

# An Ontology-based Approach to the Formalization of Information Security Policies

Fernando Náufel do Amaral  
Carlos Bazílio  
Geiza Maria Hamazaki da Silva  
Alexandre Rademaker  
Edward Hermann Haeusler

TecMF  
Dept. of Informatics  
PUC-Rio, Brazil

VORTE 2006



## Project Anubis

### Participants

- ▶ **IS Consulting Firm** ⇒ Experienced at developing and implementing tools and techniques for Information Security and Risk Analysis. Strong presence in the marketplace.
- ▶ **TecMF** ⇒ Experienced at developing and using logic- and formal-semantic-based techniques, languages and frameworks. Intensional programming (TXL, XSLT, MAUDE, etc).

## Project Anubis

### Demands

- ▶ **IS Consulting Firm** ⇒ Rethink / refactor / adapt a proprietary tool for Risk Analysis and Information Security
- ▶ **TeCMF** ⇒ Develop case studies and solutions for real-world, industrial-scale problems

## Working Environment

### Main Concepts in Information Security

- ▶ Standards, Control Objectives
- ▶ Security Policies, Actions, Security Controls
- ▶ The big picture

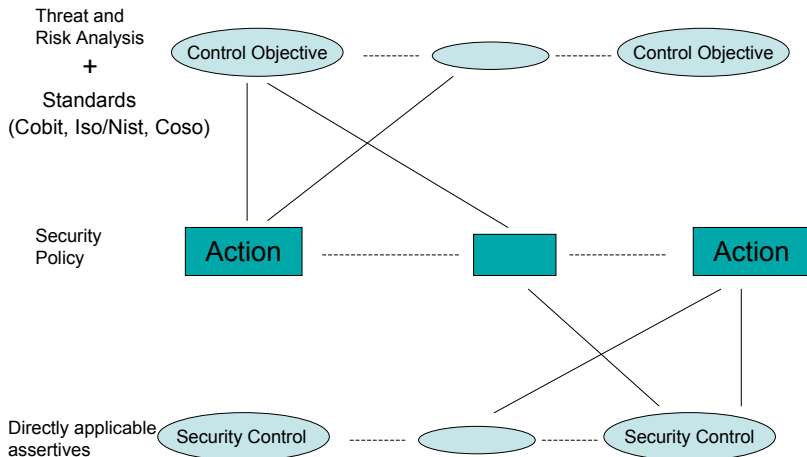
## Standards

- ▶ Public documents in normative text
- ▶ Set of Control Objectives to be accomplished by the organization desiring a higher level of security
- ▶ State what should be achieved at a higher level of abstraction
- ▶ Control-based × threat-based approach to security

## Security Policies

- ▶ The organization's Security Policy is implemented through a set of Actions
- ▶ Actions should achieve the Control Objectives and protect the organization against potential threats
- ▶ Actions are implemented by a set of Security Controls
- ▶ Security Controls are low-level technical measures that can be directly observed / implemented

## The Security Landscape Nowadays



## Computer-Aided Risk Analysis Tools

- ▶ Implemented from an initial set of empirically defined security controls
- ▶ Updated on demand
- ▶ Human-performed conformance analysis
- ▶ Designed in bottom-up fashion
- ▶ Represents the knowledge of an expert group
- ▶ Need for conformance
- ▶ Computer stores data and performs minimal inference
- ▶ Based on the needs of the market

## Computer-Aided Risk Analysis Tools

- ▶ Implemented from an initial set of empirically defined security controls
- ▶ Updated on demand
  - ▶ Human-performed conformance analysis
  - ▶ Designed in bottom-up fashion
- ▶ Represents the knowledge of an expert group
- ▶ Need for conformance
  - ▶ Computer stores data and performs minimal inference
  - ▶ Based on the needs of the market

## Computer-Aided Risk Analysis Tools

- ▶ Implemented from an initial set of empirically defined security controls
- ▶ Updated on demand
- ▶ Human-performed conformance analysis
- ▶ Designed in bottom-up fashion
- ▶ Represents the knowledge of an expert group
- ▶ Need for conformance
- ▶ Computer stores data and performs minimal inference
- ▶ Based on the needs of the market

## Computer-Aided Risk Analysis Tools

- ▶ Implemented from an initial set of empirically defined security controls
- ▶ Updated on demand
- ▶ Human-performed conformance analysis
- ▶ Designed in bottom-up fashion
- ▶ Represents the knowledge of an expert group
- ▶ Need for conformance
- ▶ Computer stores data and performs minimal inference
- ▶ Based on the needs of the market

