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

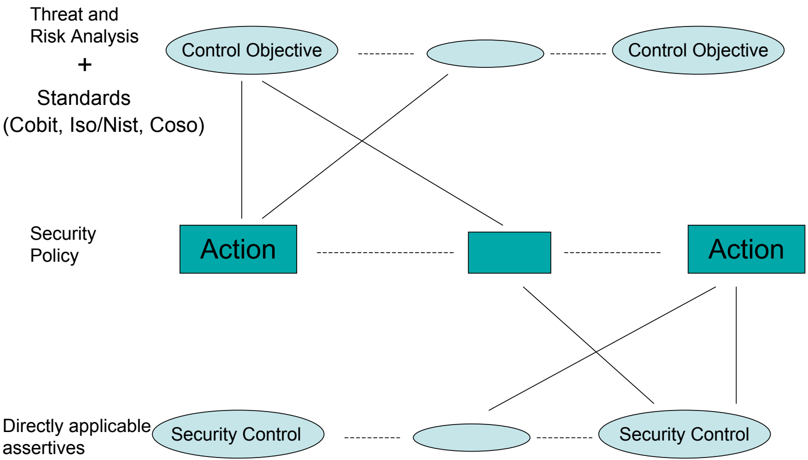
Standards

- 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 $\times$ 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

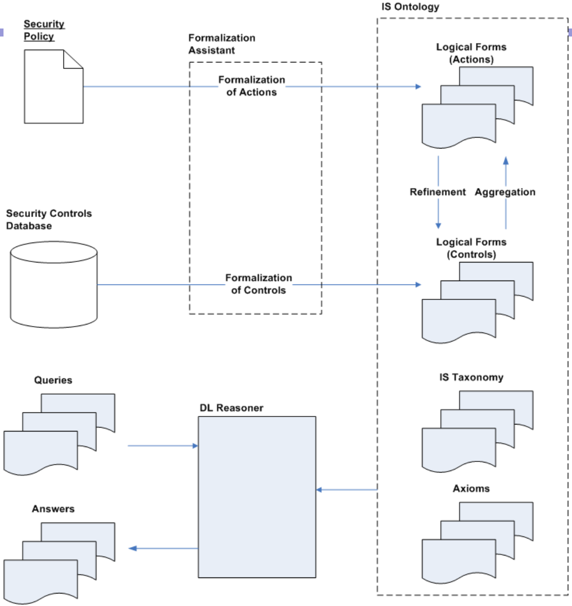
The Chosen Techniques / Tools

- 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

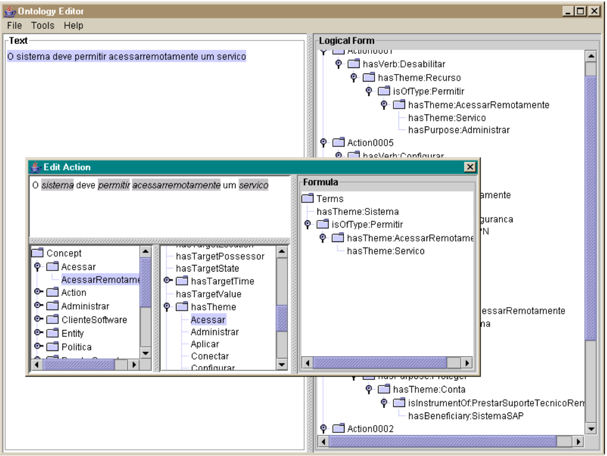
An Ontology-based Approach to Security Policies

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


Security Policy
Formalization Assistant
Formalization of Actions
IS Ontology
Logical Forms (Actions)
Refinement
Aggregation
Security Controls Database
Formalization of Controls
Logical Forms (Controls)
Queries
DL Reasoner
IS Taxonomy
Axioms
Answers

The Front-End



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

- $\underline{\text{Action0002}}$
- $\underline{\text{Control0001}}$
- $\underline{\text{Control0001}} \sqsubseteq \underline{\text{Action0002}}$

Action0002

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

$$\begin{aligned}&\mathit{Action0002} \equiv \\ &\ \exists \mathit{hasVerb}.(\mathit{Configure} \sqcap \exists \mathit{hasTheme}.\mathit{System} \sqcap \\ &\ \exists \mathit{hasPurpose}.(\mathit{Encrypt} \sqcap \exists \mathit{hasTheme}.(\mathit{NetworkConnect} \sqcap \\ &\ \exists \mathit{isInstrumentOf}.(\mathit{AccessRemotely} \sqcap \exists \mathit{hasTheme}.\mathit{System}))))\end{aligned}$$

PUC RIO

Controls $\sqsubseteq$ Actions

- Action0002
- Control0001
- Control0001 $\sqsubseteq$ Action0002

Control0001

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

$$\mathit{Control0001} \equiv \exists \mathit{hasVerb}.(\mathit{Encrypt} \sqcap \exists \mathit{hasTheme}.\mathit{NetworkTraffic} \sqcap \exists \mathit{hasInstrument}.\mathit{SSL} \sqcap \exists \mathit{isInstrumentOf}.(\mathit{AdministerRemotely} \sqcap \exists \mathit{hasTheme}.\mathit{NetwareServer}))$$

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

$$\exists hasVerb.(Encrypt \sqcap \exists hasTheme.NetworkConnect)$$
$$\equiv$$
$$\exists hasVerb.(Encrypt \sqcap \exists hasTheme.NetworkTraffic)$$

