UNIVERSITÄT
KOBLENZ · LANDAU

Reality vs. Security Model vs. Software – Bridging the Gaps

FUNDP Namur, September 25, 2012
Virtual Goods 2012

Daniel Pähler, tulkas@uni-koblenz.de

University of Koblenz-Landau

Institute for IS Research

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

Agenda

Where I fit in

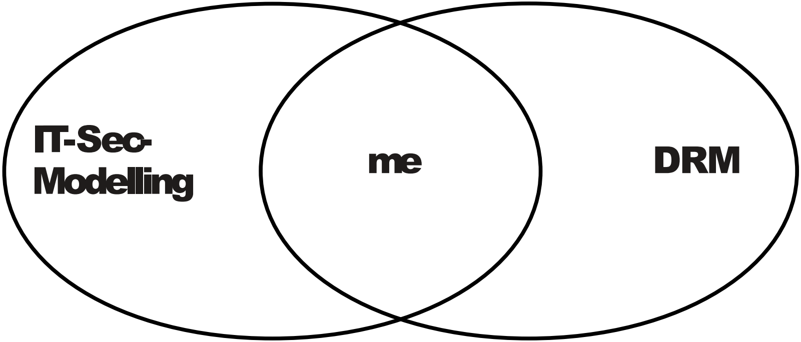
- Research Area
- Research Objective / Research Question
- Research Method

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

Research Area



Agenda

Where I fit in

- Research Area
- Research Objective / Research Question
- Research Method

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

Research...

... objective

Trade with and usage of virtual goods shall be modelled in a way that allows for realistic statements about the legal statuses of the parties that are involved.

... question

How can the handling of virtual goods be described in a way that allows for a realistic assessment of the legality of specific actions?

Detailed Definition

1. The model should be able to represent reality
2. In practice, the model should allow users a self-assessment of whether they behave legally

Agenda

Where I fit in

- Research Area
- Research Objective / Research Question
- Research Method

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

Research Method – Design Science Research

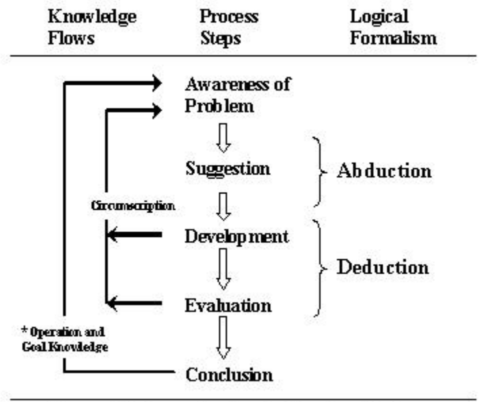


Figure 3. Reasoning in the Design Cycle

Design Science Research according to Vaishnavi und Kuechler [VK04]

Research Method – Design Science Research (cont.)

- Awareness of Problem: mostly done
- Suggestion: mostly done
- Development: partially done
- Evaluation: to be done via implementation
- Conclusion: ???

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

A formal Digital Rights Model without Enforcement

- Article published at the VG 2011, [PG11]
- contains the "mostly done" steps
- Model was recently dubbed "Formosa"

What's already done

Awareness of Problem

Existing digital rights models...

- try to be complete *and* decidable (impossible!)
- focus only on rights holders' perspective
- make unrealistic assumptions about their enforcability
- divide the world into (absolutely) *legal* and (absolutely) *illegal*

What's already done

Suggestion

A new model should…

- not try to be complete
- take the customers' point of view into account
- not assume that enforcement is solved elsewhere
- allow for a "gray area" between legal and illegal

Graduation from legal to illegal in Formosa

- (Illegal) actions can cost a user money
- Their overall debt (= "burden") is tracked
- When the burden crosses a user-defined threshold, the user becomes "too" illegal

What's already done

Development

Formosa...

- is the artefact that has been developed
- has the suggested features
- is written in a "homebrew" notation that uses set algebra and predicate logic
- is an IT security model

Formosa's superior security objective

"Each actor shall be able to subjectively feel secure, even if they perform illegal actions, as long as the potential damage caused to them is below a certain threshold value"

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

- The General Problem of Modelling
- Notation
- Valid Real-World Assumptions?

Bridging the Gaps – Security Model versus Software

Bridging the Gaps – Reality versus Security Model

The General Problem of Modelling

- Models reduce complexity through abstraction
- But: what to take in, what to leave out?
  - Features might prove useful/neccessary later
  - Too many features make the model needlessly complex (cf. “Occam's Razor“)
- Example in Formosa: Time

Occam's Razor according to Heylighen [Hey97]

"[Occam's Razor] admonishes us to choose from a set of otherwise equivalent models of a given phenomenon the simplest one.“

Bridging the Gaps – Reality versus Security Model

The General Problem of Modelling (cont.)

