



Towards a Privacy Policy Enforcement Middleware with Location Intelligence

Yi Zheng, Dickson K. W. Chiu, Hongbing Wang, Patrick C. K. Hung**

**Faculty of Business and IT*

University of Ontario Institute of Technology (UOIT), Canada

{Yi.Zheng, Patrick.Hung}@uoit.ca

- The Electronic Healthcare Record (EHR), defined as a “digitally stored health care information about an individual’s lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times.”
 - The EHR includes all types of information regarding patient’s treatments, such as observations, treatments, therapies, drugs administered, patient identifying information, etc.
 - The rapidly growing information automation in healthcare services results in a severe interoperability problem in the healthcare informatics domain.
-

Clinical Document Architecture (CDA)

- Released by Health Level 7 (HL7)
- XML-based document markup standard
 - specifies the structure and semantics of clinical documents for the purpose of exchange
- Create, store and communicate all health related information transactions as a set of standard XML messages
 - e.g. the standard transaction for an electronic claim (X12N 837)



http://www.hl7.org/memonly/downloads/Attachment_Specifications/HIPAA_and_Claims_Attachments_White_Paper_20040518.pdf

- ❏ Several XML-based EHR standards developed by organizations operating in healthcare arena, such as Health-Level 7(HL7), Medical Markup Language (MML), etc.
- ❏ Their primary objective is to draft specifications that can form the basis for the exchange, management, and integration of clinical patient care and healthcare services related data.
- ❏ Hemodialysis Medical Record Exchange Format (HeMX) is designed to structure and describe medical records on dialysis therapy, as a format for exchanging information and data both online and offline.

Introduction (cont.)

- ❏ Home dialysis is a healthcare scenario with mobile healthcare applications.
 - ❏ *Hemodialysis* is a process of filtering wastes and excess water from the blood when an individual is experiencing chronic kidney disease or kidney failure.
 - ❏ Patients are now able to undergo hemodialysis in their home, having the opportunity to carry out their treatment themselves, and on their own schedule, while freeing up limited space available in hospitals.
 - ❏ Hemodialysis conducted within the home is more comfortable and convenient, and less costly, while also improving client care and vitality.
 - ❏ Home dialysis is becoming increasingly popular in many countries, such as the USA, Canada, etc.
-

Introduction (cont.)

```
<?xml version="1.0" encoding="UTF-8" ?>
<?xml-stylesheet type="text/xsl" href="HeMX_0.94b.xsl"?>
<HeMX version="1.00" createDate="2000-5-23T12:00:00">
  <HDHeader>
    <facility>
      <facilityName>Lakeridge Healthcare Institute</facilityName>
      <facilityId type="insurance">88-14774</facilityId>
    </facility>
    <patient>
      <patientId type="facility">12345678</patientId>
      <personName>
        <familyName>Simpson</familyName>
        <givenName>Bart</givenName>
        <middleName>James</middleName>
      </personName>
      <birthday>1960-04-02</birthday>
      <sex>male</sex>
      <address>
        <countryCode>CAN</countryCode>
        <zip>L1G3T9</zip>
        <prefecture>Toronto</prefecture>
        <city>Pickering</city>
        <otherDescriptor>Taunton 1-5-45</otherDescriptor>
      </address>
      <note>Lefthanded</note>
    </patient>
  </HDHeader>
```

