CITY UNIVERSITY
LONDON
EST 1894

Analyzing and Enforcing Security Mechanisms on Requirements Specifications

Tong Li[1], Jennifer Horkoff[2] and John Mylopoulos[1]
[1] University of Trento, Trento, Italy
[2] City University, London, UK

The 21th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2015)
Essen, Germany
March 24, 2015

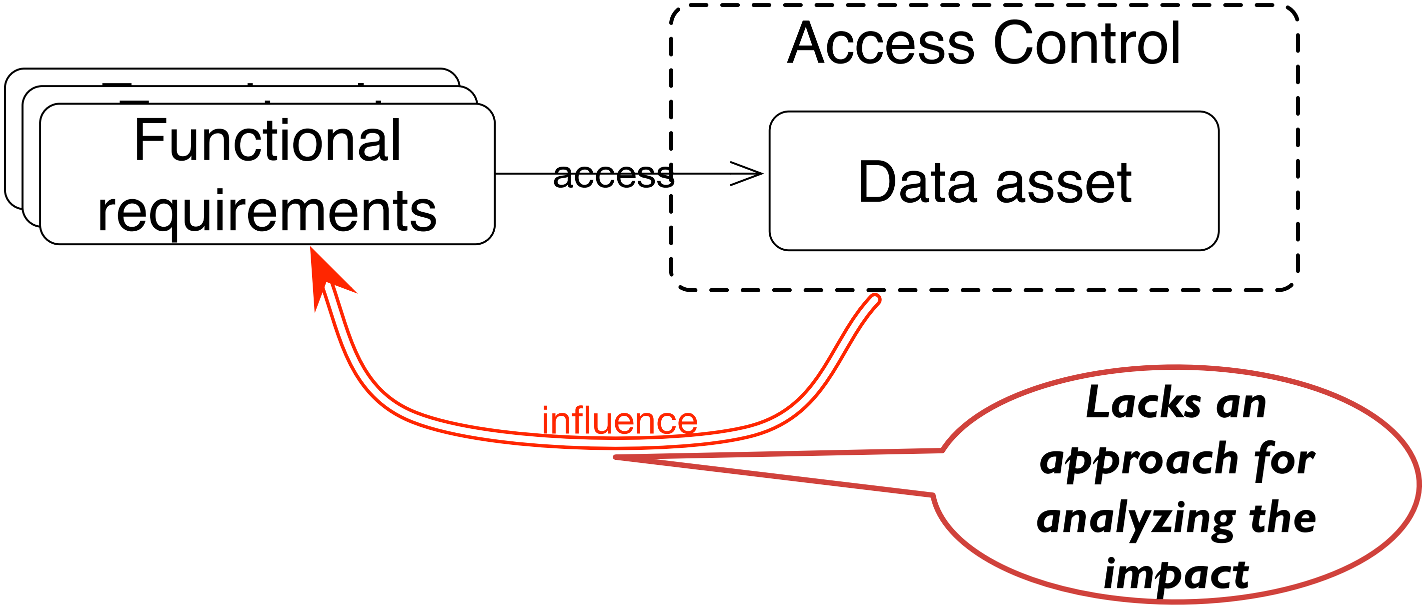
Essen, Germany, March 23-26, 2015
REFSQ
21st Intl. Working Conference on Requirements Engineering: Foundation for Software Quality
2015

Outline

- Background and Motivation
- Baseline
- Research Proposal
  - An Enriched Requirements Specification
  - Modeling Security Mechanisms
  - Analyzing the Impact of Security Mechanisms
- Evaluation
  - Expressiveness: model 20 security mechanisms
  - Effectiveness: apply the analysis approach to a HCN (Healthcare Collaboration Network) scenario
- Related Work
- Conclusion and Future Work

Background and Motivation

- Security mechanisms
  - E.g., access control, encryption, auditing, virtual private network, intrusion detection system
  - The application of security mechanisms affects system requirements specifications [Heyman2011, Okubo2012]



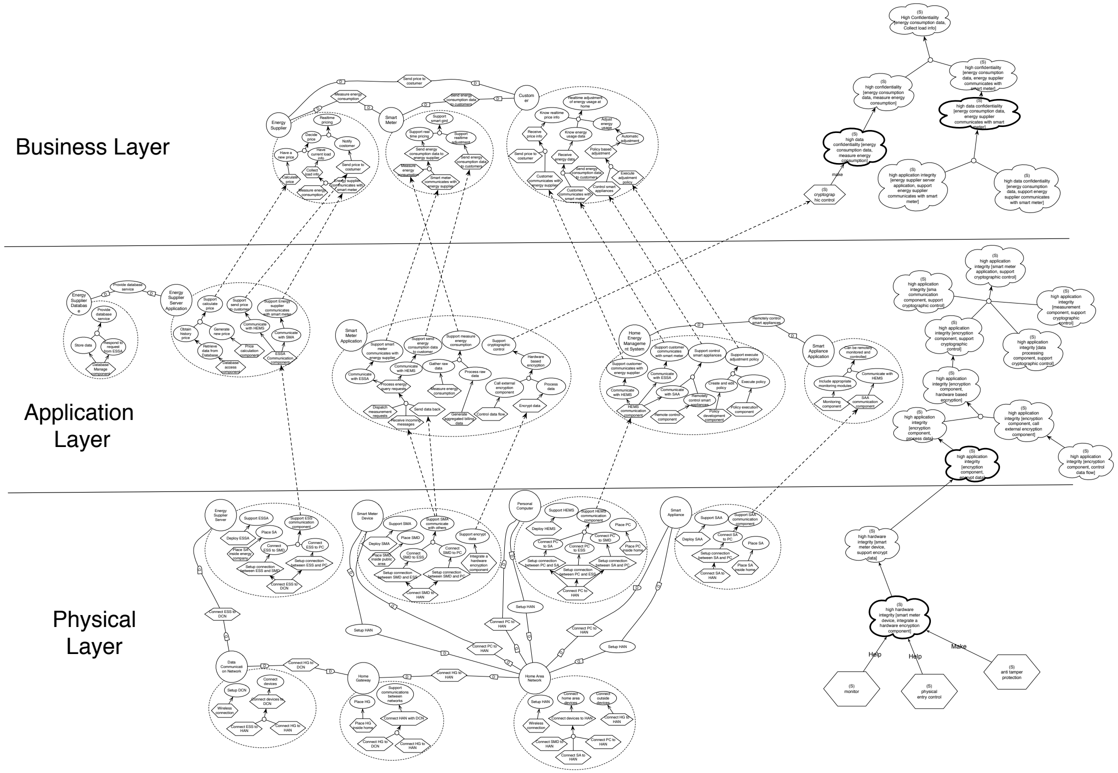
Lacks an approach for analyzing the impact

Research Plan

- **Research Objective**: capture and enforce the impact security mechanisms impose on the system
- **Research Method**: investigate more than 40 security mechanisms [Scandariato2008, Fernandez2013]

Baseline

- A goal-based approach for analyzing security requirements in a holistic manner [Li2014CAiSE]
  - baseline for requirements specification

