GLAAAS

Global Authentication, Authorization, and Auditing System

Logical Requirements for Access Control in a Totally Federated Environment

Robert J. Robbins
Fred Hutchinson Cancer Research Center
rrobbins@fhcrc.org

GLAAAS

Global Authentication, Authorization, and Auditing System

Logical Requirements for Access Control in a Totally Federated Environment

http://www.esp.org/rjr/RJR-CAMPMed.pdf

Robert J. Robbins
Fred Hutchinson Cancer Research Center
rrobbins@fhcrc.org

Abstract

Much biomedical research is carried out collaboratively across institutional boundaries. The computer infrastructure to support this research must often implement security in a manner that cannot (and should not) depend upon the enterprise security of any one institution.

In our experience, requirements analysis for a totally federated access control system shows the need for some interesting properties, such as the need to

(1) implement both groups (aggregations of human beings) and roles (aggregations of permitted actions),

(2) define formal authorization as “explicitly allowing members of group A to act in role B on resource C", where the individuals, groups, roles, and resources may all be located in different enterprises and be operated wholly independently,

(3) support the idea of formal deauthorization, defined as “explicitly prohibiting members of group A to act in role B on resource C", and

(4) support "clarity of roles", defined as ensuring that, at any one time, a user be permitted to act in one and only one role on a resource.

We believe that a properly implemented federated access-control system should, wherever possible, also provide capabilities to support federated usage auditing. We also argue that an enterprise-centric security model can be easily derived from a federation-centric model, while the converse is very difficult. Therefore, we suggest that developers of security systems would benefit from attending to the security needs of federations.

Abstract

Much biomedical research is carried out collaboratively across institutional boundaries. The computer infrastructure to support this research must often implement security in a manner that cannot (and should not) depend upon the enterprise security of any one institution.

In our ex eed for some

(1) in ed a

(2) d rent e

(3) s up A

(4) s ct in o

We believe sible, also provide capabilities to support federated usage auditing. We also argue that an enterprise-centric security model can be easily derived from a federation-centric model, while the converse is very difficult. Therefore, we suggest that developers of security systems would benefit from attending to the security needs of federations.

NOTE: This presentation will deal only with a LOGICAL specification of what services and functionality could be useful in meeting access-control needs in a totally federated environment. We will not consider any technical details of how such logical processes could be implemented or what it would take to ensure that such logical processes would operate in a genuinely secure manner.

Issues to be Covered

- Background
- Federation is Essential
- Federation is Different (& Hard)
- All Components, All the Time
- Making it work
  - Logical Simplicity
  - Social Scalability
- GLAAAS as a Model (Robust Straw Man)
- GLAAAS in Action

Background

Background

- Fred Hutchinson Cancer Research Center
  - Independent biomedical research organization
  - 2500 employees
  - Many institutional relationships with other organizations
  - Researchers collaborate outside our organization
  - Much diversity within the organization
    - Four research divisions
    - Multiple research programs
    - 25 IT departments

Background

- Fred Hutchinson Cancer Research Center
  - Is a research-only organization
  - Is a one-third partner in a metropolitan-area cancer care alliance (SCCA)
  - SCCA outpatient clinic is on our campus
  - SCCA inpatient clinics are at UW & CHRMC
  - SCCA IT support comes from FHCRC, UW, and CHRMC

Background

- Robert J. Robbins
  - VP/IT at FHCRC
  - PhD biologist
  - Experience in community information infrastructure
    - NSF: first program officer for database activities (BIO)
    - GDB: director, informatics core
    - DOE: genome program information infrastructure
  - Biases
    - Database bigot
    - Even bigger TCP/IP bigot
    - Believer in decentralized components

Personal Beliefs

- An IT professional must have some knowledge of
  - Systems analysis
  - Algorithms and programming
  - Operating systems - principles and design
  - Database theory and design
  - Networking internals and design

Personal Beliefs

- Downsizing a superset solution for a subset problem is usually easy.

Personal Beliefs

- Downsizing a superset solution for a subset problem is usually easy.
- Upsizing a subset solution to a superset problem is hard, sometimes impossible.

Personal Beliefs

- Downsizing a superset solution for a subset problem is usually easy.
- Upsizing a subset solution to a superset problem is hard, sometimes impossible.
- Therefore, it's a good idea to know the ultimate size of your problem before going too far in the direction of a solution.

Federation is Essential

Federation is Essential

- Biomedical Research Occurs in a Distributed Manner

Federation is Essential

- Biomedical Research Occurs in a Distributed Manner
- Biomedical Research Demands Secure Information Infrastructure (criminal penalties apply when security is not met)

Federation is Essential

- Biomedical Research Occurs in a Distributed Manner
- Biomedical Research Demands Secure Information Infrastructure (criminal penalties apply when security is not met)
- Biomedical Research Needs a Federated Approach to Security and Access Control

Federation is Different (& Hard)

Federation is Different (& Hard)

- Security and Access Control Systems are the means by which the people who are in charge enforce their decisions about about who should and who should not have access to the enterprise's computing systems.

Federation is Different (& Hard)

- Security and Access Control Systems are the means by which the people who are in charge enforce their decisions about about who should and who should not have access to the enterprise's computing systems.
- In a truly federated environment, NO ONE IS IN CHARGE and THERE IS NO ENTERPRISE – there is no "privileged center" to the system.

Federation is Different (& Hard)

- Security and Access Control Systems are the means by which the people who are in charge

A federated security model is NOT just a security model for a multi-site enterprise.