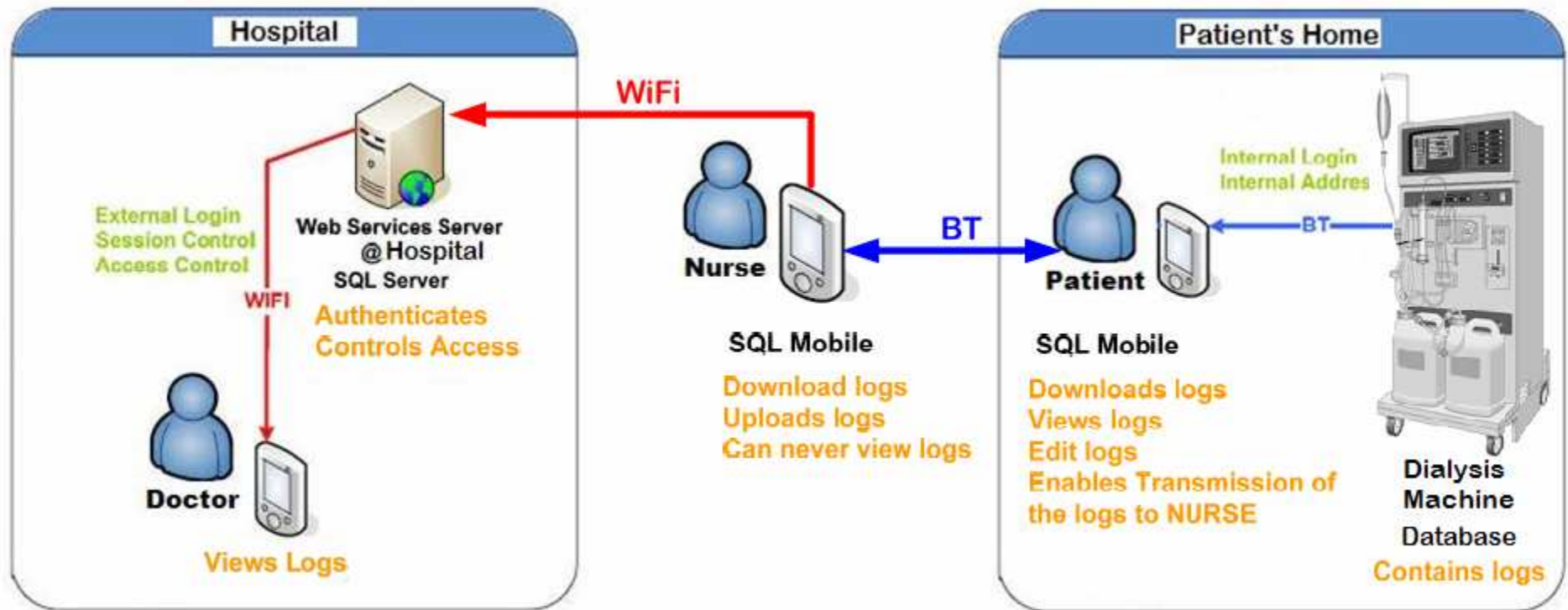
A Sample of HeMX Hemodialysis Document

Introduction (cont.)

```
<HDBody>
  <HDOrderSection>
    <hdOrders orderStatus="active" dateOrdered="2000-05-03">
      <orderGroups>
        <effectiveDays>
          <weekDay hdDay="Monday"/>
        </effectiveDays>
        <hdMethod>
          <hdMethodName code="01" tableId="hdMethodTable01">blood dialysis</hdMethodName>
          <timeHdStart timeDirection="after">PT0H0M0S</timeHdStart>
          <timeHdEnd timeDirection="after">PT4H0M0S</timeHdEnd>
        </hdMethod>
        <dryWeight unit="kg">60.0</dryWeight>
        <bloodFlow>
          <flowRate unit="ml/min">200</flowRate>
        </bloodFlow>
        <dialyser code="AM-SD-13M" type="productNumber" membraneArea="1.3" unit="m2">AMSD13M
      </dialyser>
        <dialysate>
          <dialysateName code="3410520A5024" type="price" modification="Ca=2.5mEq">kinderly
liquid 2 servings</dialysateName>
        </dialysate>
        <dialysateFlow>
          <flowRate unit="ml/min">600</flowRate>
        </dialysateFlow>
        <dialysateTemp>
          <dialysateTempValue unit="C">37</dialysateTempValue>
        </dialysateTemp>
      </orderGroups>
    </hdOrders>
  </HDOrderSection>
</HDBody>
</HeMX>
```

A Sample of HeMX Hemodialysis Document (cont.)

Introduction (cont.)



A Sample of Mobile Healthcare Services

- ❏ *Access control* is the process of limiting access to the resources of a system to only authorized users, programs, processes, or other systems.
 - ❏ Determine which users (i.e. subject) are permitted access to resources (i.e. object) according to their identities, authentication, and associated privileges authorization.
 - ❏ Authentication vs. access control
 - ❏ Authentication is the process of attempting to verify the digital identity of the sender of a request to log in.
 - ❏ Access control rests on proper user identification and on the correctness of the authorizations.
 - ❏ Access control models have traditionally included *mandatory access control* (MAC) and *discretionary access control* (DAC).
-

Privacy Access Control Model (cont.)



- ❑ Both MAC and DAC do not satisfy most of the commercial needs.
 - ❑ Alternatives, such as Role Based Access Control (RBAC) have been proposed.
 - ❑ In RBAC, permission is associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions.
 - ❑ Roles can be granted new permission, and permission can be revoked from roles as needed.
 - ❑ The Core RBAC defines five basic data elements: *users* (USERS), *roles* (ROLES), *objects* (OBS), *operations* (OPS) and *permissions* (PRMS).
 - ❑ RBAC has a natural fit with healthcare applications.
-

Privacy Access Control Model (cont.)

- “Privacy is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to.”

<http://en.wikipedia.org/wiki/Privacy>

- “All persons have a fundamental right to privacy, and hence to have control over the collection, storage, access, communication, manipulation and disposition of data about themselves.”

International Medical Informatics Association (IMIA)



Privacy Access Control Model (cont.)