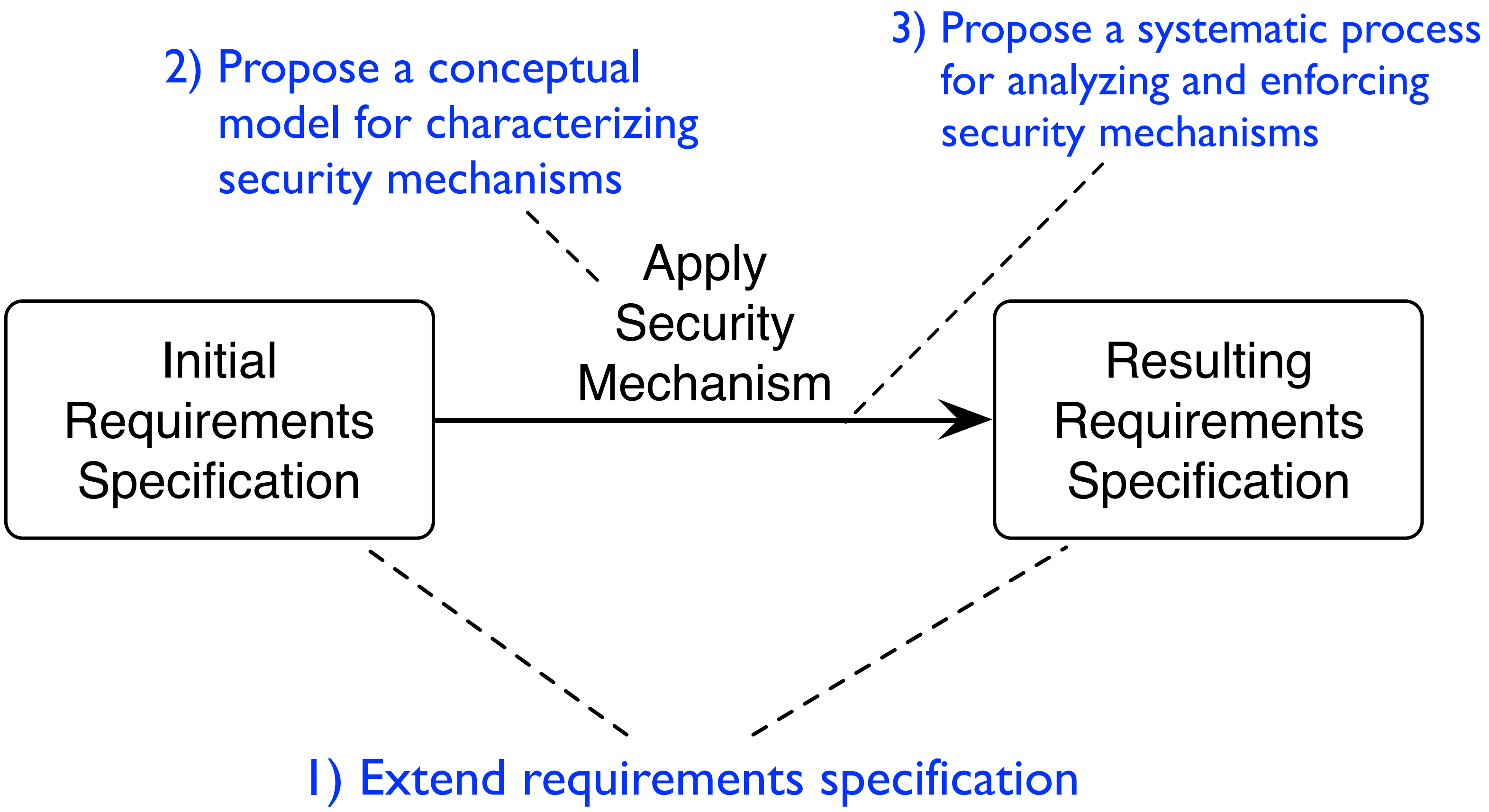


Baseline

- A method for seamlessly integrating security patterns into requirements analysis [Li2014PoEM]
  - Security pattern: specifies proven security solutions (security mechanism) to known security problems
  - Model textual security patterns in contextual goal models to support the selection and application of security patterns
    - Context → Domain property
    - Problem → Goals
    - **Solution (Security mechanism) → Tasks**
    - …

missing the impact analysis

Research Proposal

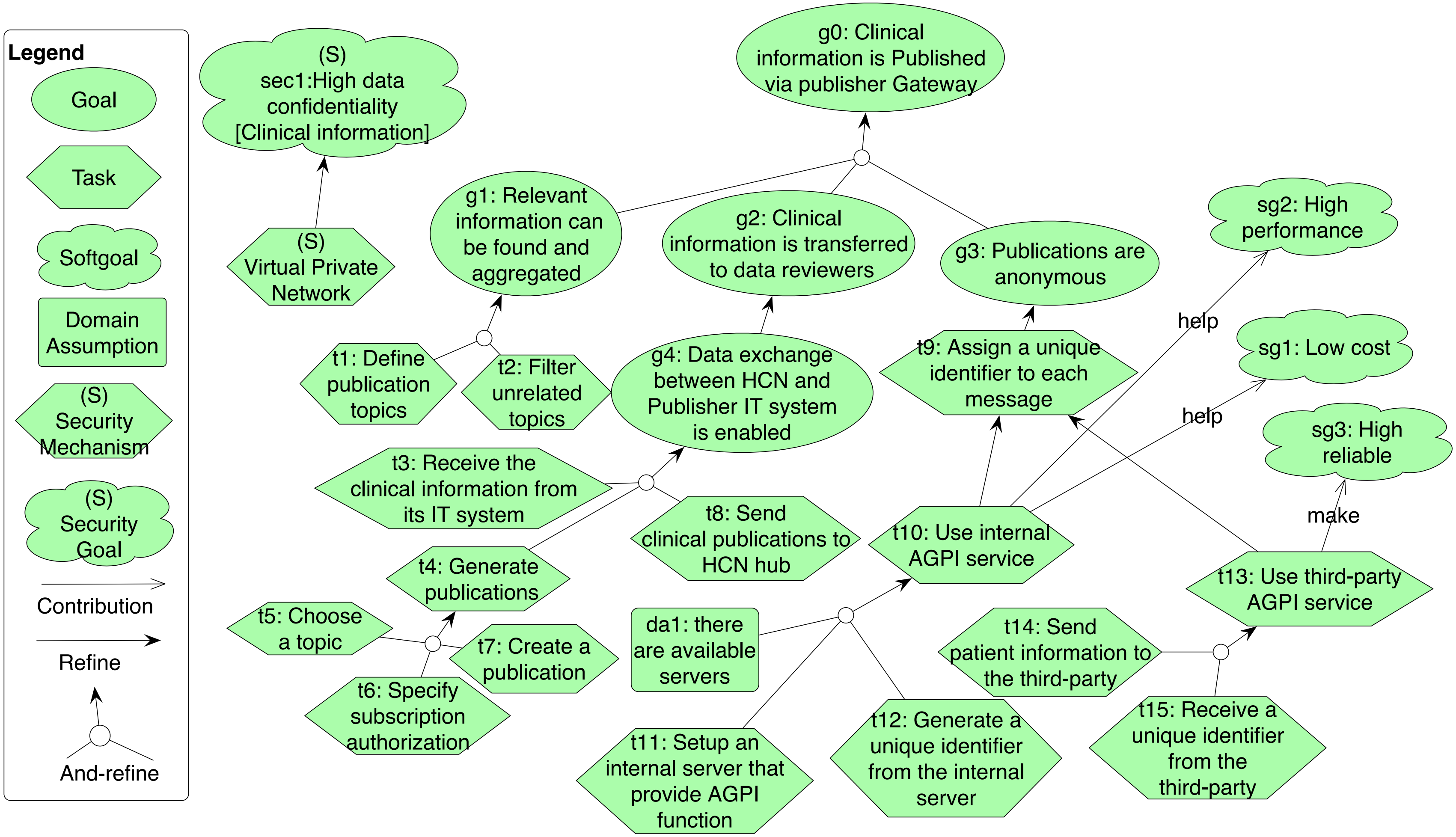

2) Propose a conceptual model for characterizing security mechanisms
3) Propose a systematic process for analyzing and enforcing security mechanisms
Apply Security Mechanism
Initial Requirements Specification
Resulting Requirements Specification
1) Extend requirements specification

An Enriched Requirements Specification

- Elements from previous work[Li2014CAiSE]:
  - Goals (*G*), softgoals (*SG*), tasks (*T*), domain assumptions (*DA*), refinements (*RE*) and contributions (*CON*)
- New Element for capturing impact of mechanisms:
  - Task constraints (*TC*)
    - task invariants
    - precondition
    - postcondition

