Access Control and Trust in the use of Widely Distributed Services

Jean Bacon, Ken Moody, Walt Yao

University of Cambridge Computer laboratory

OASIS – talk overview

(**O**pen **A**rchitecture for **S**ecure **I**nterworking **S**ervices)

- brief introduction and motivation
- OASIS - model
  - architecture
  - engineering
  - integration with PKI
- an Electronic Health Record (EHR) service
  as an example application throughout
- domains, services and clients
- more speculative ideas on trust

Requirements / Motivation

- large scale

  => role based access control (RBAC)
- potentially widely distributed systems
- heterogeneous components, developed independently but must interoperate

  => service-level agreements (SLAs)
- incremental deployment

Motivating example: a national EHR service

- MUST protect EHRs from journalists, insurance companies, family members etc.
- access policy defined both nationally and locally
- generic scalable policy **=> RBAC**
- **exception of individuals** is allowed by law,
  (all doctors except my uncle Fred Smith)
  "Patients' Charter" **=> parametrised roles**
- may need to express relationships between parameters
  treating-doctor (doctor-id, patient-id)

OASIS RBAC summary of features

- **decentralised,** service/domain - specific **role management**
- **parametrised roles**
- **session-based** role activation
- **appointment** replaces privilege delegation and role hierarchy and supports persistent credentials
- **active security**

  environmental constraints on role activation

  monitoring of role membership conditions

  implemented on active, event-based, middleware

OASIS RBAC

- OASIS services name their clients in terms of **roles**

- OASIS services specify **policy** in terms of **roles**
  - for **role entry** (activation)
  - for **service invocation**

  both in Horn clause form

OASIS model of **role activation**

a role activation rule is of the form:

condition1, condition2, ….. |- target role

where the conditions can be

- prerequisite role
- appointment credential
- environmental constraint

all are parametrised

prerequisite role

the principal must present a credential (a role membership certificate (RMC)) to prove that it is already active in some other role

of this service or another service

appointment credential

a session-independent credential to prove, e.g. professional/academic qualification, employment, membership

environmental constraint

- checks on **parameters** of other credentials (values and relationships)
- environmental conditions e.g. time,
- group membership by database lookup

these context checks contribute to an **active security environment**

OASIS role **membership** rules

as we have seen, a role activation rule:

cond1*, cond2, cond3*, ….. |- target role

role membership rule:

the role activation conditions that must **remain true**, e.g.*

for the principal to remain active in the role

monitored using event-based middleware

another contributor to an **active security environment**

OASIS – talk overview

(**O**pen **A**rchitecture for **S**ecure **I**nterworking **S**ervices)

- **brief introduction and motivation**
- **OASIS** **- model**
  - architecture
  - engineering
  - integration with PKI
- Electronic Health Records (EHR)
  as an example application throughout
- domains, services and clients
- more speculative ideas on trust

Role membership Certificates (RMCs)

role-name (parameters), issuing-service (mgt info), issuer's signature

*so integrate with **X.509** and **SSL** !*

X.509 certificate structure:

subject-id, subject public key
issuer-id, signing algorithm, signature
validity: not-before, not-after
admin: version #, serial #
extended info: role-name and parameters