- Protected Health Information (PHI)
 - PHI often contains **identifiable** and **sensitive** information such as genetic or demographic data about individuals

identifiable

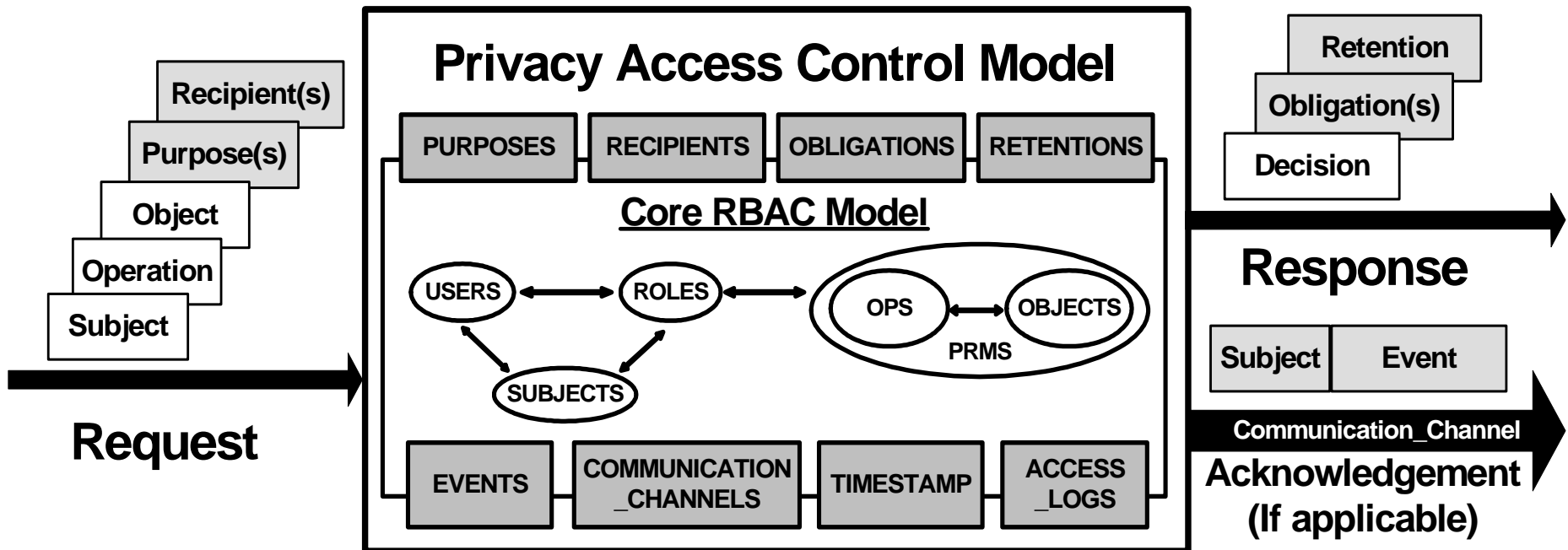
Name
Age
Sex
Address
Phone Number
Fax Number
E-mail Address



sensitive

Family composition
Employment status
DNA Profile
Voice
Fingerprints
Social Security Number
Medical Record Number

Privacy Access Control Model (cont.)



Core RBAC Entities	eXtensible Access Control Markup Language (XACML) Implementation
USERS	<Subjects>
ROLES	<Subject Attributes>
OBJECTS	<Resources>
OPS	<Actions>
PRMS	<PolicySet>, <Policy>

Extended RBAC Entities	XACML Implementation
PURPOSES	<resource:purpose> <action:purpose>
RECIPIENTS	<Subjects>
OBLIGATIONS	<Obligations>
RETENTIONS	<Retentions>

Privacy Access Control Model (cont.)

```
<Policy RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:
    rule-combining-algorithm:deny-overrides">
  <Description>An example policy </Description>
  <Rule Effect="Permit"> Permission
    <Description>
      Julius Hibbert can read Bart Simpson's medical record for
      medical treatment purpose if she follows the obligation
      "No disclosure" and "No retention"
    </Description>
    <Subjects>
      <Subject>Julius Hibbert</Subject> Subject
    </Subjects>
    <Resources>
      <Resource>
        http://medico.com/record/patient/BartSimpson Object
      </Resource>
    </Resources>
    <Actions>
      <Action action:purpose = "Medical Treatment"> Purpose
        </AttributeValue>read</AttributeValue> Operation
        <recipients>Individual</recipients> Recipient
      </Action>
    </Actions>
    <Obligations>No-disclosure</Obligations> Obligation
    <Retentions>No-retention</Retentions> Retention
  </Rule>
</Policy>
```

- ❏ The term “location” generally refers to the position an object possesses within physical space, with respect to a specific frame of reference (e.g., the position of another point or thing).
 - ❏ A real location can be assigned through the use of a specific pairing of latitude, longitude, and altitude.
 - ❏ Many location positioning systems would rather describe a locations as a place name like “Hospital”, “Office” or “Home” than its geographic coordinates such as (40.92774, -12.0953).
 - ❏ Research works have advocated that location information can be used to provide additional security.
 - ❏ D. E. Denning and P. F. MacDoran, “Location-based Authentication: Grounding Cyberspace for Better Security,” In Computer Fraud and Security, Elsevier Science, Vol. 1996, No. 2, Pages 12-16, February 1996.
 - ❏ I. Ray and L. Yu, "Short Paper: Towards a Location-Aware Role-Based Access Control Model", First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005), Pages 234-236, September 5-9, 2005.
-

Location Constraints (cont.)