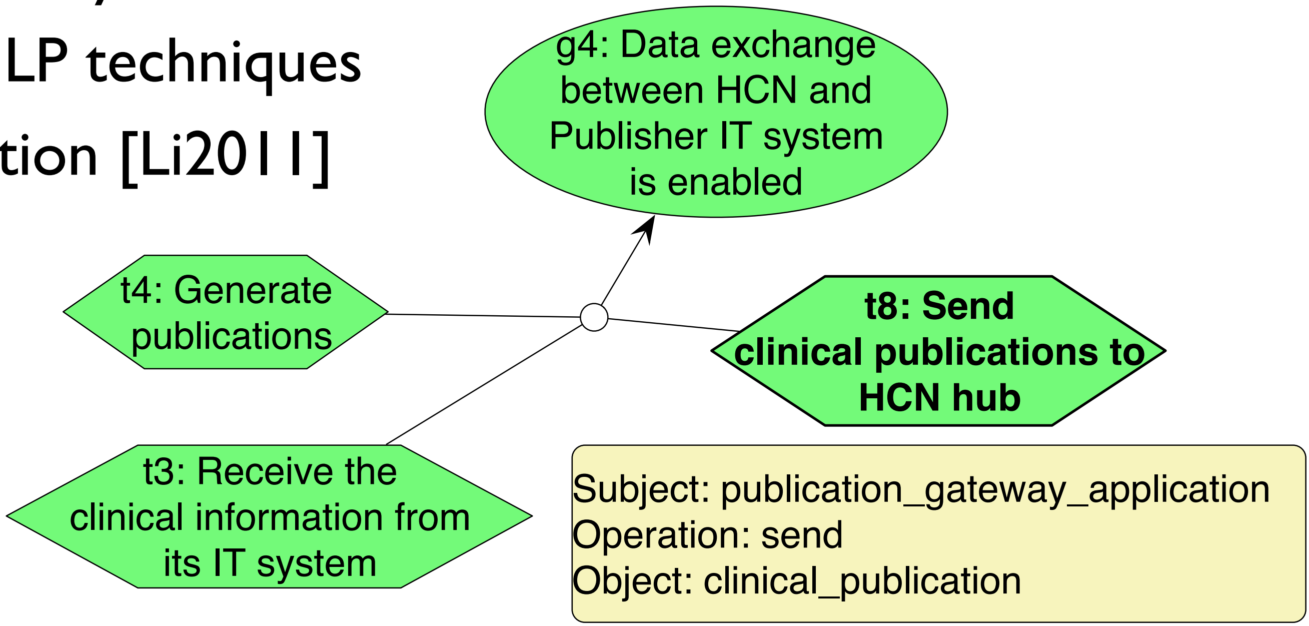
- R = {*G, SG, T, DA, REF, CON, TC*}

An Example of the Initial Requirements Specification


Legend
Goal
Task
Softgoal
Domain Assumption
(S) Security Mechanism
(S) Security Goal
Contribution
Refine
And-refine
(S) sec1:High data confidentiality [Clinical information]
(S) Virtual Private Network
g0: Clinical information is Published via publisher Gateway
g1: Relevant information can be found and aggregated
g2: Clinical information is transferred to data reviewers
g3: Publications are anonymous
sg2: High performance
sg1: Low cost
sg3: High reliable
t1: Define publication topics
t2: Filter unrelated topics
g4: Data exchange between HCN and Publisher IT system is enabled
t9: Assign a unique identifier to each message
help
help
make
t3: Receive the clinical information from its IT system
t8: Send clinical publications to HCN hub
t10: Use internal AGPI service
t13: Use third-party AGPI service
t4: Generate publications
t5: Choose a topic
t7: Create a publication
t6: Specify subscription authorization
da1: there are available servers
t14: Send patient information to the third-party
t11: Setup an internal server that provide AGPI function
t12: Generate a unique identifier from the internal server
t15: Receive a unique identifier from the third-party

An Enriched Requirements Specification

- Capture the semantics of Tasks
  - Expanded Attributes: subject, operation, object
- Attributes Elicitation
  - Manually specify
  - Leverage NLP techniques for automation [Li2011]


g4: Data exchange between HCN and Publisher IT system is enabled
t4: Generate publications
t8: Send clinical publications to HCN hub
t3: Receive the clinical information from its IT system

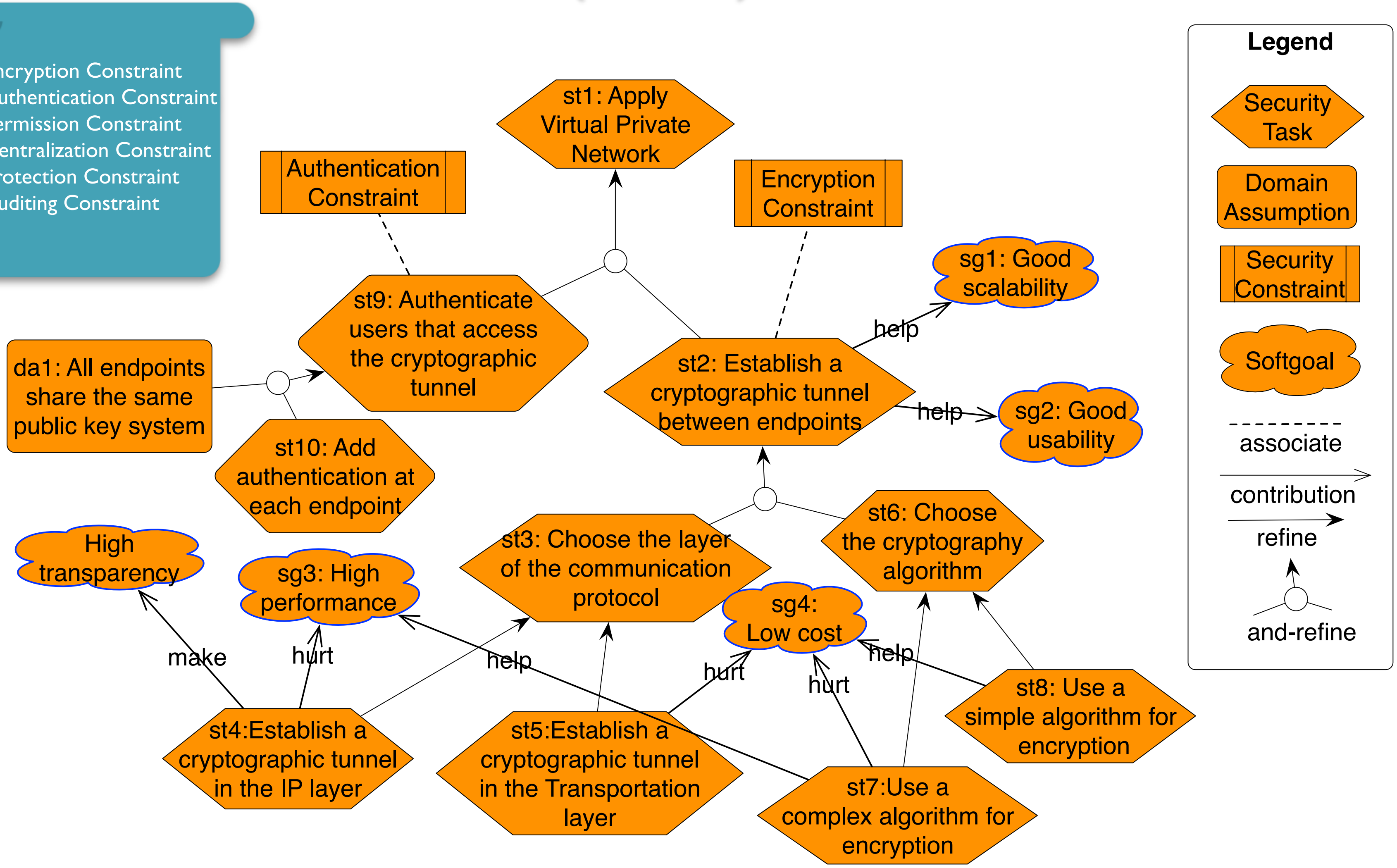
Subject: publication_gateway_application
Operation: send
Object: clinical_publication