- Earlier versions of Formosa had no notion of time
- Actors only had discrete states
- Time was introduced to allow for duty deadlines and time-limited rights

The downside:

- Actions are still "atomic" (have no duration)
- Progress of time and state changes are now "parallel" concepts

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

- The General Problem of Modelling
- Notation
- Valid Real-World Assumptions?

Bridging the Gaps – Security Model versus Software

Bridging the Gaps – Reality versus Security Model

Notation

- Notation should be maximally comprehensible *and* maximally precise
- Currently: "Homebrew“ notation
- But: does a better notation exist?
- Currently being researched in a master's thesis

Bridging the Gaps – Reality versus Security Model

Notation (cont.)

- Most notations have distinctive features – they might...
    - be easier to read
    - allow for parallel processes
    - have an integrated time concept
    - be computer-interpretable
    - ...
- But not each is apt for security models
- It's impossible to simply *try* them all

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

- The General Problem of Modelling
- Notation
- Valid Real-World Assumptions?

Bridging the Gaps – Security Model versus Software

Bridging the Gaps – Reality versus Security Model

Valid Real-World Assumptions?

- Formosa is based on assumptions about the real world
- Concrete: ”A ‘gray area’ exists in subjectively perceived legality“
- But: does this assumption hold?
- Currently being researched in a master’s thesis

Bridging the Gaps – Reality versus Security Model

Valid Real-World Assumptions? (cont.)

- Many sources (surveys etc.) give hints about the perceptions of VG users
- Many of those...
  - are biased
  - are out of date
  - focus only on specific types of virtual goods
  - contradict each other
- A comprehensive literature analysis might help

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

- Features that TURM has and Formosa doesn't have
- "Open" Definitions in Formosa
- Controllability and Observability

Bridging the Gaps – Security Model versus Software

Software implementation...

- shall become a plug-in for the "Toolkit for URM" (TURM)
- is currently being done in a master's thesis

TURM in a nutshell

- Reference implementation of "Usage Rights Management" (URM)
- URM tries to raise users' awareness of digital rights [HPG09]
- URM existed before Formosa, but they fit together well
- TURM is written in Java

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

- Features that TURM has and Formosa doesn't have
- "Open" Definitions in Formosa
- Controllability and Observability

Bridging the Gaps – Security Model versus Software

Features that TURM has and Formosa doesn't have

- Certain features lack in Formosa (cf. Occam's Razor)
- But: OOP is more manageable
- Should missing features be included in the implementation?
- Example in Formosa: count constraints

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

- Features that TURM has and Formosa doesn't have
- "Open" Definitions in Formosa
- Controllability and Observability

Bridging the Gaps – Security Model versus Software

"Open" Definitions in Formosa

- Formosa uses open definitions for sets that could be arbitrarily large in reality
- Example: *Actors*, *Actionstypes*, ...
- "Oracle functions" don't actually compute anything, but use lookup tables
- Example: *cost* function returns the cost of an action
- But: these lookup tables have to be defined somewhere

Bridging the Gaps – Security Model versus Software

"Open" Definitions in Formosa (cont.)

Solution approach:

- Definitions are read from separate configuration files
- Config files are obtained from central servers
- Config files can be updated regularly
- Sensible default values might often be sufficient

Agenda

Where I fit in

A formal Digital Rights Model without Enforcement

Bridging the Gaps – Reality versus Security Model

Bridging the Gaps – Security Model versus Software

- Features that TURM has and Formosa doesn't have
- "Open" Definitions in Formosa
- Controllability and Observability

Bridging the Gaps – Security Model versus Software

Controllability and Observability

- Traditional DRMS only work when they can control certain activities on users’ computers
- Formosa&TURM does not need to *control* activities, but it has to *observe* them
- In Formosa, actions change states
- But: how can Formosa&TURM observe actions that occur in the system?

Bridging the Gaps – Security Model versus Software

Controllability and Observability (cont.)

Solution approach:

- Create special TURM demon process
- Demon can be inserted into the OS's call chain (example: "xdg-open")
- Demon can track programm calls and warn users when they are about to do something "too illegal"
- Users have to manually inform Formosa&TURM about some actions

Literatur I

Francis Heylighen.
Occam's Razor.
Principia cybernetica web, 07 1997.

Helge Hundacker, Daniel Pähler, and Rüdiger Grimm.
URM – Usage Rights Management.
In Jürgen Nützel and Alapan Arnap, editors, *Virtual goods 2009*, Nancy, France, 09 2009.

Daniel Pähler and Rüdiger Grimm.
A formal Digital Rights Model without Enforcement.
In *Virtual Goods 2011*, 2011.

Literatur II

Vijay Vaishnavi and Bill Kuechler.
Design Science Research in Information Systems.
website, 01 2004.
last updated September 30, 2011.