An NFR Pattern Approach to Dealing with NFRs

Presenter: Sam Supakkul

Sam Supakkul
Tom Hill
Lawrence Chung
The Univ. of Texas at Dallas

Thein Than Tun
The Open University, UK

Julio CSP Leite
PUC-Rio, Brazil
An NFR Pattern Approach to Dealing with NFRs

Presenter: Sam Supakkul

Layered shells
Surrounded by water
Triangular shape

Beautiful building
Cost
Durability

Cost (criticality=high)

Help? Help/hurt?

Layered shells
Surrounded by water
Triangular shape

Sam Supakkul
Tom Hill
Lawrence Chung
The Univ. of Texas at Dallas

Thein Than Tun
The Open University, UK

Julio CSP Leite
PUC-Rio, Brazil
Some NFRs, such as security, are achieved by “dealing with bad things”

- Credit card info security (criticality=high)
- Break-in wireless network (criticality=intermediate)
- Masquerade user login
- Steal credit card info (criticality=low)
- 2-factor authentication
- Password encryption
- Biometric authentication

Thrustworthiness help/hurt?

Cost help/hurt?
Acquiring and using NFR knowledge are difficult but insufficient knowledge can be damaging.

(2nd) Biggest credit card theft
- 45.7M credit cards stolen
- $20M in fraudulent transactions
- To cost TJX $1B over 5 years

TJX Inc. used security measures
- ID/password authentication
- Data encryption

But TJX did not know enough
- Potential security problems
- Applicable mitigations
  - Proper tradeoff among NFRs

TJX not able to prevent the hacker
- 1. Break-in wireless network
- 2. Masquerade user login
- 3. Steal credit card info
This talk presents a pattern-based approach to capturing, organizing, and reusing NFR knowledge.
Different kinds of patterns for capturing different kinds of NFR knowledge

Objective pattern

Problem pattern

Alternatives pattern

Selection pattern
Objective pattern captures a definition of an NFR as softgoals to be achieved.

Security = Confidentiality, Integrity, and Availability

Confidentiality = Privacy and Proprietary

Integrity = Authenticity and Non-repudiation

Availability = Timeliness and Reliability
Problem pattern captures soft-problems or obstacles to achieving an NFR

NFR: Confidentiality [Credit Card]

Undesirable situation: Unauthorized access [Server]

Threat operations: Masquerading user login, ...

Vulnerability: Transmission of ID/password in clear text
Problem: Transmission of ID/password in clear text

Alternatives: Encrypt ID/password, Biometric authentication

Side-effects: Cost, Trustworthiness
Selection pattern captures an application independent selection scheme

**Weight-based quantitative selection**

Selection based on the **weight** of criticality of goal/problem contribution towards goal/problem

- **pro:** intuitive, widely used
- **con:** subjective weighting, scaling problem

**Rank-based qualitative selection**

Selection based on the **ranking** of criticality-contribution combination

- **pro:** less subjective, no scaling problem
- **con:** agreement on ranking
A deeper look at the selections

Weight-based quantitative selection

- selection = alternative with highest score
  \[
  \text{score(alternative)} = \sum \text{score(contribution)}
  \]
  \[
  \text{score(contr)} = \text{weight(criticality)} \times \text{weight(contr)}
  \]

- selection = alternative with best ranking
  \[
  \text{rank(alternative)} = \sum \text{rank(contribution)}
  \]
  \[
  \text{rank(contr)} = \text{rank(criticality-contr)}
  \]

Rank-based qualitative selection

- user-defined ranking:
  
  \[
  \begin{align*}
  &++!!G +!!G \ldots +S +S \ldots --S \\
  &1 \quad 2 \quad \ldots \quad 6 \quad 7 \quad \ldots \quad 15
  \end{align*}
  \]
Additional info for each pattern: credentials, applicability, refinement rules

Credentials and applicability info. help with pattern selection

Credentials
- Authors
- Sources
- Endorsements
- Known Uses

Applicability
- Who
- What
- Why
- When
- Where
- How
- How much

Refinement rules help with pattern reuse/application

NFRD decomposition refinement rule

R1

R2

R3

R4

succeed
Refinement rules used to transform the target model during pattern application.
Next, patterns may be organized along generalization, aggregation, and classification dim.

Objective pattern

Problem pattern

Alternatives pattern

Selection pattern

Capturing

Reusing

Amenable to tool support
Specialized pattern is more specific
in breadth or in depth

Generalization dimension

More specific in breadth
US Law:
Security = Conf., Integrity, Avail.

Payment Card Industry (PCI):
Security = Confidentiality

More specific in depth
PCI also concerned with
Accountability beyond Privacy
Composite pattern assembles smaller patterns to capture a larger chunk of knowledge.

Composite “whole” pattern

Applying the “whole” pattern will apply the “part-of” patterns.
A pattern is used as a template to instantiate occurrence patterns.

Classification dimension

Applying the occurrence pattern applies the meta-pattern with customization (binding):

"Security asset" mapped to "Credit Card Info" (super-class to sub-class)
"Security" mapped to "Confidentiality" (parent goal to sub-goal)
Applying the approach to the TJX case shows preliminary positive results.

**Method**
- Construct tool prototypes
- Build for reuse scenario
- Build with reuse scenario

**Hypotheses**
- Knowledge from the case can be captured and reused in a different project
- The approach works in a tool-assisted environment

Reuse knowledge in a different project.

Break-in wireless network
Masquerade user login
Steal credit card info
The NFR Pattern Assistant for pattern support

The RE-Tools for knowledge modeling

The NFR Pattern Assistant

StarUML™ extension framework

The i* Framework

KAOS

Problem Frame

UML

www.utdallas.edu/~supakkul/tools/NFRPassist

www.utdallas.edu/~supakkul/tools/RE-Tools
Build for reuse scenario: model and patternize

Model for the current project

Patternize and organize for future projects
Build with reuse scenario: select and apply

Initial Target Model

Credit Card

Apply

Objective Pattern

Apply

Problem Pattern

Apply

Alternative Solutions Pattern

Apply

Resultant Target Model

Apply

Pattern Catalog

Apply

Selection Pattern

Apply

Alternative Requirements Pattern

Apply

Selection Pattern
Results: 93% of knowledge captured and reused
The approach works but needs improvements

- Break-in wireless network
- Masquerade user login
- Steal credit card info

Sample results

Limitations (future work)

Tool/usability related
- Models not captured with original placements
- Knowledge not captured due to missing refinement rules (25 rules defined)
- Pattern search and selection are currently manual

Approach related
- Need to support dealing with NFRs during architecture/design
- Need more case studies
In summary, the difficulty of acquiring and using NFR knowledge can be alleviated by NFR patterns.
Backup slides
Five operations are defined for manipulating NFR patterns
NFR pattern concepts are defined in a meta-model and implemented by the tool.
Modeling concepts are integrated in a meta-model and implemented by the tool.
Refinement rules for objective pattern
Example of refinement rules in an objective pattern
Refinement rules for problem pattern
Example of refinement rules in a problem pattern
Refinement rules for alternatives pattern
Example of refinement rules in an alternatives pattern
Refinement rules for selection pattern
Example of refinement rules in a selection pattern
Constraints for pattern aggregation
Constraints for pattern instantiation