Modeling Security Mechanisms

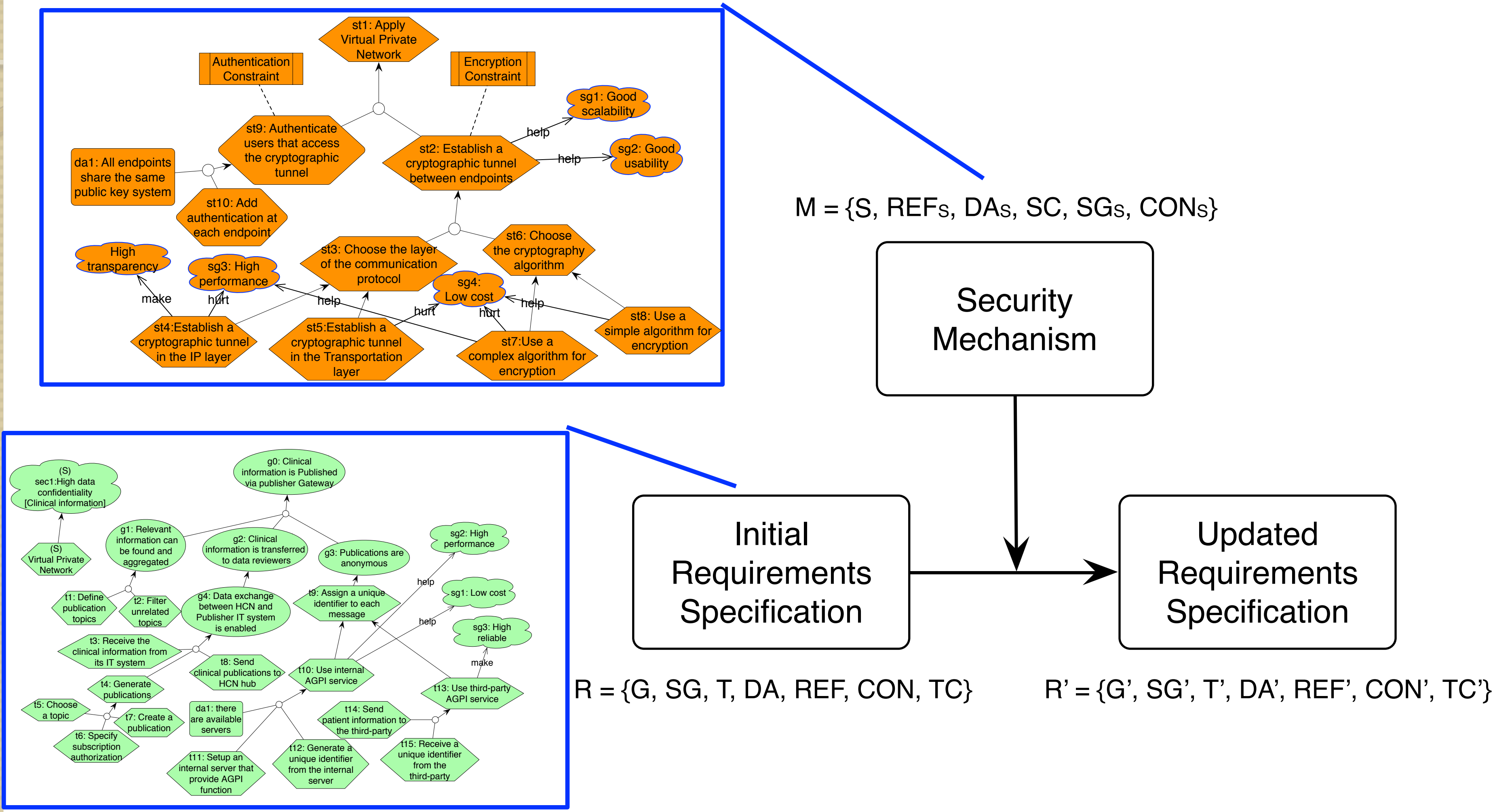
- Concepts:
  - Security Task
    - A detailed function performed by a system to achieve certain security goals
  - Assumption
    - An expected state of affairs, under which the security mechanism can be applied correctly
  - Security Constraint
    - A constraint that imposes a specific type of impact on specific tasks
  - Quality Influence
    - A positive/negative influence on system qualities

Security Mechanism Example-Virtual Private Network(VPN)

Encryption Constraint
Authentication Constraint
Permission Constraint
Centralization Constraint
Protection Constraint
Auditing Constraint


st1: Apply Virtual Private Network
Authentication Constraint
Encryption Constraint
sg1: Good scalability
st9: Authenticate users that access the cryptographic tunnel
st2: Establish a cryptographic tunnel between endpoints
help
help
sg2: Good usability
da1: All endpoints share the same public key system
st10: Add authentication at each endpoint
st6: Choose the cryptography algorithm
st3: Choose the layer of the communication protocol
High transparency
sg3: High performance
sg4: Low cost
make
hurt
help
hurt
hurt
help
st8: Use a simple algorithm for encryption
st4:Establish a cryptographic tunnel in the IP layer
st5:Establish a cryptographic tunnel in the Transportation layer
st7:Use a complex algorithm for encryption
Legend
Security Task
Domain Assumption
Security Constraint
Softgoal
associate
contribution
refine
and-refine