- ❏ Michalakis presents Pervasive Access Control (PAC) that uses a lightweight security solution to authenticate a user's location by avoiding heavy security at the end-points and minimizing the number of trusted components.
 - ❏ The Location ID (LID) authority authenticates the membership of a user in a location group by mappings between location groups and client LID and keeping track of the corresponding time-varying location code.
 - ❏ N. Michalakis, "PAC: Location Aware Access Control for Pervasive Computing Environments," 2002. [online] Available: <http://sow.csail.mit.edu/2002/proceedings/michalakis.pdf>
 - ❏ Damiani et al. present GEO-RBAC, which extends the RBAC model enhanced with spatial and location-based information.
 - ❏ GEO-RBAC relies on the Open GIS Consortium (OGC) spatial model to model (spatial) objects, user positions, and geographically bounded roles.
 - ❏ Moreover this model has the ability to deal with both real positions, obtained from a given mobile terminal such as cellular phone or PDA, and logical position, possibly represented at different granularities.
 - ❏ M. L. Damiani, E. Bertino, B. Catania and P. Perlasca, "GEO-RBAC: A Spatially Aware RBAC," In Proceedings of the Tenth ACM symposium on Access Control Models and Technologies, Pages 29-37, 2005.
-

Location Constraints (cont.)

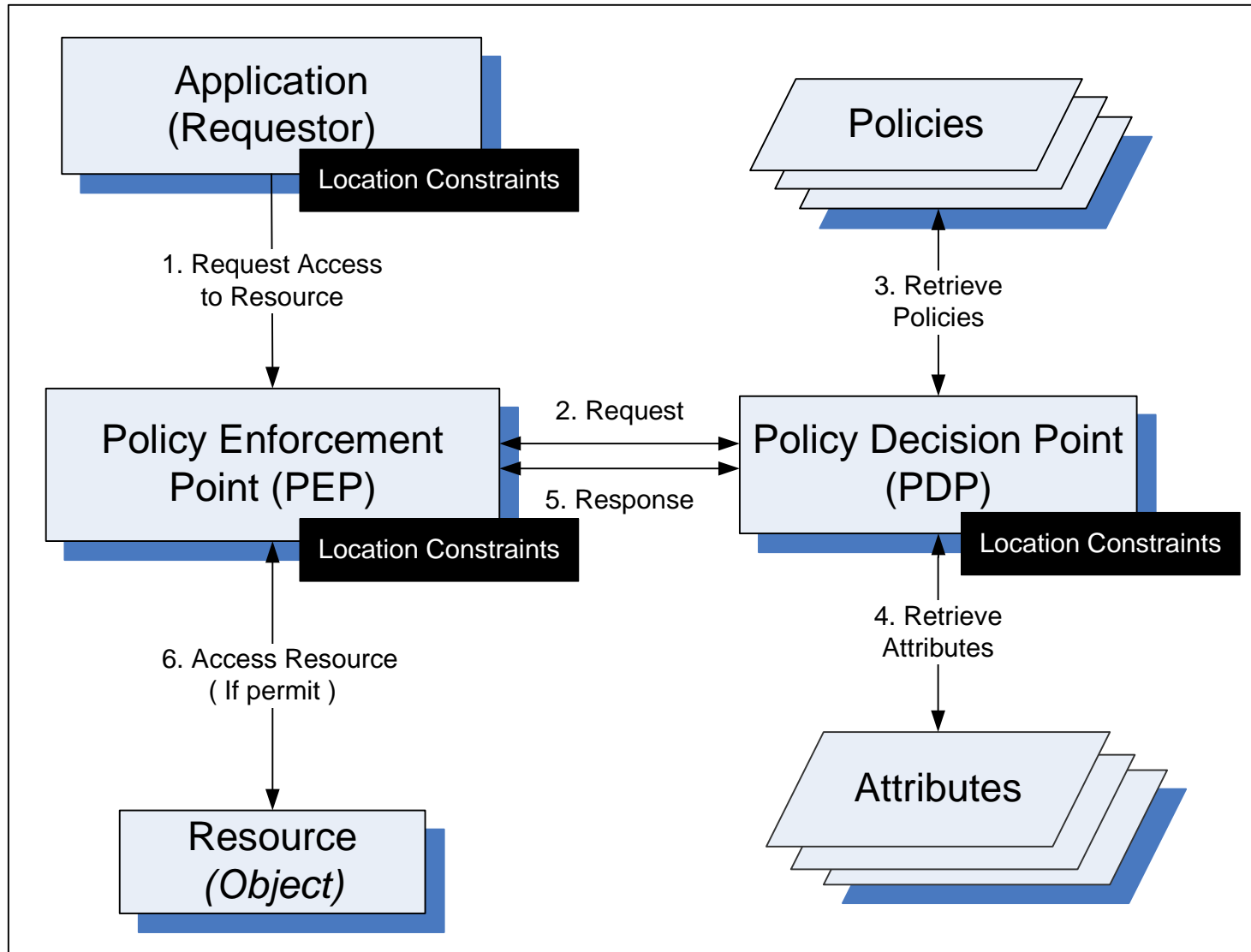


The Great Wall of China