- In a truly federated environment, NO ONE IS IN CHARGE and THERE IS NO ENTERPRISE – there is no “privileged center” to the system.

Federation is Different (& Hard)

Q: If NO ONE IS IN CHARGE, then how do we build a security and access control system?

Federation is Different (& Hard)

Q: If NO ONE IS IN CHARGE, then how do we build a security and access control system?

A: By developing a grid of components that can be used totally independently, but which can also be integrated in subsets to deliver virtual security and access control systems for virtual organizations that choose to use the components.

Federation is Different (& Hard)

If all of the computers in one “virtual” organization happen to be run by the central IT department of one enterprise, an enterprise solution falls out of the federated model as a trivial exercise in parameter setting.

Federation is Different (& Hard)

If all of the computers in one “virtual” organization happen to be run by the central IT department of one enterprise, an enterprise solution falls out of the federated model as a trivial exercise in parameter setting.

Conversely, evolving an enterprise solution into a federated solution is hard, if not impossible.

All Components, All the Time

All Components, All the Time

- In a truly federated environment, security and access control depend upon the availability of technically secure components that can be deployed in any way a user chooses (so long as the usage matches the technical specifications for the components).

All Components, All the Time

- In a truly federated environment, security and access control depend upon the availability of technically secure components that can be deployed in any way a user chooses (so long as the usage matches the technical specifications for the components).
- Users are free to use the components in as sophisticated (or as stupid) a manner as they choose.

All Components, All the Time

- In database design, one should always model the data at the finest used resolution. That is, if a use case requires that a data element be parsed into subcomponents, then decompose that data element into finer pieces.

All Components, All the Time

- In database design, one should always model the data at the finest used resolution. That is, if a use case requires that a data element be parsed into subcomponents, then decompose that data element into finer pieces.
- When designing a federated security model, one should devise the components at the finest used resolution. That is, if a use case requires that a service be delivered independently, then develop that service as a stand-alone component.

Possible Independent Components

- Identity Management
- Group Membership Management
- Authentication
- Authorization (assignment of permissions)
- Authorization (real time access control)
- Auditing
- More…

Making it Work

Logical Simplicity

Logical Simplicity

- In a federated, component-based environment, the biggest challenge is managing complexity.
- This requires a commitment to simplicity.
- Components must be entirely self-contained.
- All inter-component communication occurs only through well defined interfaces.
- Systems must be designed to accommodate change.

Assumptions

- Many use case requirements across the federation will be inconsistent and some will be genuinely contradictory.
- The federation must work anyway.
- The only certainty is uncertainty.
- Design must occur at a high level of abstraction.
- Refactoring is a constant requirement.

Making it Work

Social Scalability

Social Scalability

- In a truly federated environment, long term success for a federated security model will depend upon social scalability.
- Social scalability CANNOT be achieved through normative pronouncements.
- Experience suggests that social scalability is best achieved through a combination of pure laissez faire individualism and social consequences.

Social Consequences

- Every individual is free to do whatever he/she chooses.

Social Consequences

- Every individual is free to do whatever he/she chooses.
- Every other individual is free to respond however he/she chooses.

Social Consequences

- Every individual is free to do whatever he/she chooses.
- Every other individual is free to respond however he/she chooses.
- Interactive relationships then sort things out.

Social Consequences

- Every individual is free to do whatever he/she chooses.
- Every other individual is free to respond however he/she chooses.
- Interactive relationships then sort things out.
- Examples:

  One cuts, the other chooses.

Social Consequences

- Every individual is free to do whatever he/she chooses.
- Every other individual is free to respond however he/she chooses.
- Market relationships then sort things out.
- Examples:

  Caller IDs

Social Consequences

- Every individual is free to do whatever he/she chooses.
- Every other individual is free to respond however he/she chooses.
- Market relationships then sort things out.
- Examples:

  You are free to run your systems in as stupid and insecure manner as you choose; I am free to refuse to have anything to do with your systems.

Social Scalability: Required Reading

Alexander Hamilton

James Madison

John Jay

The Federalist Papers

Social Scalability: Required Reading

Alexander Hamilton

James Madison

John Jay

The Federalist Papers

There is no better source of ideas on how to build systems that work in a decentralized social environment.

Remember, you can't change human nature, so you must design systems that work **despite** human nature.

Social Scalability: Required Reading

Ale
Ja
Jo

THEOREM:

When there is no authority to **compel** participation in standard systems, then one must **entice** participation in standard systems.

Social Scalability: Required Reading

Ale
Ja
Jo

COROLLARY:

Pushing a wet noodle up a straw is hard.

Sucking a wet noodle up a straw is easy.

GLAAAS

Federation Requirements

- There is NO central enterprise.
- Everything is (potentially) decentralized:
  - Identity Management
  - Group Membership
  - Authentication
  - Authorization
  - Auditing
- Participation is Voluntary
- Solutions Must Scale

Groups vs. Roles

- Groups are collections of people
- Criteria for membership in a group is strictly up to the manager of that group (e.g., could be “officers of company X” or “physicians with attending privileges at hospital Z” or “people whose birthday is a prime number”)
- Management of group membership can be done informally or formally (i.e., with an audit trail)

Groups vs. Roles

- Roles are aggregations of permitted actions that a user may take on a computer resource (e.g., the role of standard user or superuser or DBA)
- Roles are associated with computer resources (e.g., the role of standard user on computer X)
- The manager of a resource determines what roles are to be made available on the resource.