A Process for Applying Security Mechanism

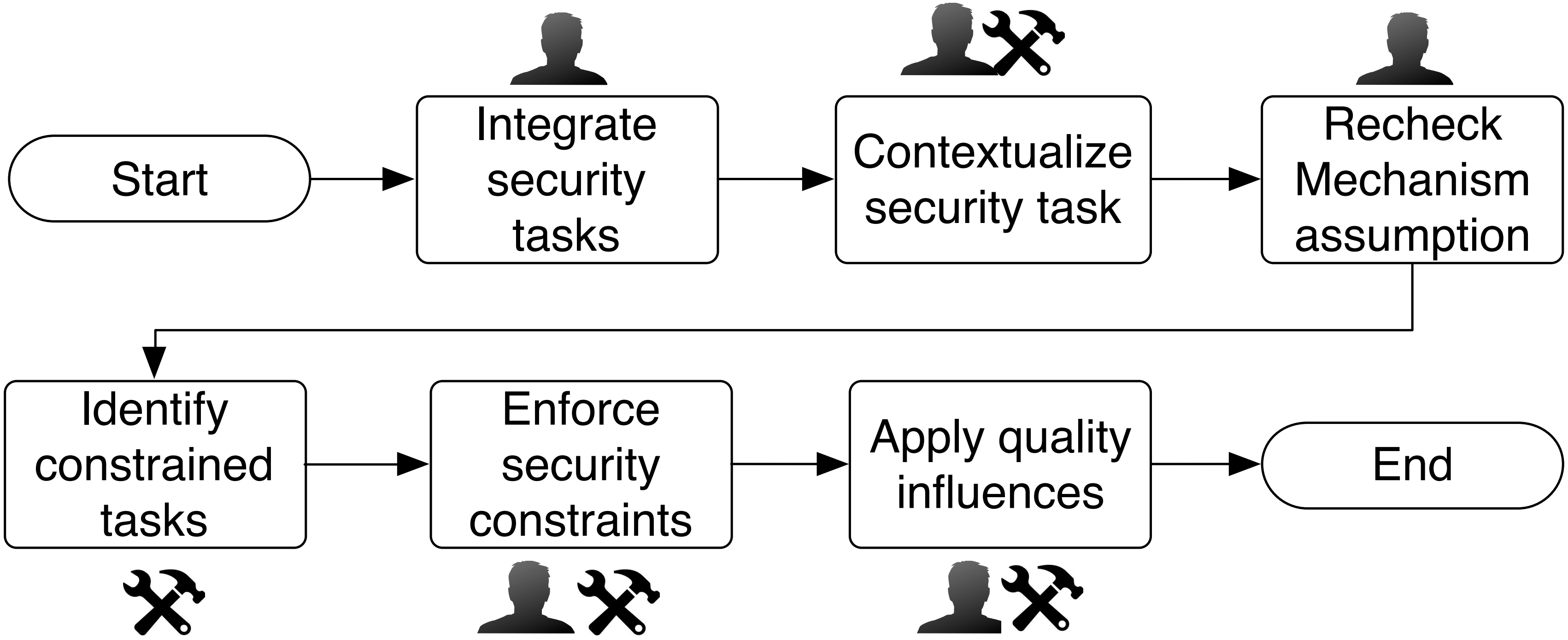

st1: Apply Virtual Private Network
Authentication Constraint
Encryption Constraint
sg1: Good scalability
st9: Authenticate users that access the cryptographic tunnel
st2: Establish a cryptographic tunnel between endpoints
help
help
sg2: Good usability
da1: All endpoints share the same public key system
st10: Add authentication at each endpoint
High transparency
sg3: High performance
st3: Choose the layer of the communication protocol
st6: Choose the cryptography algorithm
sg4: Low cost
make
hurt
help
hurt
hurt
help
st4:Establish a cryptographic tunnel in the IP layer
st5:Establish a cryptographic tunnel in the Transportation layer
st7:Use a complex algorithm for encryption
st8: Use a simple algorithm for encryption
(S) sec1:High data confidentiality [Clinical information]
g0: Clinical information is Published via publisher Gateway
(S) Virtual Private Network
g1: Relevant information can be found and aggregated
g2: Clinical information is transferred to data reviewers
g3: Publications are anonymous
sg2: High performance
t1: Define publication topics
t2: Filter unrelated topics
g4: Data exchange between HCN and Publisher IT system is enabled
t9: Assign a unique identifier to each message
help
sg1: Low cost
help
sg3: High reliable
t3: Receive the clinical information from its IT system
t8: Send clinical publications to HCN hub
t10: Use internal AGPI service
make
t4: Generate publications
t13: Use third-party AGPI service
t5: Choose a topic
t7: Create a publication
da1: there are available servers
t14: Send patient information to the third-party
t6: Specify subscription authorization
t11: Setup an internal server that provide AGPI function
t12: Generate a unique identifier from the internal server
t15: Receive a unique identifier from the third-party
Security Mechanism
Initial Requirements Specification
Updated Requirements Specification

$M = \{S, REF_S, DA_S, SC, SG_S, CON_S\}$

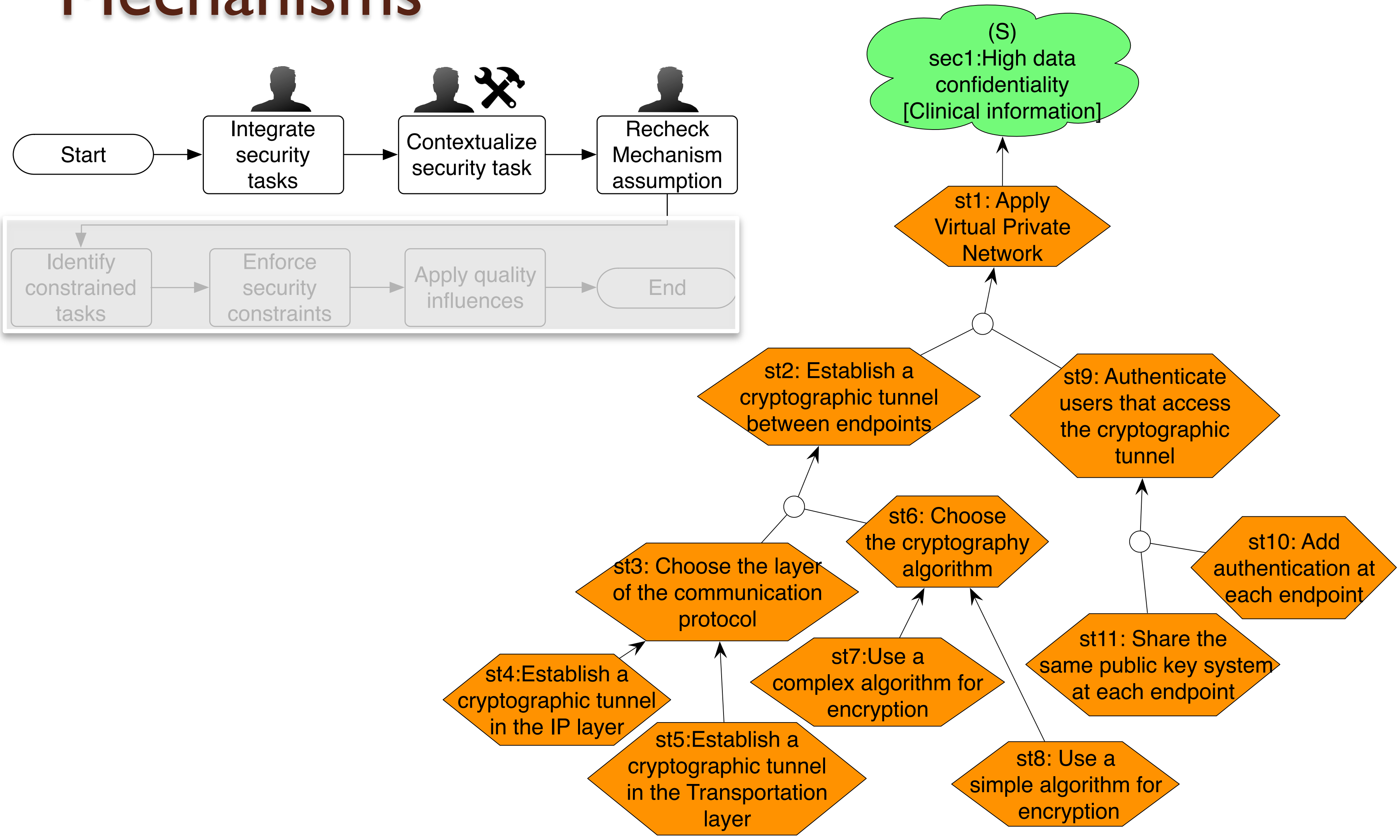
$R = \{G, SG, T, DA, REF, CON, TC\}$

$R' = \{G', SG', T', DA', REF', CON', TC'\}$

A Process for Applying Security Mechanism


Start
Integrate security tasks
Contextualize security task
Recheck Mechanism assumption
Identify constrained tasks
Enforce security constraints
Apply quality influences
End