- ❏ Constraints are used to specify configurations of the model that the specific requirements needed to be enforced in the system.
 - ❏ Location Reference Group
 - ❏ Where the relative location of a group of *beacons* are consistently referenced in a specific location within a certain period of time.
 - ❏ Use *location beacons* to announce the current location information, e.g., Bluetooth beacons.
 - ❏ In the hemodialysis scenario, we specify the location constraints as that the nurse can only collect the medical records (i.e., object) while both the nurse PDA (i.e., subject) and patient PDA (i.e., subject) are at the patients' home.
-

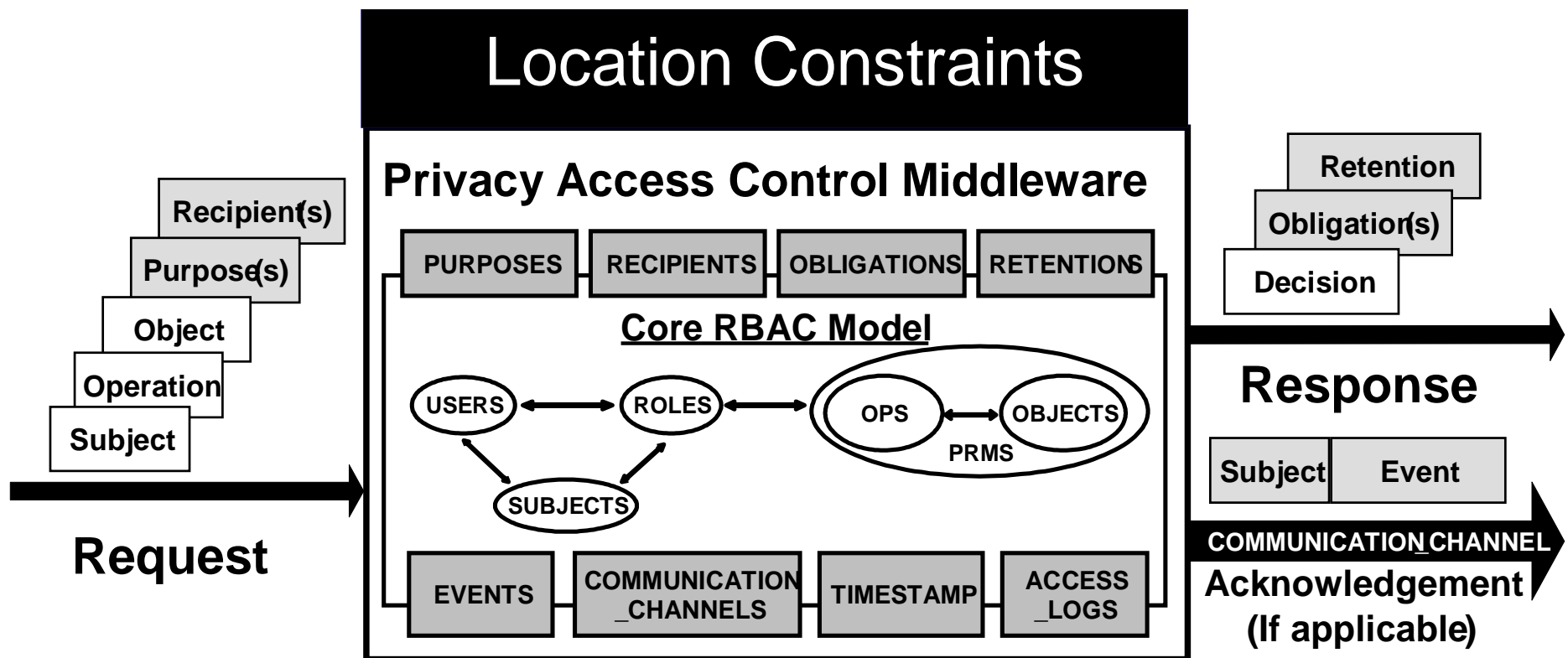
- ❏ The Internet Engineering Task Force (IETF) defines an abstract model for policy enforcement which is applied by eXtensible Access Control Markup Language (XACML)
 - ❏ *Policy Decision Point (PDP)*: The point where policy decisions are made.
 - ❏ The PDP does not control the enforcement of the decision.
 - ❏ *Policy Enforcement Point (PEP)*: The point where the policy decisions are actually enforced.
 - ❏ Any requests for access to a protected resource go through the PEP
 - ❏ *Resource*: Something of value in a network infrastructure to which rules or policy criteria are first applied, before access is granted.
 - ❏ *Policies*: The combination of rules and services where rules define the criteria for resource access and usage.
-

Location Constraints (cont.)