Authorization

- Authorization is the granting of permission from members of Group X to act in Role Y on Resource Z
- The authority to grant permissions on Resource Z resides with the “manager” of resource Z.

De-Authorization is Needed

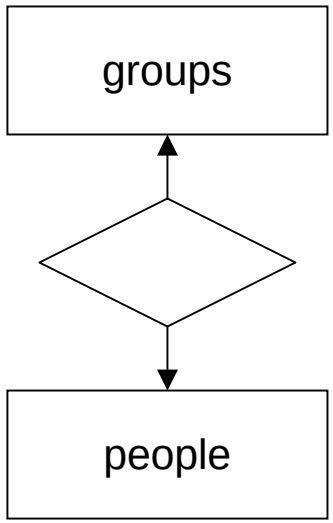
- De-Authorization is the prohibition of members of Group X to act in Role Y on Resource Z
- The authority to define de-authorizations on Resource Z resides with the “manager” of resource Z.

De-Authorization is Needed

- De-Authorization is the prohibition of members of Group X to act in Role Y on Resource Z
- The authority to define de-authorizations on Resource Z resides with the “manager” of resource Z.

This addresses both a technical problem (latency of information propagation in a federation) and a social problem (I might trust you to say who I should let in, but I reserve the right to determine who I’ll keep out).

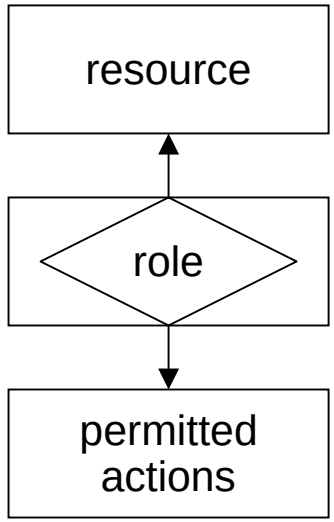
Groups



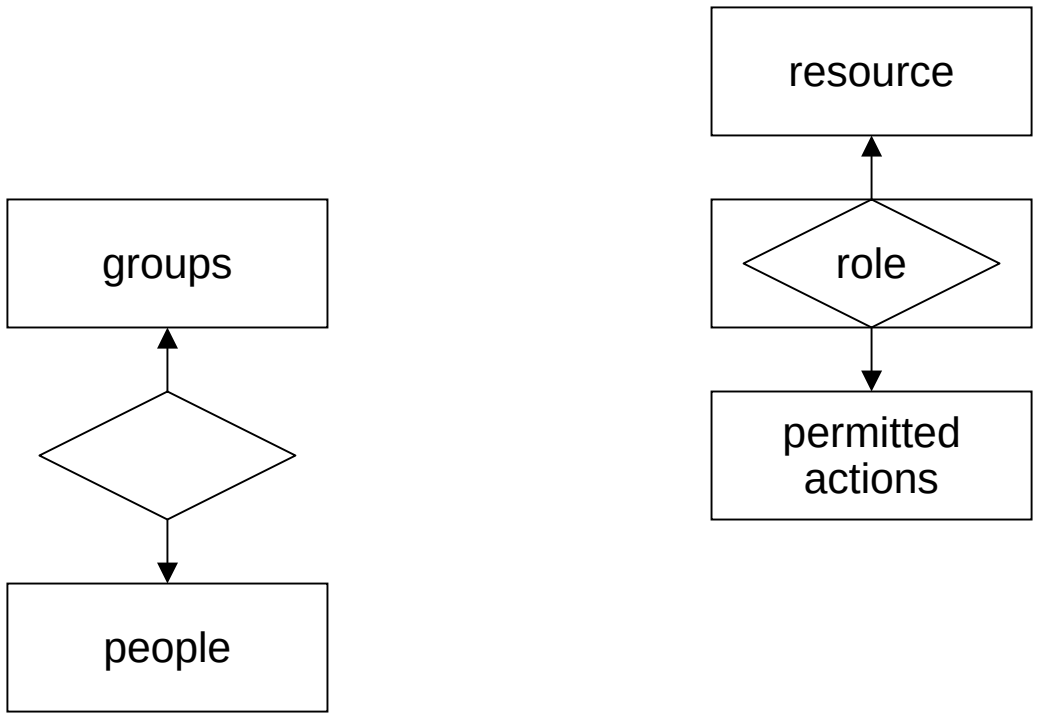
- Groups are collections of people
- Criteria for membership in a group is strictly up to the manager of that group (e.g., could be “officers of company X” or “physicians with attending privileges at hospital Z” or “people whose birthday is a prime number”)
- Management of group membership can be done informally or formally (i.e., with an audit trail)