Example – Application of the VPN Mechanisms

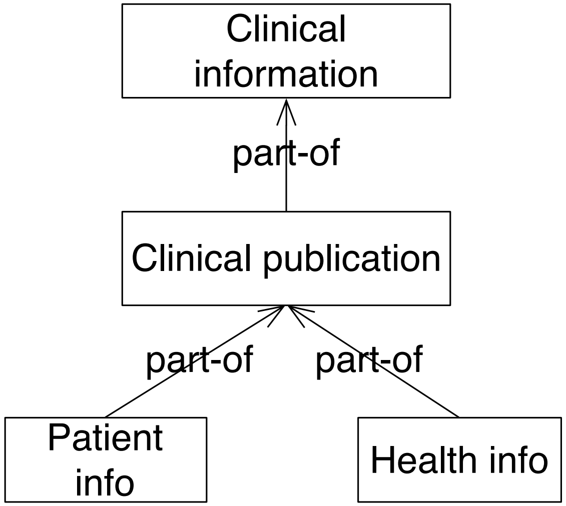

Start
Integrate security tasks
Contextualize security task
Recheck Mechanism assumption
Identify constrained tasks
Enforce security constraints
Apply quality influences
End
(S) sec1:High data confidentiality [Clinical information]
st1: Apply Virtual Private Network
st2: Establish a cryptographic tunnel between endpoints
st9: Authenticate users that access the cryptographic tunnel
st3: Choose the layer of the communication protocol
st6: Choose the cryptography algorithm
st10: Add authentication at each endpoint
st4:Establish a cryptographic tunnel in the IP layer
st5:Establish a cryptographic tunnel in the Transportation layer
st7:Use a complex algorithm for encryption
st8: Use a simple algorithm for encryption
st11: Share the same public key system at each endpoint

Identify Constrained Tasks

Identification rules for encryption constraints

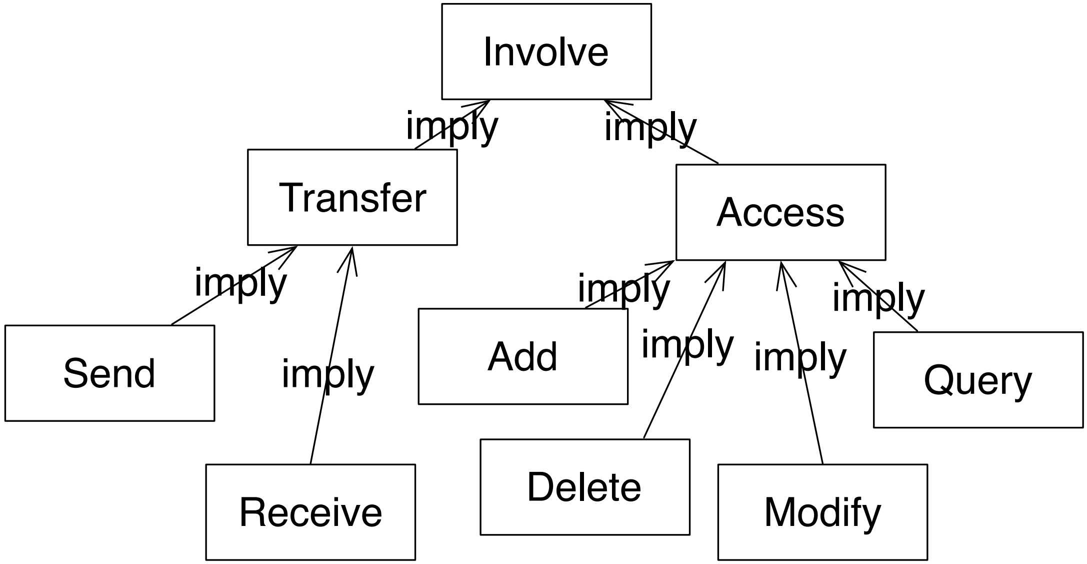
$$\begin{aligned}&Rule\_1 : constrain(ST,T) \leftarrow has\_operation(T,OP)\\&\wedge transfer\_operation(OP) \wedge has\_object(T,O) \wedge protect(ST,O)\\&\wedge has\_constraint(ST, encryption\_constraint)\end{aligned}$$

Data Schema



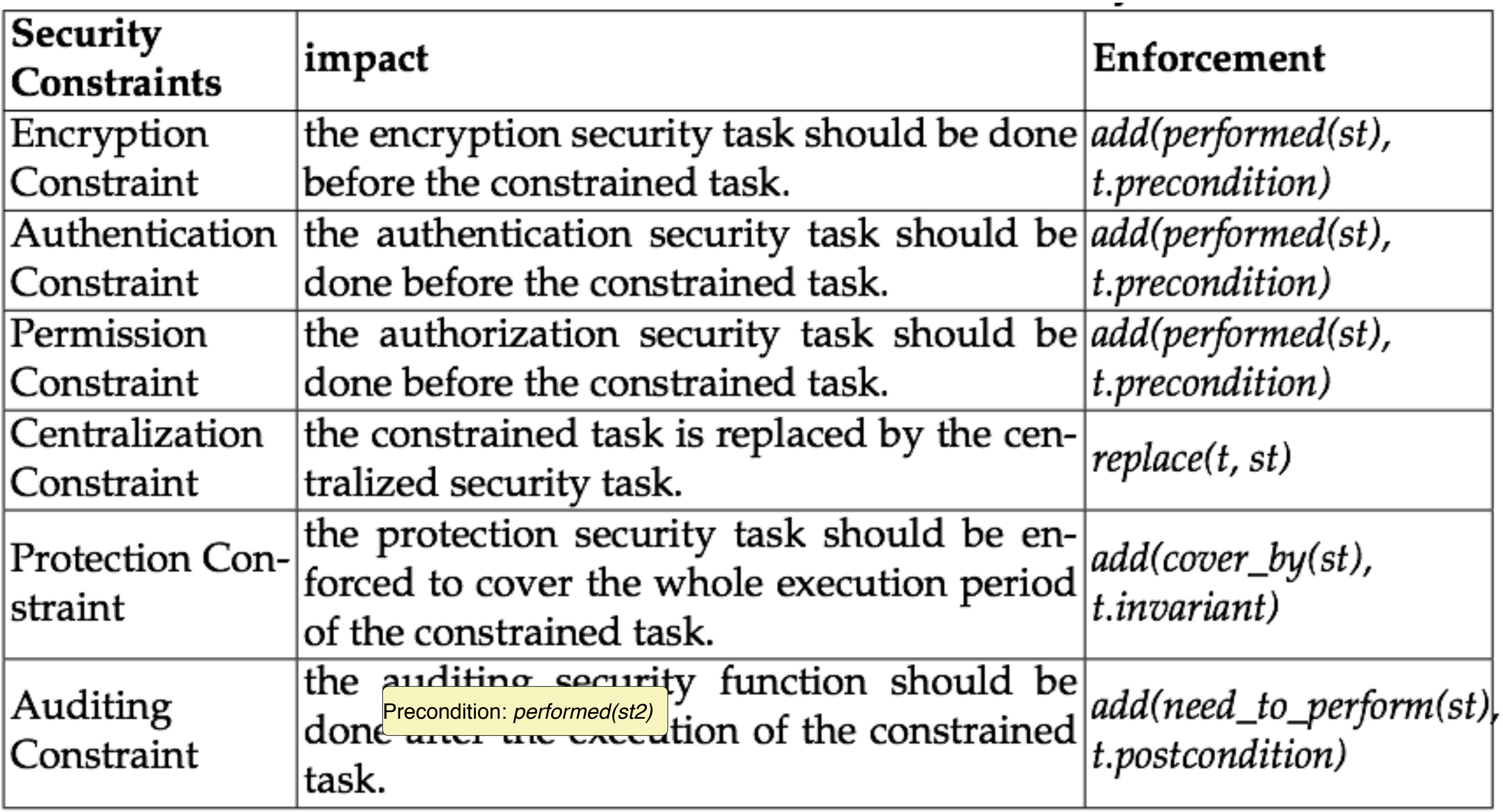
$$Rule\_7 : protect(ST,A2) \leftarrow protect(ST,A1) \wedge part\_of(A1,A2)$$