# An Ontology-based Approach to Security Policies

## The Role of Formal Analysis of Systems / Theories

Provide techniques, tools and methodologies to work with the Principle of Falseability of Theories towards the (formal) validation of software and specifications

# An Ontology-based Approach to Security Policies

## Known Techniques / Tools

- ▶ Ad-hoc and systematic testing
- ▶ Simulation (including stochastic modeling)
- ▶ Logical and algebraic languages: theorem proving and model checking

# An Ontology-based Approach to Security Policies

## The Chosen Techniques / Tools

- ▶ **Declarative knowledge +**
- ▶ Conformance validation as an imperative feature
- ▶ = Logical approach with computer-aided validation cycle
- ▶ Description-logic-based ontology + set of tools for CAV
- ▶ Knowledge extraction from natural language texts (standards)
- ▶ Context-independent representation of utterances

# An Ontology-based Approach to Security Policies

## The Chosen Techniques / Tools

- ▶ Declarative knowledge +
- ▶ Conformance validation as an imperative feature
- ▶ = Logical approach with computer-aided validation cycle
- ▶ Description-logic-based ontology + set of tools for CAV
- ▶ Knowledge extraction from natural language texts (standards)
- ▶ Context-independent representation of utterances

# An Ontology-based Approach to Security Policies

## The Chosen Techniques / Tools

- ▶ Declarative knowledge +
- ▶ Conformance validation as an imperative feature
- ▶ = Logical approach with computer-aided validation cycle
- ▶ Description-logic-based ontology + set of tools for CAV
- ▶ Knowledge extraction from natural language texts (standards)
- ▶ Context-independent representation of utterances

# An Ontology-based Approach to Security Policies

## The Chosen Techniques / Tools

- ▶ Declarative knowledge +
- ▶ Conformance validation as an imperative feature
- ▶ = Logical approach with computer-aided validation cycle
- ▶ Description-logic-based ontology + set of tools for CAV
- ▶ Knowledge extraction from natural language texts (standards)
- ▶ Context-independent representation of utterances

# An Ontology-based Approach to Security Policies

## The Chosen Techniques / Tools

- ▶ Declarative knowledge +
- ▶ Conformance validation as an imperative feature
- ▶ = Logical approach with computer-aided validation cycle
- ▶ Description-logic-based ontology + set of tools for CAV
- ▶ Knowledge extraction from natural language texts (standards)
- ▶ Context-independent representation of utterances

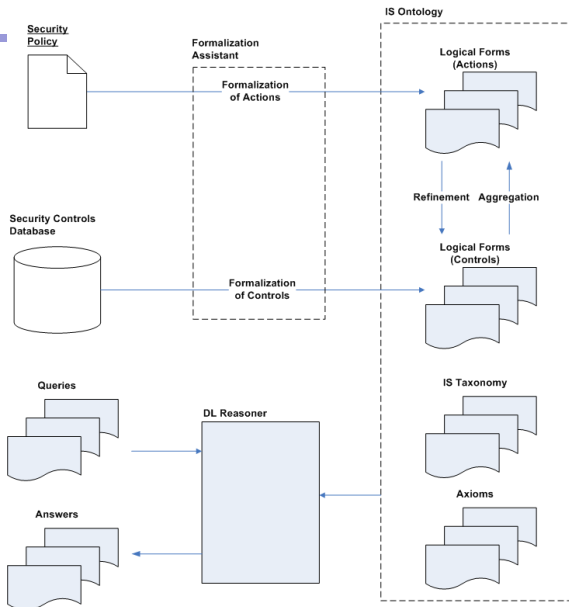
# An Ontology-based Approach to Security Policies

## The Chosen Techniques / Tools

- ▶ Declarative knowledge +
- ▶ Conformance validation as an imperative feature
- ▶ = Logical approach with computer-aided validation cycle
- ▶ Description-logic-based ontology + set of tools for CAV
- ▶ Knowledge extraction from natural language texts (standards)
- ▶ Context-independent representation of utterances

# An Ontology-based Approach to the Formalization of Information Security Policies

└ Main Goal: Computer-Aided Formulation and Validation of Security Policies



## The Front-End

The screenshot displays the 'Ontology Editor' application with several windows open:

- Text Window:** Contains the sentence "O sistema deve permitir acessar remotamente um serviço".
- Logical Form Window:** Shows a hierarchical tree structure of logical forms, including:
  - hasVerb:Desabilitar
  - hasTheme:Recurso
    - isOfType:Permitir
      - hasTheme:AcessarRemotamente
        - hasTheme:Servico
        - hasPurpose:Administrar
- Action0005
- hasVerb:Configurar