Extended policy enforcement and decision model with location constraints

Location Constraints (cont.)



Location Constraints (cont.)

```
<Apply FunctionId="function:must-be-located">
```

```
<AttributeSelector DataType="location:civilAddress">
```

```
  Lakeridge Healthcare Institute
```

```
</AttributeValue>
```

```
<xacml:EnvironmentAttributeDesignator
```

```
  AttributeId="urn:oasis:names:tc:xacml:2.0:conformance-test:IIA1:rule"
```

```
  RequestContextPath="/Policy/Rule/Subjects/Subject:Created/text()">
```

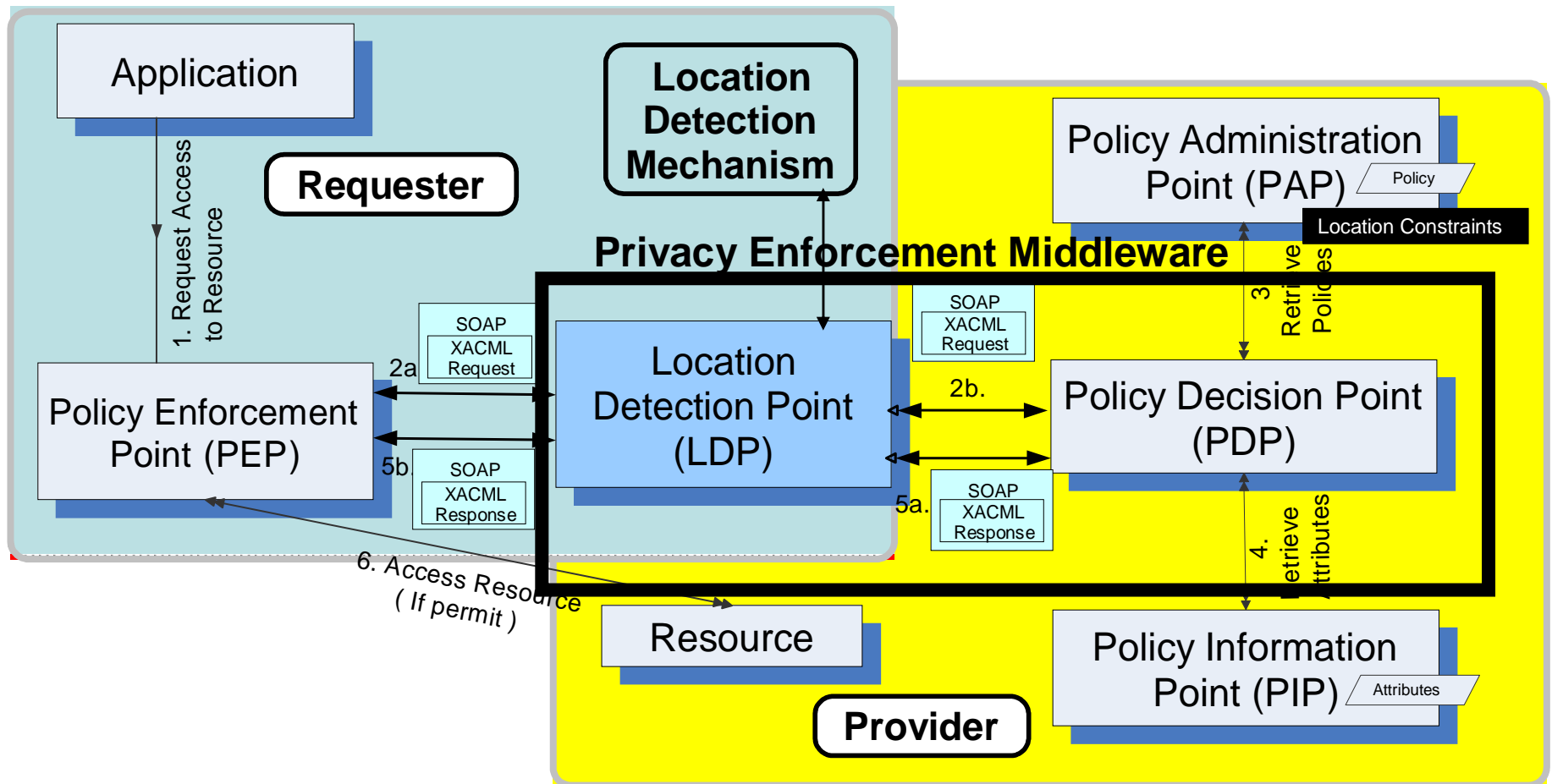
```
  Hemodialysis
```

```
</xacml:EnvironmentAttributeDesignator>
```

```
</Apply>
```