Word Semantic Hierarchy



$$Rule\_8 : transfer\_operation(O) \leftarrow send\_operation(O)$$

Example – Identify Constrained Tasks

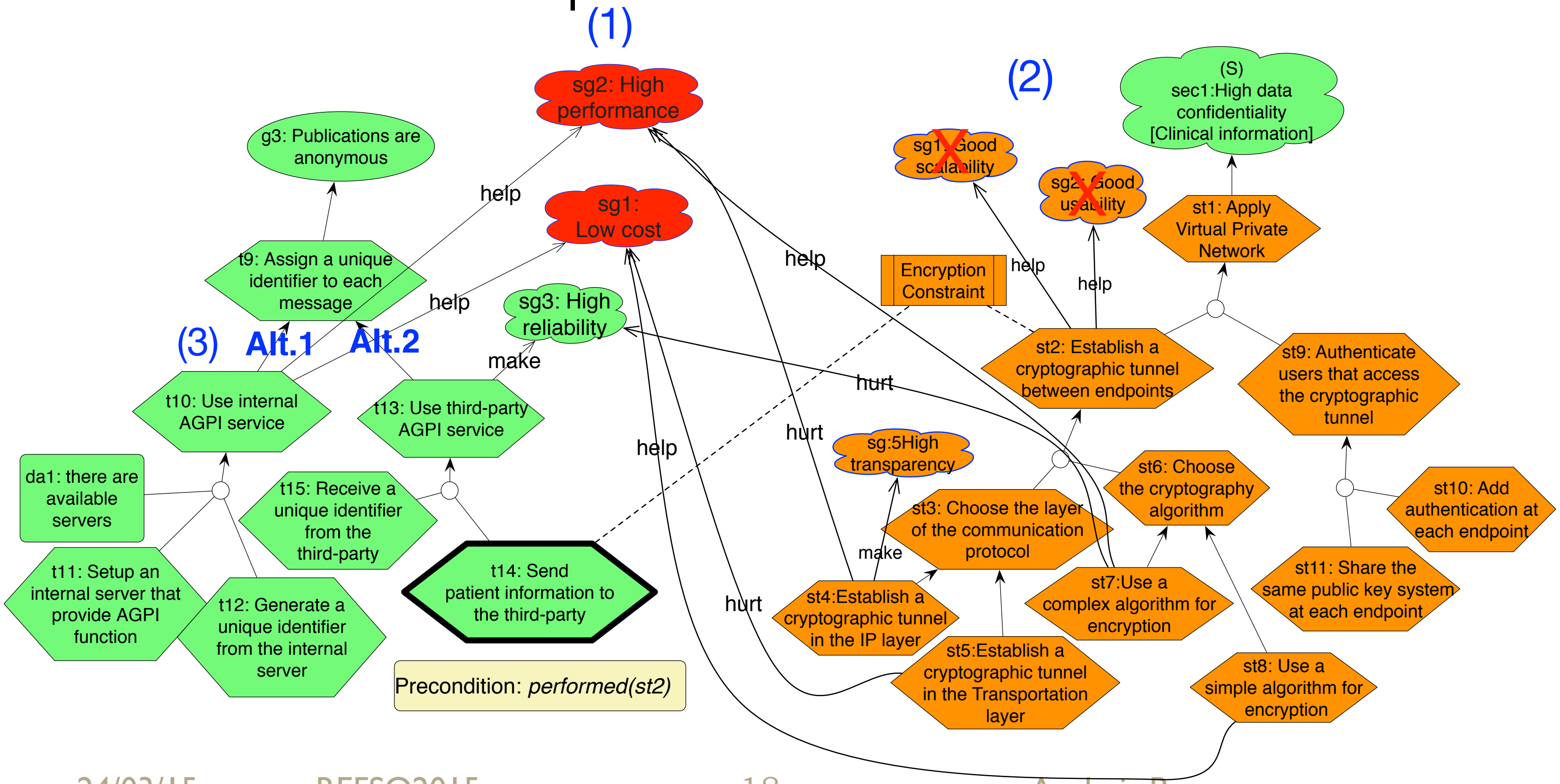


Security Constraints	**impact**	**Enforcement**
Encryption Constraint	the encryption security task should be done before the constrained task.	*add(performed(st), t.precondition)*
Authentication Constraint	the authentication security task should be done before the constrained task.	*add(performed(st), t.precondition)*
Permission Constraint	the authorization security task should be done before the constrained task.	*add(performed(st), t.precondition)*
Centralization Constraint	the constrained task is replaced by the centralized security task.	*replace(t, st)*
Protection Constraint	the protection security task should be enforced to cover the whole execution period of the constrained task.	*add(cover_by(st), t.invariant)*
Auditing Constraint	the auditing security function should be done [illegible]tion of the constrained task.	*add(need_to_perform(st), t.postcondition)*

Precondition: *performed(st2)*

Analyze Quality Influences

- Correlate softgoals
- Assess uncorrelated softgoals
- Reevaluate influenced requirements alternatives



(1)
(2)
(3)
Alt.1
Alt.2
sg2: High performance
sg1: Low cost
sg3: High reliability
g3: Publications are anonymous
t9: Assign a unique identifier to each message
t10: Use internal AGPI service
t13: Use third-party AGPI service
da1: there are available servers
t11: Setup an internal server that provide AGPI function
t12: Generate a unique identifier from the internal server
t15: Receive a unique identifier from the third-party
t14: Send patient information to the third-party
Precondition: performed(st2)
sg1: Good scalability
sg2: Good usability
(S) sec1:High data confidentiality [Clinical information]
st1: Apply Virtual Private Network
Encryption Constraint
st2: Establish a cryptographic tunnel between endpoints
st9: Authenticate users that access the cryptographic tunnel
sg:5High transparency
st3: Choose the layer of the communication protocol
st6: Choose the cryptography algorithm
st10: Add authentication at each endpoint
st4:Establish a cryptographic tunnel in the IP layer
st5:Establish a cryptographic tunnel in the Transportation layer
st7:Use a complex algorithm for encryption
st8: Use a simple algorithm for encryption
st11: Share the same public key system at each endpoint
help
help
help
help
help
help
help
make
make
hurt
hurt
hurt

Evaluate the Conceptual Model

- Model 20 security mechanisms [Scandariato2008, Fernandez2013] using the proposed conceptual model