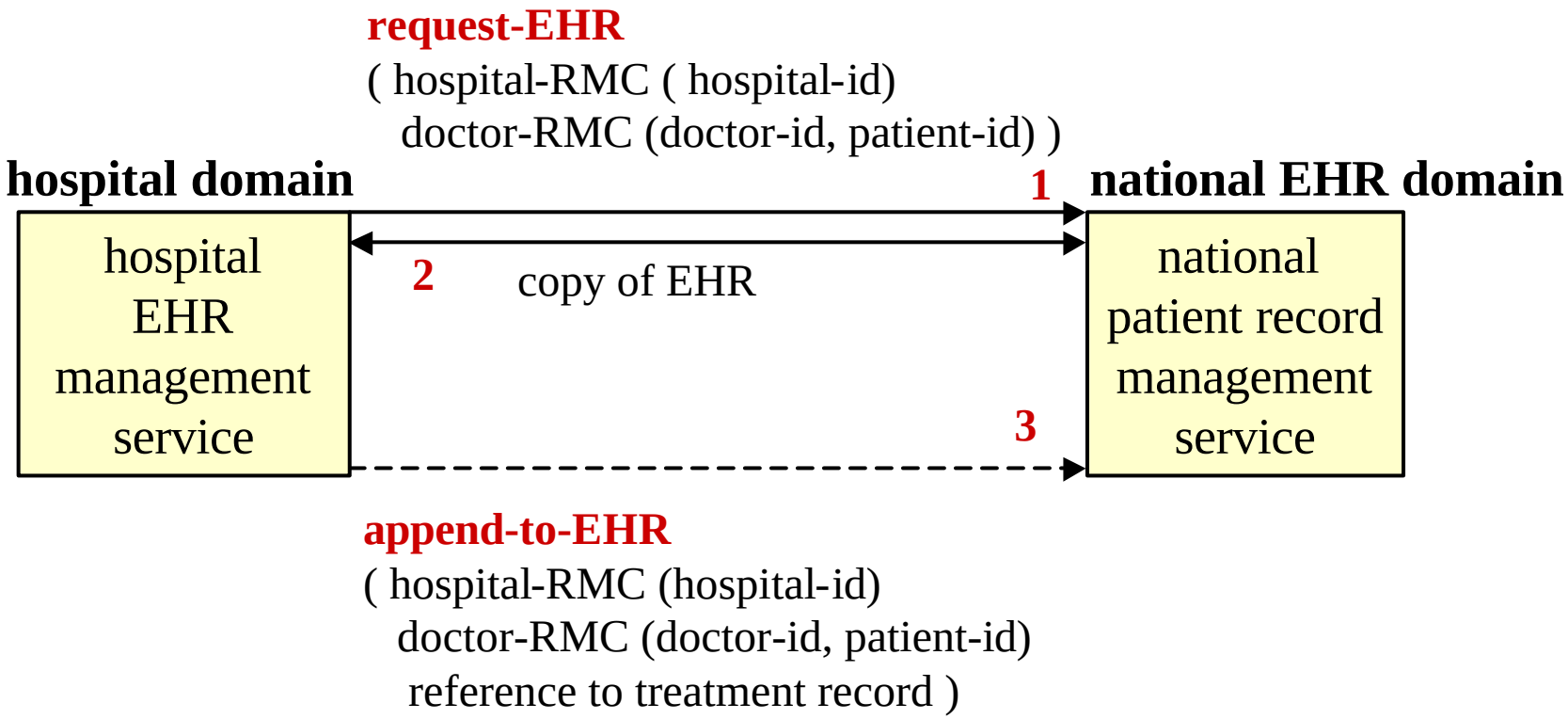
*and use **challenge-response** for authentication*

OASIS - talk overview

(Open Architecture for Secure Interworking Services)

- **brief introduction and motivation**
- **OASIS - model**
  - architecture
  - engineering
  - integration with PKI
- **Electronic Health Records (EHR)**
  as an example application throughout
- **domains, services and clients**
- **more speculative ideas on trust**

Example of service invocation from the home domain to an external domain



Example continued:

- certificates (RMCs) are **checked by call-back** to the issuer

  optimisation: caching + event channels for invalidation
- **hospital-RMC** is issued by the national EHR domain to a well-known and trusted client hospital's EHR service
- **doctor-RMC** is issued by the hospital domain to an employed doctor
- certificates are stored with data for **audit** purposes
- access policy and **exclusions** are enforced at the national EHR service

  so we need RMC **parameters** and service call parameters

Principal working in an external domain

- mutual trust between home and external domains

  e.g. hospital and research centre
- SLA: home domain issues an **appointment certificate**

  e.g. ***employed-as-doctor (doctor-id, hospital-id)***

  external domain allows it for entry to some role

  e.g. ***visiting-doctor (doctor-id)***
- appointment certificate is validated by call-back to issuing domain at role-activation time

Anonymous use of services

- a **role-name** (without the principal identity as a parameter) allows anonymous use of services
- an anonymous **appointment certificate** (without the principal identity as a parameter) may authorise role activation, provided environmental conditions are satisfied (e.g. expiry date of a membership)
- SLAs negotiate available services

  e.g. related organisations, sensitive tests

Mutually unknown services and principals (1)

- how can mutual trust be established?
  or a **calculated** risk be taken?
- both parties present **verifiable credentials** which provide:
  - a history of services given to previous clients
  - a history of client's payment for previous services
  as evidence of their trustworthiness

Mutually unknown services and principals (2)

- client and service agree a **certified contract** in advance
- after service and payment the contract is used as the basis for an **audit certificate** which both parties can use
- need a network of **trusted audit services** to validate audit certificates, c.f. certification authorities
- pedigree of certification service allows risk to be calculated – past experience, which domain, ….

work-in-progress …EU SECURE project is about to start

OASIS – talk overview

(Open Architecture for Secure Interworking Services)

- **brief introduction and motivation**
- **OASIS - model**
  - architecture
  - engineering
- **Electronic Health Records (EHR)**
  as an example application throughout
- **integration with PKI**
- **domains, services and clients**
- **more speculative ideas on trust**