within a domain) and interrelations (between domains) of a system’s components. Aggregations and interrelations not administered but independently ruled by the nature of the business domain's concept space such as biomedical concepts (e.g., relations between systolic and diastolic blood pressure) are not called policies but represented by ontological relationships.
New Approaches to Security and Privacy

BerndBlobel
University of Regensburg, Germany
HL7 Germany

HL7 Working Group Meeting
Security WG Tutorial
San Antonio, 22 January 2014
New Approaches to Security and Privacy

Domain Perspective

System’s Architectural Perspective

Development Process Perspective

Admin Domain
Policy Domain
Medical Domain

Business Concepts
Relations Networks
Aggregations
Details

System Viewpoint

System Component Composition

Business View
Information View
Computational View
Engineering View
Technology View
New Approaches to Security and Privacy

Bernd Blobel
University of Regensburg, Germany
HL7 Germany

HL7 Working Group Meeting
Security WG Tutorial
San Antonio, 22 January 2014
New Approaches to Security and Privacy

Bernd Blobel
University of Regensburg, Germany
HL7 Germany

HL7 Working Group Meeting
Security WG Tutorial
San Antonio, 22 January 2014

Business Concepts
Relations Networks
Aggregations
Details
Security Policy (ISO 22600)

- Security policy is a complex of legal, organizational, functional, social, ethical and technical aspects to be considered in the context of privacy and security.
- Security policy defines a framework, privileges and obligations, but also consequences and penalties when the regulations are ignored.
Policy-Driven Role-Based Access Control

SR_Policy

Structural_Role

Role_Hierarchy

FR_Policy

Target_Policy

Principal

User_Session

User_Assignment

Functional_Role

Permission_Assignment

Session

Session_Role

Process_Policy

Target_Component

Permission_Assignment

Security Labels

- Security Labels are tags linking an information object with a set of security and privacy attributes. They can be bound to data, but also to persons and resources. In the new HL7 Healthcare Privacy and Security Classification System (HCS), the following security labels have been defined: Confidentiality, Sensitivity, Integrity, Compartment and Handling Caveats.
Conclusions 1

• Communication and cooperation in healthcare requires intelligent and transparent methods for communicating and imposing security and privacy aspects in an open environment.

• Security labels enable the binding of more or less detailed policies to objects serving this communication and cooperation. This Access Control Information and the derived Access Control Decision Information can be standardized to enable interoperability in health and social care by respecting the required legal conditions and patient’s intentions.

• The use of Security Labels requires structuring and classifying medical multimedia information as well as a common security domain.
Conclusion 2

- In a coarse-grained variant, the presented solution for security labeling of segmented medical information realizes a context-sensitive RBAC, which goes beyond the RBAC extensions of the HL7 RBAC Healthcare Permission Catalog.
- The specification defines a normative set of interoperable Security Labels for healthcare to be used for the transfer of data between systems or domains.
- Furthermore, a vocabulary for standard-conformant Security Labels has been defined.
Conclusion 3

- A segmentation up to a atomic level would go close to the ISO 22600 policy definition. However, the static classification and some further limitations must be overcome.

- In summary, the presented solution proposes a roadmap to the complex use of ISO 22600 and the ontology-based, explicit policy definitions provided there. This allows users to start with minimal solutions and scale them up and develop them consistently. The HL7 Healthcare Security and Privacy Classification System went out for ballot in September 2013. The presented standard will have a positive impact on solutions practically ensuring privacy and security.
Thank you very much for your kind attention!

Prof. Dr. rer. nat. habil. Bernd Blobel, FACMI, FACHI, FHL7
Former Head, eHealth Competence Center at the
University of Regensburg Medical Center

Email: bernd.blobel@ehealth-cc.de
Email: bernd.blobel@klinik.uni-regensburg.de