Roles

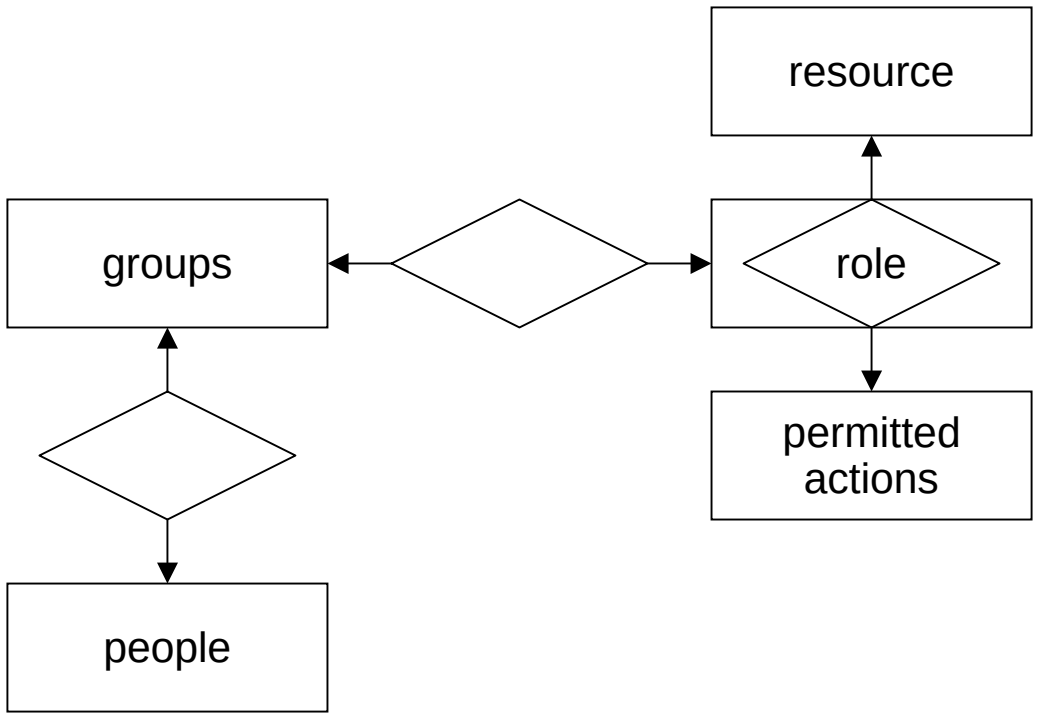
- Roles are aggregations of permitted actions that a user may take on a computer resource (e.g., the role of standard user or superuser or DBA)
- Roles are associated with computer resources (e.g., the role of standard user on computer X)
- The manager of a resource determines what roles are to be made available on the resource.



Authorization Joins Groups & Roles



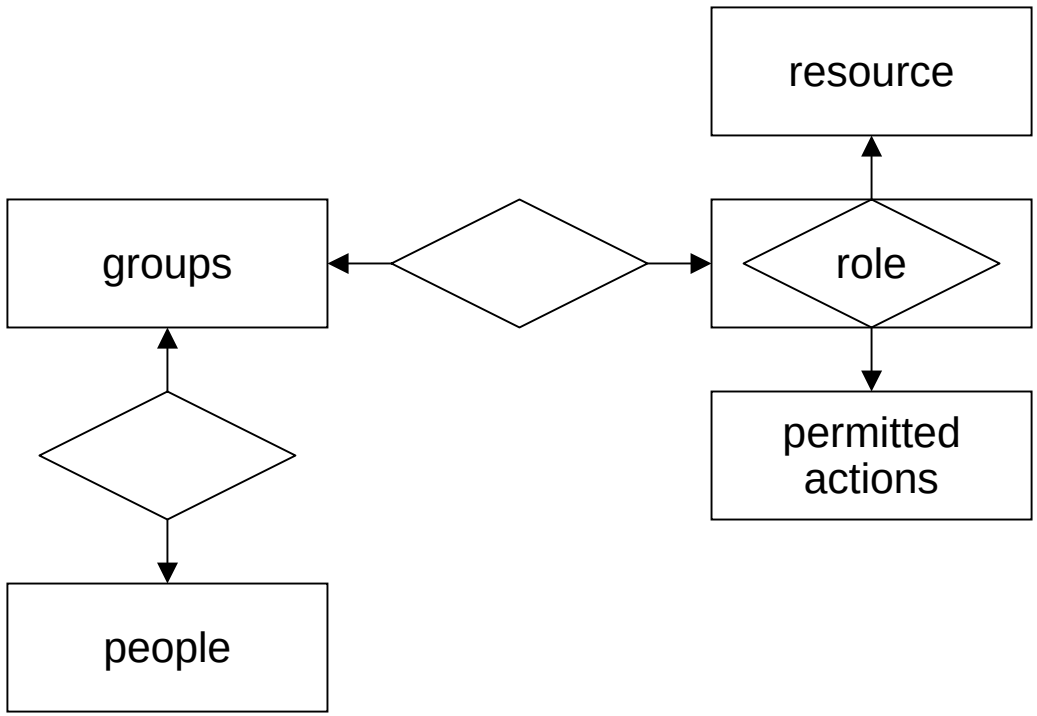
Authorization Joins Groups & Roles



Prior authorization occurs when a resource manager grants permission to members of a Group X to act in Role Y on Resource Z.

Real-time authorization occurs when a user requesting access to a resource is determined to satisfy a prior-authorization rule set.

Authorization Joins Groups & Roles



NOTE: In an enterprise-free federation, it is not possible (indeed, it is inconceivable) that group membership in any particular group could always control the permission to act in a particular role on an arbitrary resource. Therefore, in a federation **IT IS ESSENTIAL THAT A CLEAR LOGICAL AND TECHNICAL DISTINCTION BE MADE BETWEEN THE CONCEPTS OF GROUPS AND ROLES.**

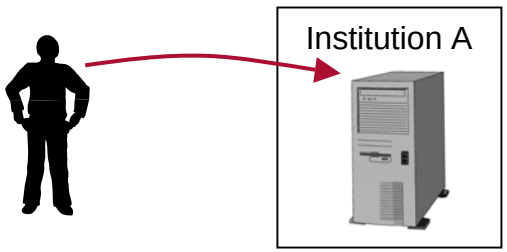
GLAAAS In Action

GLAAAS in Action

Institution A

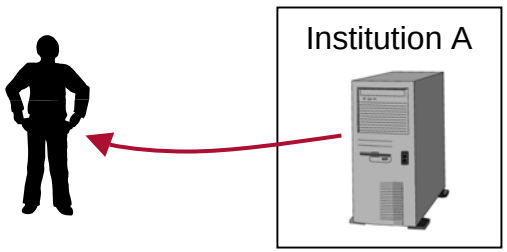
Institution A maintains a database resource associated with a multi-site clinical trial head-quartered elsewhere. Access to the database is tightly controlled according to rules based on groups to which individual requesting access belongs.

