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).

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

Motivation

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

Motivation

Working Environment

The Security Landscape Nowadays

Threat and Risk Analysis
+ Standards (Cobit, Iso/Nist, Coso)

Control Objective

Security Policy

Directly applicable assertives

Action

Security Control

Standards (Cobit, Iso/Nist, Coso)

Control Objective

Action
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 the Formalization of Information Security Policies

Motivation

The Big Picture

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 the Formalization of Information 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

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

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

Motivation

The Big Picture

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

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

The Front-End
Looking into the ontology

- \textit{AdministerRemotely} ⊑ \textit{AccessRemotely} and \textit{NetwareServer} ⊑ \textit{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:
  \[ \exists \text{hasVerb}. (\text{Configure} \sqcap \exists \text{hasTheme}. X \sqcap \exists \text{hasPurpose}. Y) \equiv \exists \text{hasVerb}. Y \]
Looking into the ontology

- **AdministerRemotely** ⊆ **AccessRemotely** and **NetwareServer** ⊆ **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:
  \[ \exists \text{hasVerb}. (Configure \sqcap \exists \text{hasTheme}. X \sqcap \exists \text{hasPurpose}. Y) \equiv \exists \text{hasVerb}. Y \]
An Ontology-based Approach to the Formalization of Information Security Policies

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

An Example

Controls □ Actions

- Action0002
- Control0001
- Control0001 □ Action0002
Action0002

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

Action0002 ≡

∃hasVerb.(Configure ⊓ ∃hasTheme.System ⊓ ∃hasPurpose.(Encrypt ⊓ ∃hasTheme.(NetworkConnect ⊓ ∃isInstrumentOf.(AccessRemotely ⊓ ∃hasTheme.System))))
An Ontology-based Approach to the Formalization of Information Security Policies

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

An Example

Controls □ Actions

- Action0002
- Control0001
- Control0001 □ Action0002
Control0001

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

Control0001 ≡
∃hasVerb.(Encrypt ⊓ ∃hasTheme.NetworkTraffic ⊓ ∃hasInstrument.SSL ⊓ ∃isInstrumentOf.
(AdministerRemotely ⊓ ∃hasTheme.NetwareServer))
An Ontology-based Approach to the Formalization of Information Security Policies

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

An Example

Controls ⊑ Actions

- Action0002
- Control0001
- Control0001 ⊑ Action0002
Control0001 ⊑ 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 ⊑ 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 ⊑ 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 ⊑ 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 ⊑ 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 ⊑ 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 ⊑ 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

\[ \exists \text{hasVerb.}(Encrypt \sqcap \exists \text{hasTheme}.\text{NetworkConnect}) \equiv \exists \text{hasVerb.}(Encrypt \sqcap \exists \text{hasTheme}.\text{NetworkTraffic}) \]
An Ontology-based Approach to the Formalization of Information Security Policies

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

An Example

Part of IS Taxonomy

$NetwareServer \subseteq System$

$AdministerRemotely \subseteq AccessRemotely$
An Ontology-based Approach to the Formalization of Information Security Policies

- Main Goal: Computer-Aided Formulation and Validation of Security Policies
- An Example
A (New) Sequent Calculus for \( \mathcal{ALC} \)

\[
\frac{\alpha \Rightarrow \alpha}{\Delta_1 \Rightarrow \Gamma, \ell \cdot \alpha \ell, \Delta_2 \Rightarrow \Gamma_2}
\]

\[
\frac{L_1 \approx L'_1 \quad L_2 \approx L'_2}{\Delta_1, \Delta_2 \Rightarrow \Gamma_1, \Gamma_2}
\]

\[
\frac{\Delta \Rightarrow \Gamma}{\Delta, \alpha \Rightarrow \Gamma}
\]

\[
\text{weak} - l
\]

\[
\frac{\Delta \Rightarrow \Gamma}{\Delta \Rightarrow \Gamma, \alpha}
\]

\[
\text{weak} - r
\]

\[
\frac{\Delta_1, \alpha, \beta, \Delta_2 \Rightarrow \Gamma}{\Delta_1, \beta, \alpha, \Delta_2 \Rightarrow \Gamma}
\]

\[
\text{perm} - l
\]

\[
\frac{\Delta \Rightarrow \Gamma_1, \alpha, \beta, \Delta_2 \Rightarrow \Gamma_2}{\Delta \Rightarrow \Gamma_1, \beta, \alpha, \Gamma_2}
\]

\[
\text{perm} - r
\]
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
An Ontology-based Approach to the Formalization of Information Security Policies

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

Concluding Remarks

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