Part of IS Taxonomy

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{NetSvr \Rightarrow Sys}\ \text{ISTax-Seq}}{NetSvr^{hT} \Rightarrow sys^{hT}}\ \text{prom}}{(\exists hT.NetSvr) \Rightarrow sys^{hT}}\ \exists\text{-l}}{AdRem, (\exists hT.NetSvr) \Rightarrow Sys^{hT}}\ \text{weak}}{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow Sys^{ht}}\ \sqcap\text{-l}$$

$$\dfrac{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow Sys^{ht}}{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow (\exists hT.Sys)}\ \exists\text{-r}$$

$$\dfrac{\dfrac{\dfrac{}{AdRem \Rightarrow AcRem}\ \text{ISTax-Seq}}{AdRem, (\exists hT.NetSvr) \Rightarrow AcRem}\ \text{weak-l}}{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow AcRem}\ \sqcap\text{-l}$$

$$\dfrac{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow AcRem \qquad AdRem \sqcap (\exists hT.NetSvr) \Rightarrow (\exists hT.Sys)}{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow acRem \sqcap (\exists hT.Sys)}\ \sqcap\text{-r}$$

$$\dfrac{\dfrac{\dfrac{AdRem \sqcap (\exists hT.NetSvr) \Rightarrow acRem \sqcap (\exists hT.Sys)}{(AdRem \sqcap \exists hT.NetSvr)^{iO} \Rightarrow (acRem \sqcap \exists hT.Sys)^{iO}}\ \text{prom}}{(AdRem \sqcap \exists hT.NetSvr)^{iO} \Rightarrow (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \exists\text{-r}}{(\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \exists\text{-l}$$

$$\dfrac{(\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists iO.(acRem \sqcap \exists hT.Sys))}{(\exists hT.NetTr), (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \text{weak-l}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{NetTr \Rightarrow NetCon}\ \text{ISTax-Seq}}{NetTr^{hT} \Rightarrow NetCon^{hT}}\ \text{prom}}{NetTr^{hT} \Rightarrow (\exists hT.NetCon)}\ \exists\text{-r}}{(\exists hT.NetTr) \Rightarrow (\exists hT.NetCon)}\ \exists\text{-l}}{(\exists hT.NetTr), (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon)}\ \text{weak-l}$$

$$\dfrac{(\exists hT.NetTr), (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \qquad (\exists hT.NetTr), (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists iO.(acRem \sqcap \exists hT.Sys))}{(\exists hT.NetTr), (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \sqcap\text{-r}$$

$$\dfrac{\dfrac{\dfrac{(\exists hT.NetTr), (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}{(\exists hI.SSL), (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \text{weak-l}}{(\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \sqcap\text{-l}}{Ec, (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \text{weak-l}$$

$$\dfrac{\dfrac{}{Ec \Rightarrow Ec}\ \text{I-Seq}}{Ec, (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow Ec}\ \text{weak-l}$$

$$\dfrac{Ec, (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow Ec \qquad Ec, (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}{Ec, (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \sqcap\text{-r}$$

$$\dfrac{Ec, (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}{Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}\ \sqcap\text{-l}$$

$$\dfrac{Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)) \Rightarrow Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))}{(Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)))^{hV} \Rightarrow (Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))^{hV}}\ \text{prom}$$

$$\dfrac{(Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)))^{hV} \Rightarrow (Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))^{hV}}{\exists hV.(Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr))) \Rightarrow (Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))^{hV}}\ \exists\text{-l}$$

$$\dfrac{\exists hV.(Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr))) \Rightarrow (Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))^{hV}}{\exists hV.(Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)))) \Rightarrow \exists hV.(Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))}\ \exists\text{-r}$$

$$\dfrac{\exists hV.(Ec \sqcap (\exists hI.SSL) \sqcap (\exists hT.NetTr) \sqcap (\exists iO.(AdRem \sqcap \exists hT.NetSvr)))) \Rightarrow \exists hV.(Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))}{Control0001 \Rightarrow \exists hV.(Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys)))}\ \text{Naming}$$

$$\dfrac{}{\exists hV.(Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))) \Rightarrow Action0002}\ \text{LF-Axiom}$$

$$\dfrac{Control0001 \Rightarrow \exists hV.(Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))) \qquad \exists hV.(Ec \sqcap (\exists hT.NetCon) \sqcap (\exists iO.(acRem \sqcap \exists hT.Sys))) \Rightarrow Action0002}{Control0001 \Rightarrow Action0002}\ \text{cut}$$

A (New) Sequent Calculus for $\mathcal{ALC}$

$$\frac{}{\alpha \Rightarrow \alpha}$$

$$\frac{\Delta_1 \Rightarrow \Gamma_1, {}^{L_1}\alpha^{L_2} \quad {}^{L'_1}\alpha^{L'_2}, \Delta_2 \Rightarrow \Gamma_2 \quad \begin{array}{c} L_1 \approx L'_1 \\ L_2 \approx L'_2 \end{array}}{\Delta_1, \Delta_2 \Rightarrow \Gamma_1, \Gamma_2} \; cut$$

$$\frac{\Delta \Rightarrow \Gamma}{\Delta, \alpha \Rightarrow \Gamma} \; weak-l \qquad \frac{\Delta \Rightarrow \Gamma}{\Delta \Rightarrow \Gamma, \alpha} \; weak-r$$

$$\frac{\Delta_1, \alpha, \beta, \Delta_2 \Rightarrow \Gamma}{\Delta_1, \beta, \alpha, \Delta_2 \Rightarrow \Gamma} \; perm-l \qquad \frac{\Delta \Rightarrow \Gamma_1, \alpha, \beta, \Gamma_2}{\Delta \Rightarrow \Gamma_1, \beta, \alpha, \Gamma_2} \; perm-r$$

Results – Obtained and Expected

- An architecure 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 architecure 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 architecure 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 architecure 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

PUC RIO

Results – Obtained and Expected

- An architecure 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 architecure 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 architecure 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