GLAAAS in Action



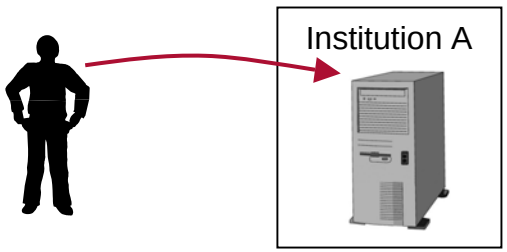
Dr. Jones attempts to access the research database maintained at Institution A.

GLAAAS in Action



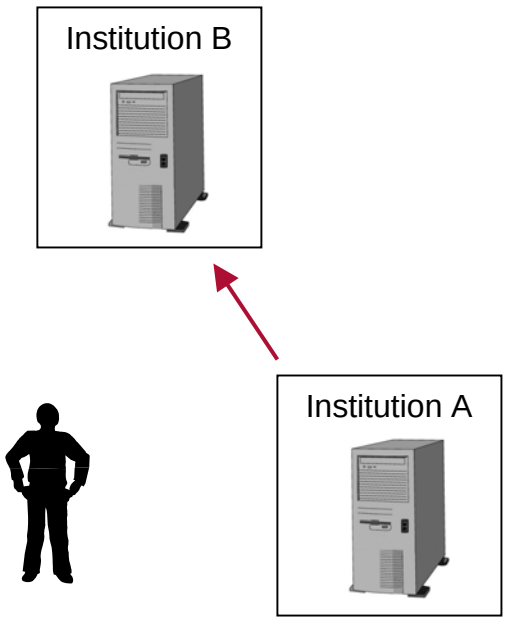
The database resource responds by asking, WHO ARE YOU AND WHERE ARE YOU FROM?

GLAAAS in Action



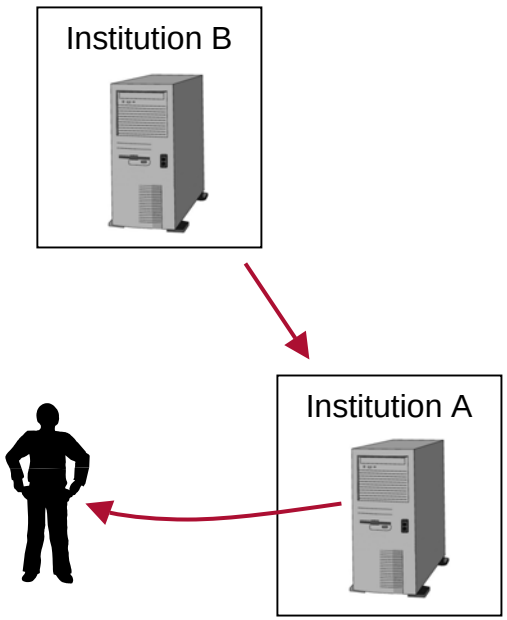
Dr. Jones replies, I AM DR JONES FROM INSTITUTION B.

GLAAAS in Action



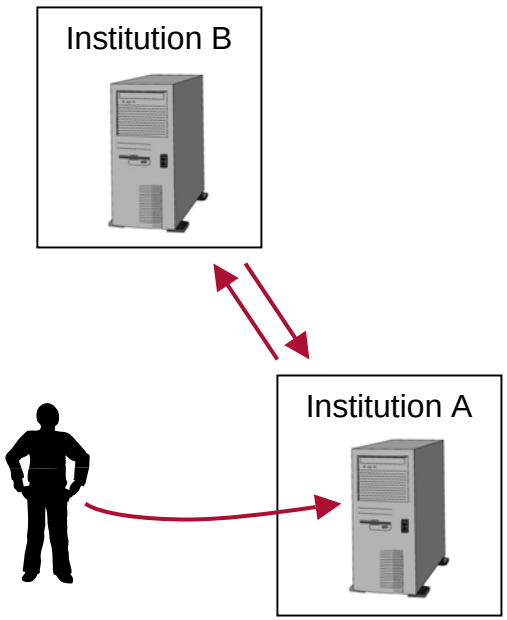
The database resource asks Institution B, WHAT INFORMATION DO I NEED TO COLLECT TO AUTHENTICATE DR JONES?

GLAAAS in Action



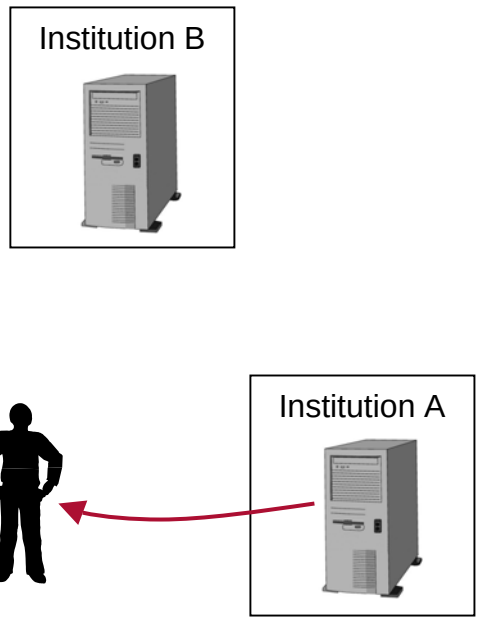
Institution B sends appropriate information and the database resource presents Dr. Jones with a login interface.