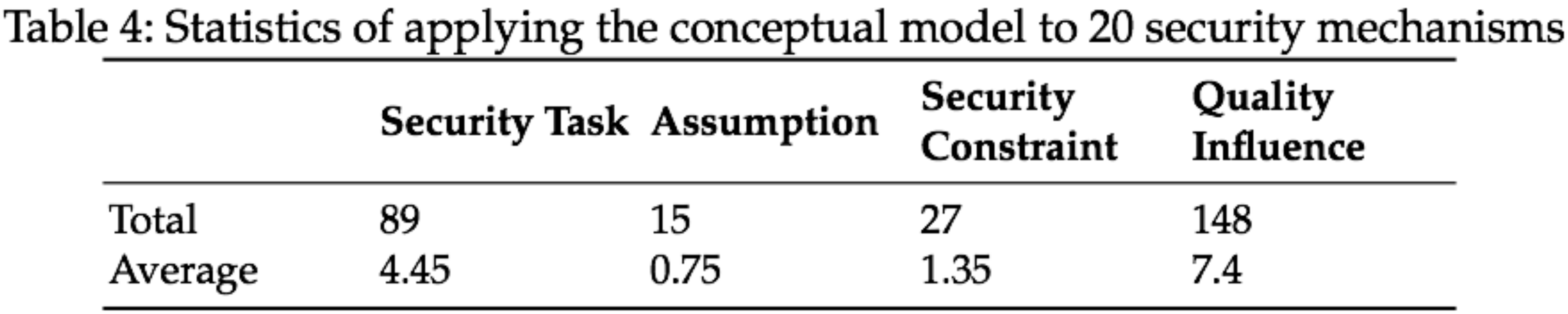


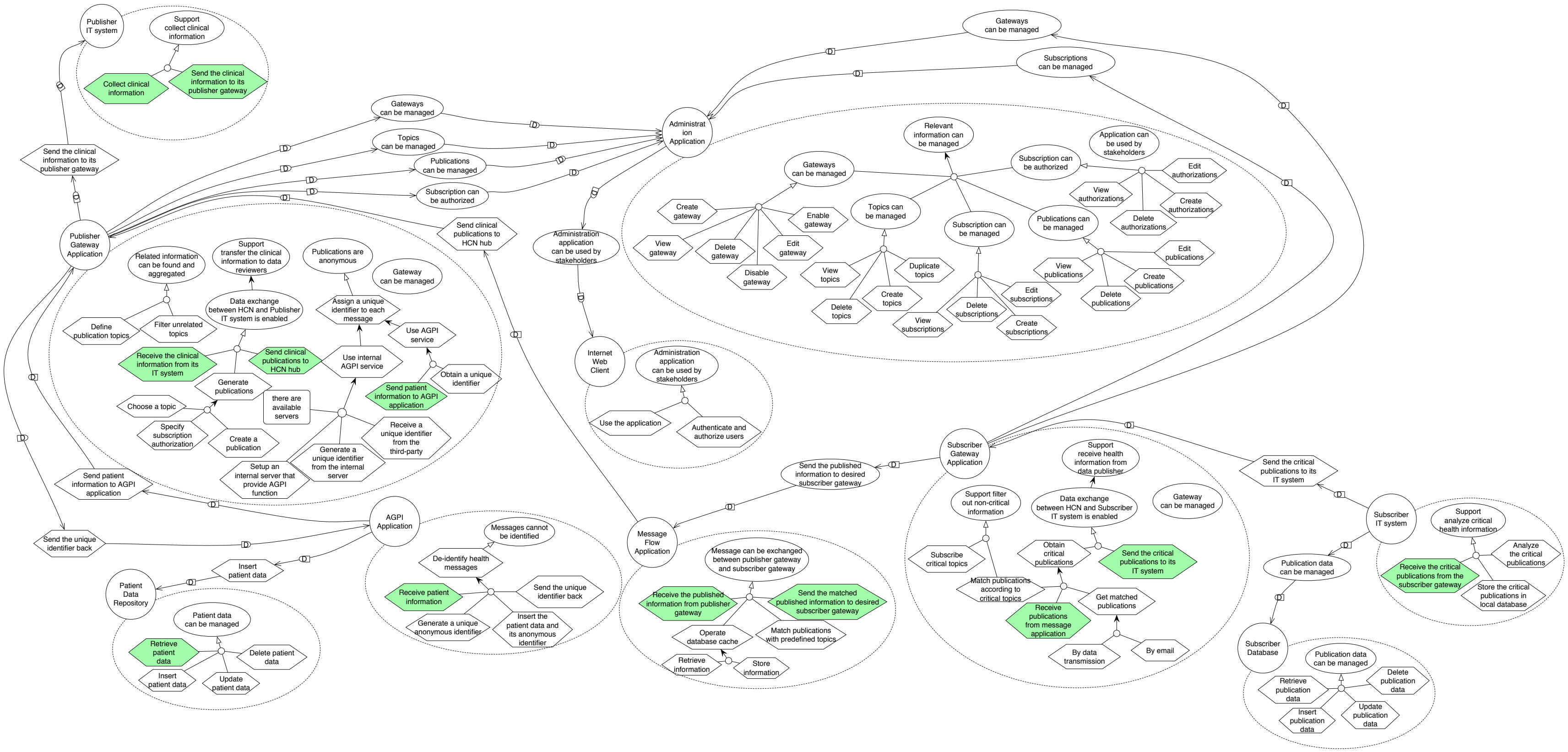
Table 4: Statistics of applying the conceptual model to 20 security mechanisms

	Security Task	**Assumption**	**Security Constraint**	**Quality Influence**
Total	89	15	27	148
Average	4.45	0.75	1.35	7.4

Evaluate the Impact Analysis

- Analyze the impact of the VPN mechanism on the HCN (Healthcare Collaboration Network) Scenario
  - Input:
    - Scenario: 23 goals, 8 softgoals, 67 tasks, and 75 refinement links
    - VPN mechanism: 9 security tasks, 1 assumption, 2 security constraints, and 8 quality influences
  - Output:
    - 12 tasks are constrained by the VPN mechanism
    - 2 tasks constraints and 3 quality influences are applied to each constrained task

Identified Constrained Tasks


Publisher IT system
Support collect clinical information
Collect clinical information
Send the clinical information to its publisher gateway
Send the clinical information to its publisher gateway
Gateways can be managed
Topics can be managed
Publications can be managed
Subscription can be authorized
Send clinical publications to HCN hub
Publisher Gateway Application
Related information can be found and aggregated
Support transfer the clinical information to data reviewers
Publications are anonymous
Gateway can be managed
Define publication topics
Filter unrelated topics
Data exchange between HCN and Publisher IT system is enabled
Assign a unique identifier to each message
Use AGPI service
Receive the clinical information from its IT system
Send clinical publications to HCN hub
Use internal AGPI service
Obtain a unique identifier
Generate publications
there are available servers
Send patient information to AGPI application
Choose a topic
Specify subscription authorization
Create a publication
Receive a unique identifier from the third-party
Generate a unique identifier from the internal server
Setup an internal server that provide AGPI function
Send patient information to AGPI application
AGPI Application
Send the unique identifier back
Messages cannot be identified
De-identify health messages
Receive patient information
Send the unique identifier back
Generate a unique anonymous identifier
Insert the patient data and its anonymous identifier
Insert patient data
Patient Data Repository
Patient data can be managed
Retrieve patient data
Delete patient data
Insert patient data
Update patient data
Administration Application
Administration application can be used by stakeholders
Internet Web Client
Administration application can be used by stakeholders
Use the application
Authenticate and authorize users
Gateways can be managed
Subscriptions can be managed
Relevant information can be managed
Gateways can be managed
Subscription can be authorized
Application can be used by stakeholders
Edit authorizations
View authorizations
Create authorizations
Delete authorizations
Create gateway
Enable gateway
View gateway
Delete gateway
Edit gateway
Disable gateway
Topics can be managed
Subscription can be managed
Publications can be managed
View topics
Duplicate topics
Delete topics
Create topics
View subscriptions
Delete subscriptions
Edit subscriptions
Create subscriptions
View publications
Edit publications
Create publications
Delete publications
Message Flow Application
Send the published information to desired subscriber gateway
Message can be exchanged between publisher gateway and subscriber gateway
Receive the published information from publisher gateway
Send the matched published information to desired subscriber gateway
Operate database cache
Match publications with predefined topics
Retrieve information
Store information
Subscriber Gateway Application
Support receive health information from data publisher
Support filter out non-critical information
Data exchange between HCN and Subscriber IT system is enabled
Gateway can be managed
Subscribe critical topics
Obtain critical publications
Send the critical publications to its IT system
Match publications according to critical topics
Get matched publications
Receive publications from message application
By data transmission
By email
Send the critical publications to its IT system
Subscriber IT system
Support analyze critical health information
Publication data can be managed
Receive the critical publications from the subscriber gateway
Analyze the critical publications
Store the critical publications in local database
Subscriber Database
Publication data can be managed
Retrieve publication data
Delete publication data
Insert publication data
Update publication data
D

Conclusions

- Present a conceptual model which characterizes security mechanism from a requirements viewpoint
- Propose a systematic way to analyze and enforce the impact of a security mechanism imposed on system requirements.
- Initially evaluate the proposed approach using a HCN scenario
- A prototype tool has been developed to support the analysis process

Future work

- Generalize our approach to other mechanisms (e.g., performance mechanisms)
- Investigate more security mechanisms to further check the coverage of the proposed security constraints
- Carry out more case studies for better evaluation
- Involve practitioners into the evaluation of the approach

Thank You!

Contact: tong.li@disi.unitn.it