Extended WS-PolicyConstraints framework for expressing the location constraints

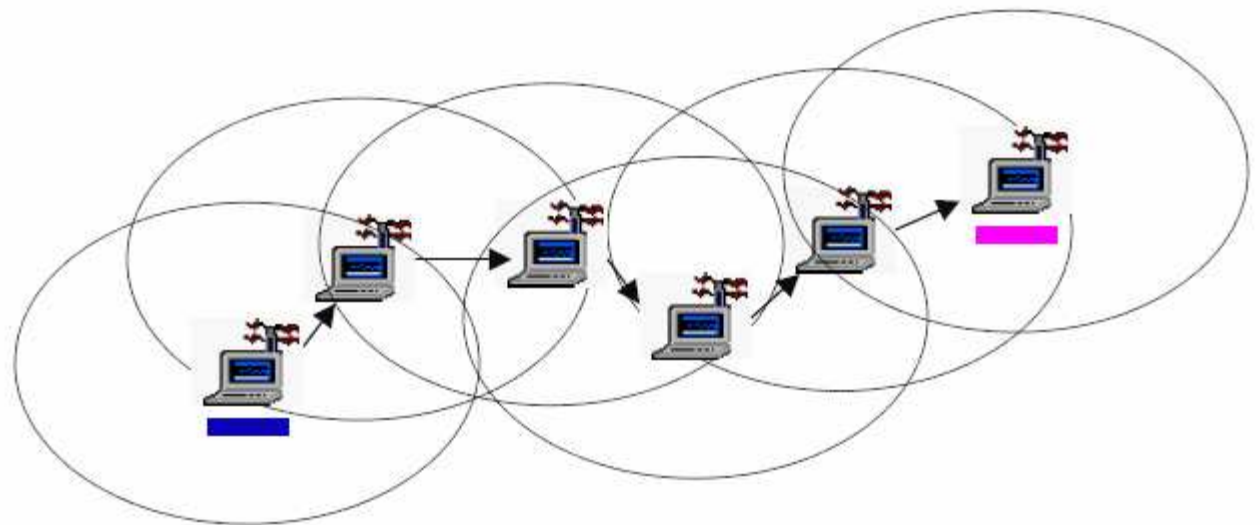
Location Constraints (cont.)



- ❏ Mobile applications have been increasingly used to exchange patient's electronic health information.
 - ❏ In this research presentation, we discuss a variety of research issues of developing a privacy access control model with location constraints in mobile XML-based healthcare services.
 - ❏ As we are moving towards an age of ubiquitous computing, location information is becoming an important component of access control.
-

Mobile Ad hoc NETWORK (MANET)

- MANETs are often termed infrastructure-less, self-organized, or spontaneous networks.
- MANET is a multi-hop autonomous system.
- The system may operate in isolation, or may have gateways to and interface with a fixed network.



Properties of MANET

- The five fundamental mobile ad hoc properties that the model must meet:
 1. **Mobility:** M-services should only be limited by the range (distance) and location, which is set by the access control and business logic of the application.
 2. **Peer-to-Peer:** M-services have to interact and communicate directly or indirectly in a certain location and distance, with or without using a central node/server, with each other.
 3. **Collocation:** All logical interactions between m-services have to result in a physical interaction between location-based users.
 4. **Collaboration:** Collocated m-services need to be willing to collaborate in a certain location and distance.
 5. **Transitory Community:** M-services may join and withdraw from the interactions at any time, making it an ever changing map.
-

The Proposed Model of Communication and Application Security

Secure Routing Protocol	Privacy Policy
Public Key Infrastructure (PKI)	Authorization Service
Wi-Fi Protected Access 2 (WPA2)	Secure Service Discovery
IEEE 802.1x standard	

Note:

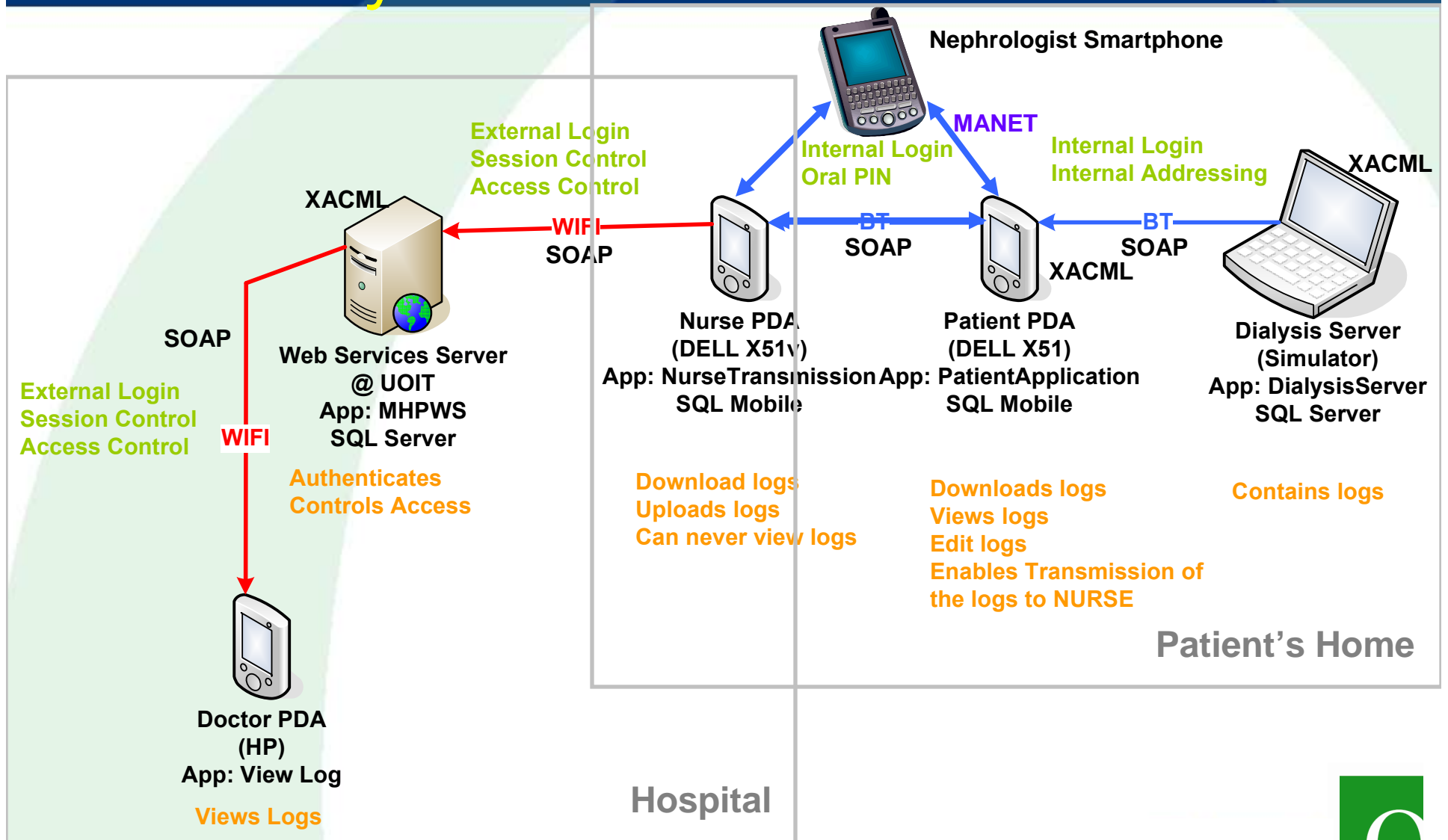
Communication Security

Application Security



Hemodialysis Proof-of-Concepts Demo

Preliminary Version 0.2



Team Members – (Started on May 1, 2006)

- ❏ **Principal Investigator:** *Patrick Hung (UOIT and University of Waterloo, Canada)*
- ❏ **Research Assistant:** *Ms. Jordanne Christie (UOIT, Canada)*
- ❏ **Co-Investigators:**
 - ❏ *Prof. Jay Tashiro, Prof. Wendy Stanyon and Prof. Otto Sanchez (Health Sciences, UOIT, Canada) and Prof. Mike Elkund (Engineering, UOIT, Canada)*
 - ❏ *Prof. Eric Yu (Information Studies, University of Toronto, Canada)*
 - ❏ *Prof. Pin-Han Ho (Electrical and Computer Engineering, University of Waterloo, Canada)*
- ❏ **Guest Researcher:** *Ms. Jasmine Li (University of New South Wales, Australia) – In town!*
- ❏ **Students in 2007-Present:**
 - ❏ *Mr. Ryan Bishop, Ms. Stephanie Chow, Ms. Michelle Watson, Ms. Amanda Paul, Mr. Joshua Boudens, Mr. Rajan.Mistry and Mr. Ranny Huang (UOIT, Canada)*
 - ❏ *Ms. Yi Zheng (UOIT, Canada and Technical University of Munich, Germany) – **Currently work at SAP Research, Montreal for an internship position***
 - ❏ *Mr. Mohammed Liakat Ali, Mr. Chen Chen, and Mr. Ming Gong (University of Waterloo, Canada)*
- ❏ **Students in 2006-2007:**
 - ❏ *Mr. Yongming Chen, Dr. A. K. M. Harun-Ar-Rashid, Mr. Kapil Pradhan, Ms. Donna Rousell and Mr. Jude Andrade (UOIT, Canada)*
 - ❏ *Mr. Parsa Shabani, Ms. Nidhi Sachdev, Ms. Faranak Farzad, Mr. Catalin Bidian and Mr. Vic Chung (University of Toronto, Canada)*
 - ❏ *Ms. Vivying Cheng (Hong Kong University of Science and Technology, Hong Kong)*



Thank You!

The End

Thank you for your time!