GLAAAS in Action



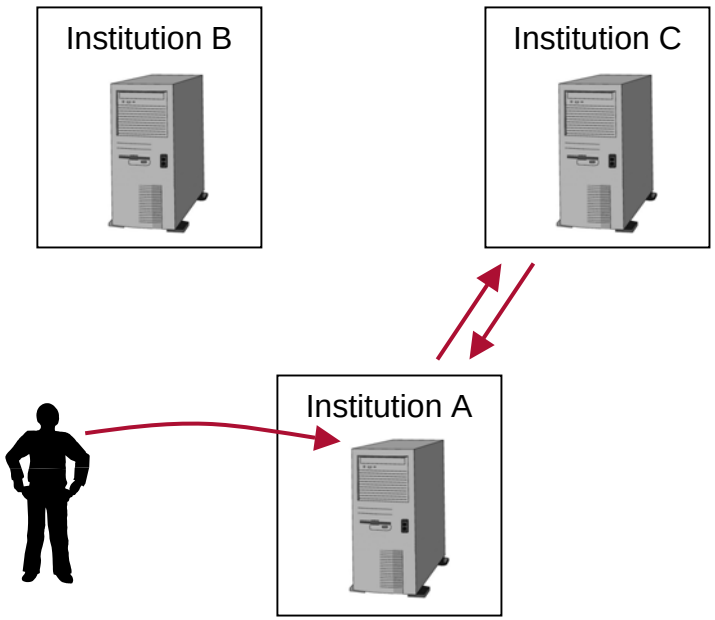
Jones responds to the login interface, A sends the information to B, and B responds: THAT IS OUR DR JONES.

GLAAAS in Action



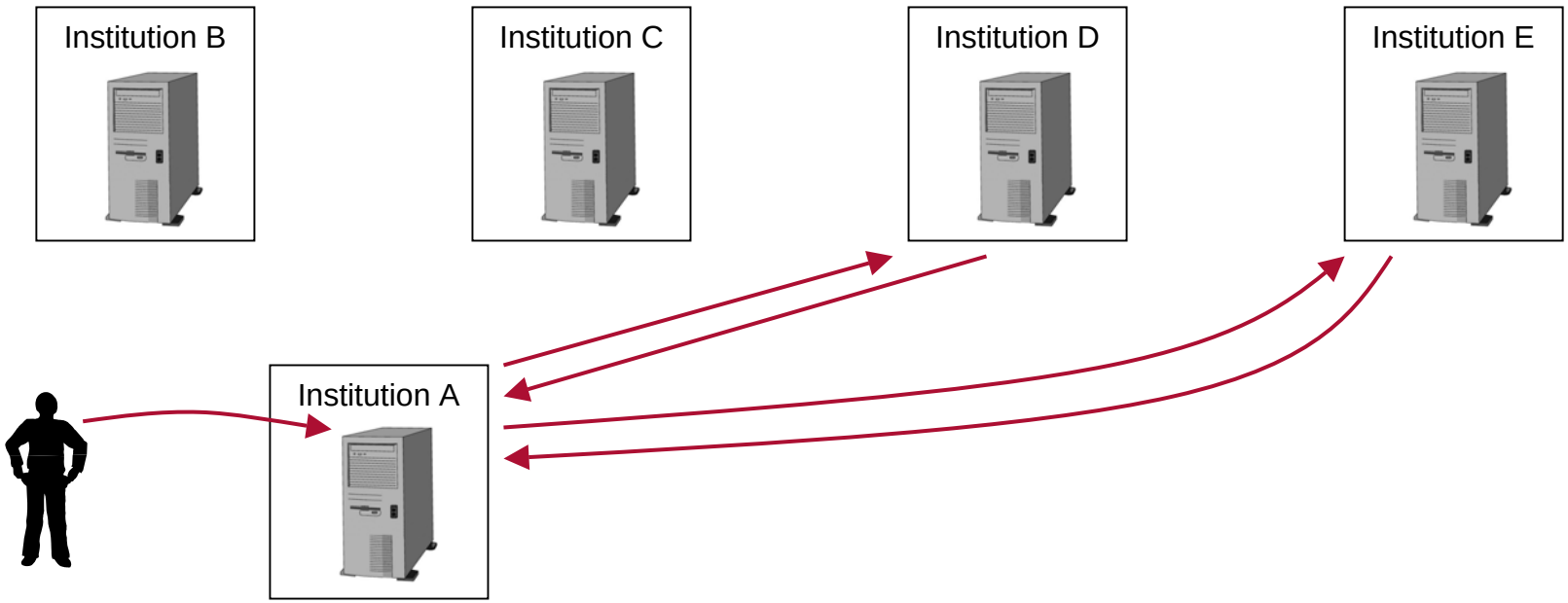
The database resource checks its authorization information and determines that users can access the database in several different roles, including GUEST FACULTY, RESEARCH FACULTY, and DBA. The resource asks Dr. Jones to specify the role he wishes to use.