- Edit Action Window:** Shows the same sentence with "permitir" highlighted. Below it is a list of concepts:
- Concept
  - Acessar
  - AcessarRemotamente
  - Action
  - Administrar
  - ClienteSoftware
  - Entity
  - Politica
- Formula Window:** Shows a tree structure of formulas:
- Terms
  - hasTheme:Sistema
  - isOfType:Permitir
    - hasTheme:AcessarRemotamente
      - hasTheme:Servico

## Looking into the ontology

- ▶ *AdministerRemotely*  $\sqsubseteq$  *AccessRemotely* and *NetwareServer*  $\sqsubseteq$  *System* are assertions in the IS taxonomy
- ▶ “Configuring X to achieve Y” is equivalent to “Achieving Y” is asserted in the Axioms section of the ontology:  
 $\exists hasVerb.(Configure \sqcap \exists hasTheme.X \sqcap \exists hasPurpose.Y) \equiv \exists hasVerb.Y$

## Looking into the ontology

- ▶ *AdministerRemotely*  $\sqsubseteq$  *AccessRemotely* and *NetwareServer*  $\sqsubseteq$  *System* are assertions in the IS taxonomy
- ▶ “Configuring X to achieve Y” is equivalent to “Achieving Y” is asserted in the Axioms section of the ontology:  
 $\exists hasVerb.(Configure \sqcap \exists hasTheme.X \sqcap \exists hasPurpose.Y) \equiv \exists hasVerb.Y$

## Controls $\sqsubseteq$ Actions

- ▶ Action0002
- ▶ Control0001
- ▶ Control0001  $\sqsubseteq$  Action0002

## Action0002

*Configure every system to encrypt connections used for remote access to the system.*

*Action0002*  $\equiv$

$\exists hasVerb.(Configure \sqcap \exists hasTheme.System \sqcap$   
 $\exists hasPurpose.(Encrypt \sqcap \exists hasTheme.(NetworkConnect \sqcap$   
 $\exists isInstrumentOf.(AccessRemotely \sqcap \exists hasTheme.System))))$

## Controls $\sqsubseteq$ Actions

- ▶ Action0002
- ▶ Control0001
- ▶ Control0001  $\sqsubseteq$  Action0002

## Control0001

*Network traffic for the remote administration of the Netware server must be encrypted using SSL.*

*Control0001*  $\equiv$

$\exists hasVerb.(Encrypt \sqcap \exists hasTheme.NetworkTraffic \sqcap$

$\exists hasInstrument.SSL \sqcap \exists isInstrumentOf.$

$(AdministerRemotely \sqcap \exists hasTheme.NetwareServer))$

## Controls $\sqsubseteq$ Actions

- ▶ Action0002
- ▶ Control0001
- ▶ Control0001  $\sqsubseteq$  Action0002

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## *Control0001* $\sqsubseteq$ *Action0002*

Since “Encrypt the NetworkConnection” is the same as “Encrypt the NetworkTraffic”, NetwareServer is a System, and AdministerRemotely implies AccessRemotely, then

- ▶ Control0001, requiring that one
- ▶ Encrypt the NetworkTraffic using SSL in order to AdministerRemotely the NetwareServer, implies
- ▶ Encrypt the NetworkTraffic in order to AdministerRemotely the NetwareServer, and hence,
- ▶ Encrypt the NetworkTraffic in order to AccessRemotely a System, and hence,
- ▶ Encrypt the NetworkConnection in order to AccessRemotely a System, which conforms to
- ▶ Action0002, according to this detailed proof...

## Synonyms

$$\begin{aligned} \exists hasVerb.(Encrypt \sqcap \exists hasTheme.NetworkConnect) \\ \equiv \\ \exists hasVerb.(Encrypt \sqcap \exists hasTheme.NetworkTraffic) \end{aligned}$$

## Part of IS Taxonomy

*NetwareServer*  $\sqsubseteq$  *System*  
*AdministerRemotely*  $\sqsubseteq$  *AccessRemotely*



## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture

## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture

## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture

## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture

## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture

## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture

## Results – Obtained and Expected

- ▶ An architecture for the construction, validation and maintenance of knowledge bases in IS
  1. Assisted knowledge extraction from normative text
  2. Use of natural language in documenting the cycle of formal analysis of the knowledge base
  3. Integrated environment supporting version control of aspects of the knowledge base
- ▶ Use of Curry-Howard isomorphism to provide explanation of proofs
- ▶ Model checking and user support under development
- ▶ Domain-independent version of the architecture