GLAAAS in Action



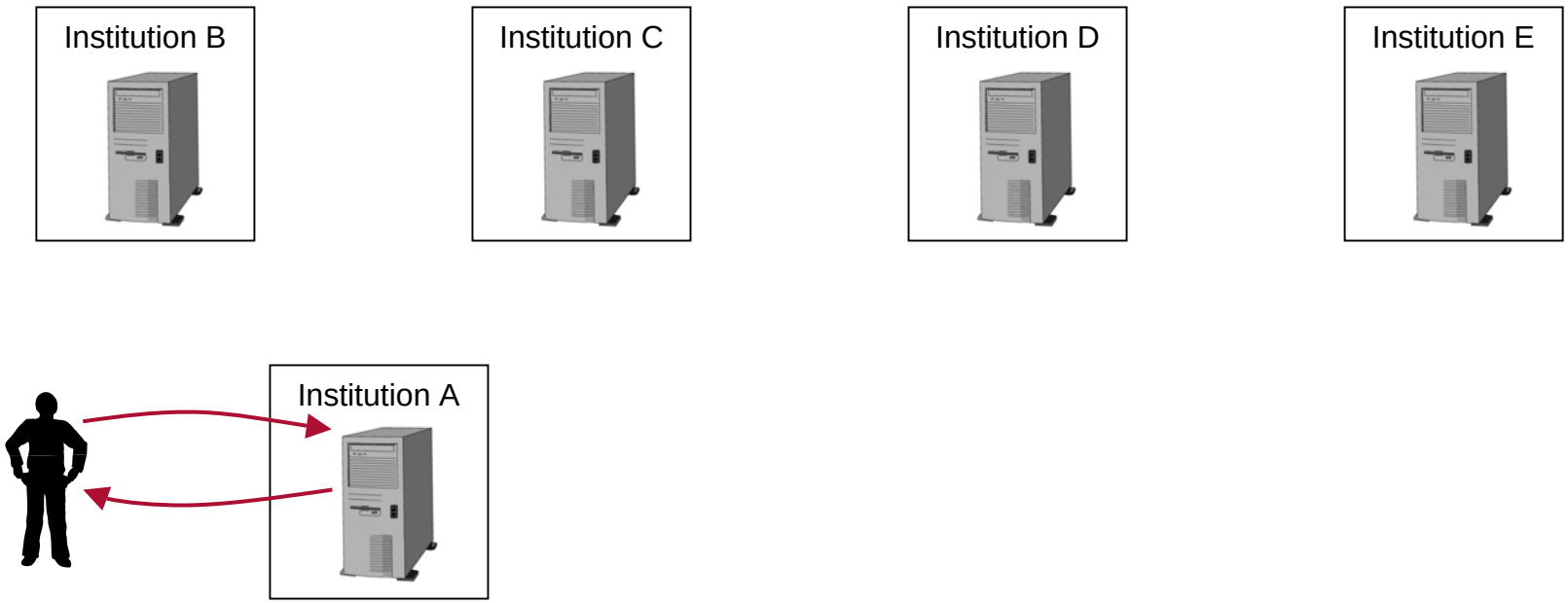
Jones responds: RESEARCH FACULTY. The database resource knows that the group-membership rule sets governing access to the clinical-trial resources are maintained at Institution C. The database resource queries the rule-server at C to obtain the latest rule set.

GLAAAS in Action



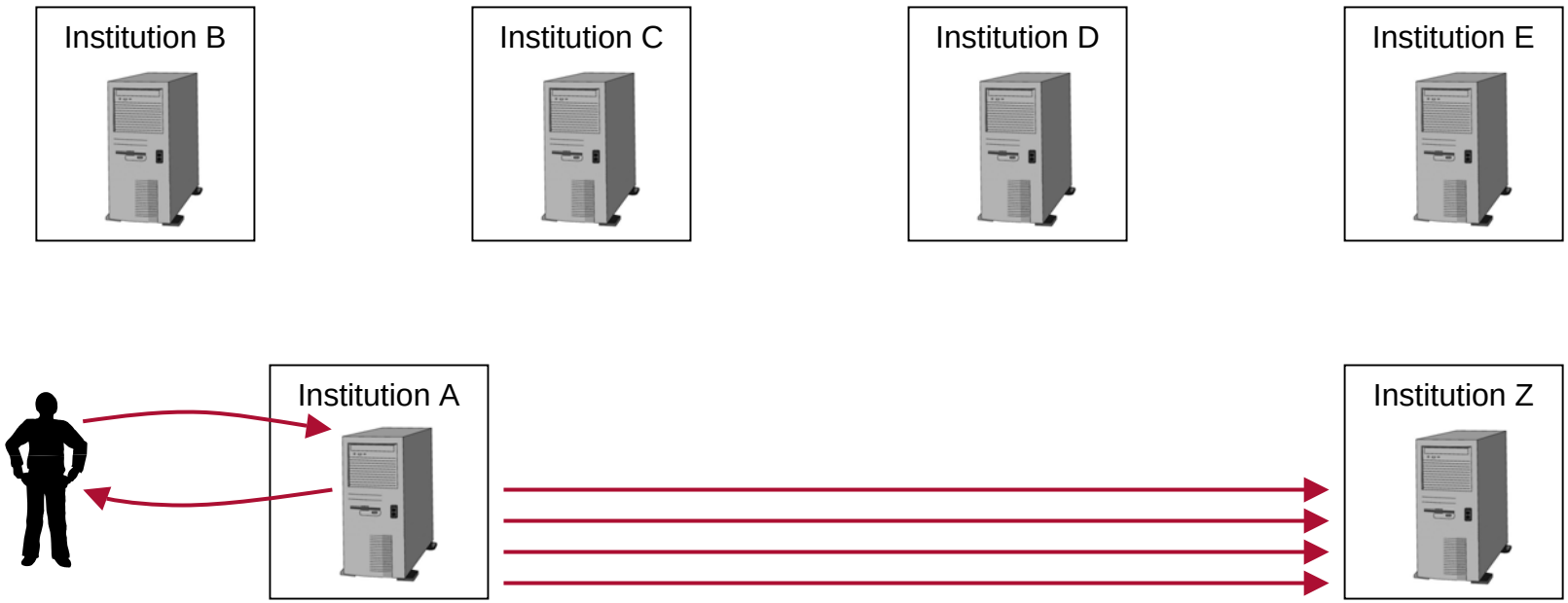
The rules show that the role is PERMITTED to individuals who are in the APPROVED FACULTY group maintained at the clinical trial headquarters at Institution D. The rules also stipulate that the role is EXPLICITLY PROHIBITED for individuals who are in the CONFLICT OF INTEREST group maintained by a watchdog organization at Institution E.

GLAAAS in Action



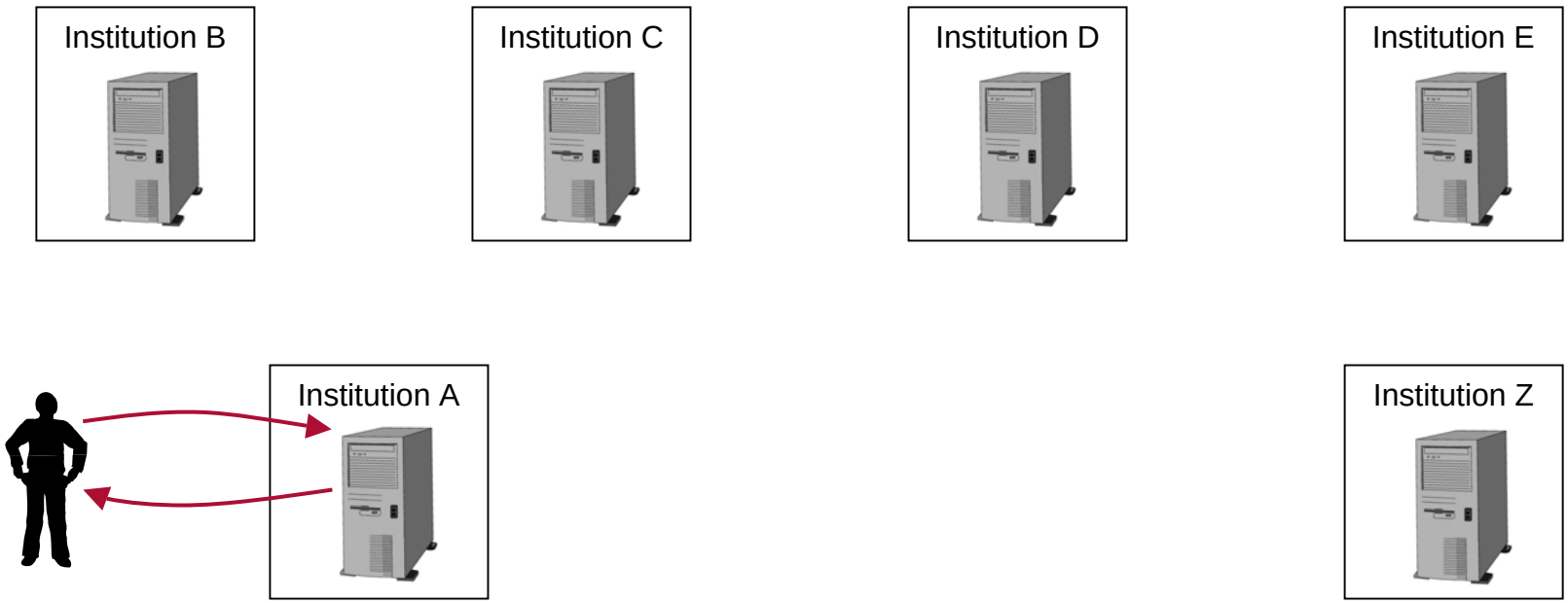
Jones is a member of the permitted group and he is not a member of the prohibited group. Therefore, he is authorized to access the database in the role of RESEARCH FACULTY. To decide whether or not to allow Jones in, the database resource used information maintained at four other, independent organizations. The decision to use these other resources was a local decision.

GLAAAS in Action



According to the auditing rules governing the database, Jones' request to access the database, his authorization to access the database, and all of his activities while accessing the database are logged in a logging system maintained at Institution Z. Now five other institutions have been involved in permitting and tracking Jones' use of the database resource.

GLAAAS in Action



Although multiple resources were involved in the access-control process, the logical was simple: (1) determine who is requesting access, (2) determine the roles and rule sets governing access, (3) determine the user's membership in the relevant groups, (4) decide to grant or prohibit permission based on a simple Boolean evaluation over a rule set, and (5) log all activities.

CAMP Med

http://www.esp.org/rjr/RJR-CAMPMed.pdf

EXTRAS

Biomedical Research is Special

Biomedical Research is Special

- Human beings are the users of the systems, so their identity should be managed in a common identity management system – the single sign-on system.
- Human beings are the subjects of the research, so their identity should be managed in a common identity management system – the master patient index.
- The single sign-on system and the master patient index should be able to interoperate so that James Jones, the researcher, can be determined to be identical with Jim Jones, the subject.