STSM Report

COST STSM IS0605 6658

Written by
Iztok Starc
University of Ljubljana
Faculty of Computer and Information Science
Slovenia

Host
Prof.Dr. Burkhard Stiller
University of Zürich
Department of Informatics
Switzerland

6. December 2010

Purpose of the STSM

Current trend in the development of computer networks is towards Internet of Things, where especially RFID devices play an important role. Currently, RFID systems are mostly standardized and are widely used with increasing demand in many business applications. But as mentioned, they are becoming interconnected to other networks such as Internet.

This kind of deployment makes them also more open to public access and various threat agents. Thus, networked RFID systems face more threats that may damage business assets when compared to traditional proprietary systems, not to mention privacy risk.

The key objectives of this STSM were to research solutions for enabling quantitative risk management by analyzing the RFID systems specifics, and to develop architecture of an integrating testing platform, which address logical threats effectively and shortens the testing phase of system's security life-cycle.

Description of the work carried out during the STSM

Security management for Embedded Networked Systems

Two views on security management for embedded networked systems were presented. First, a test environment for embedded networked systems and secondly, security metrics and qualitative risk management for embedded networked systems (ENS). The group expressed more interest in the latter, so we put more effort in researching qualitative risk management for ENS. The general information technology risk management model, which formed the basis of our work, is presented in the figure below.

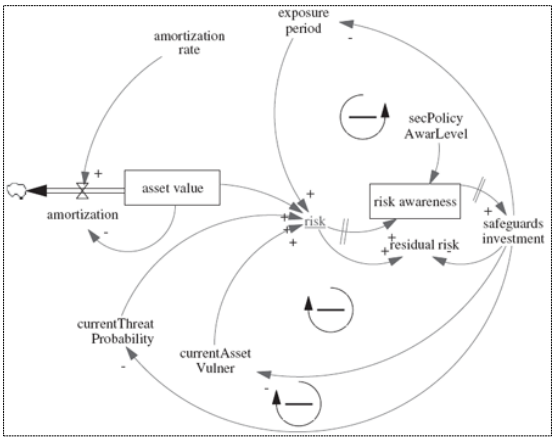


Figure 1: General Information Technology Risk Management System (GIT-RM) Dynamics Model [1]

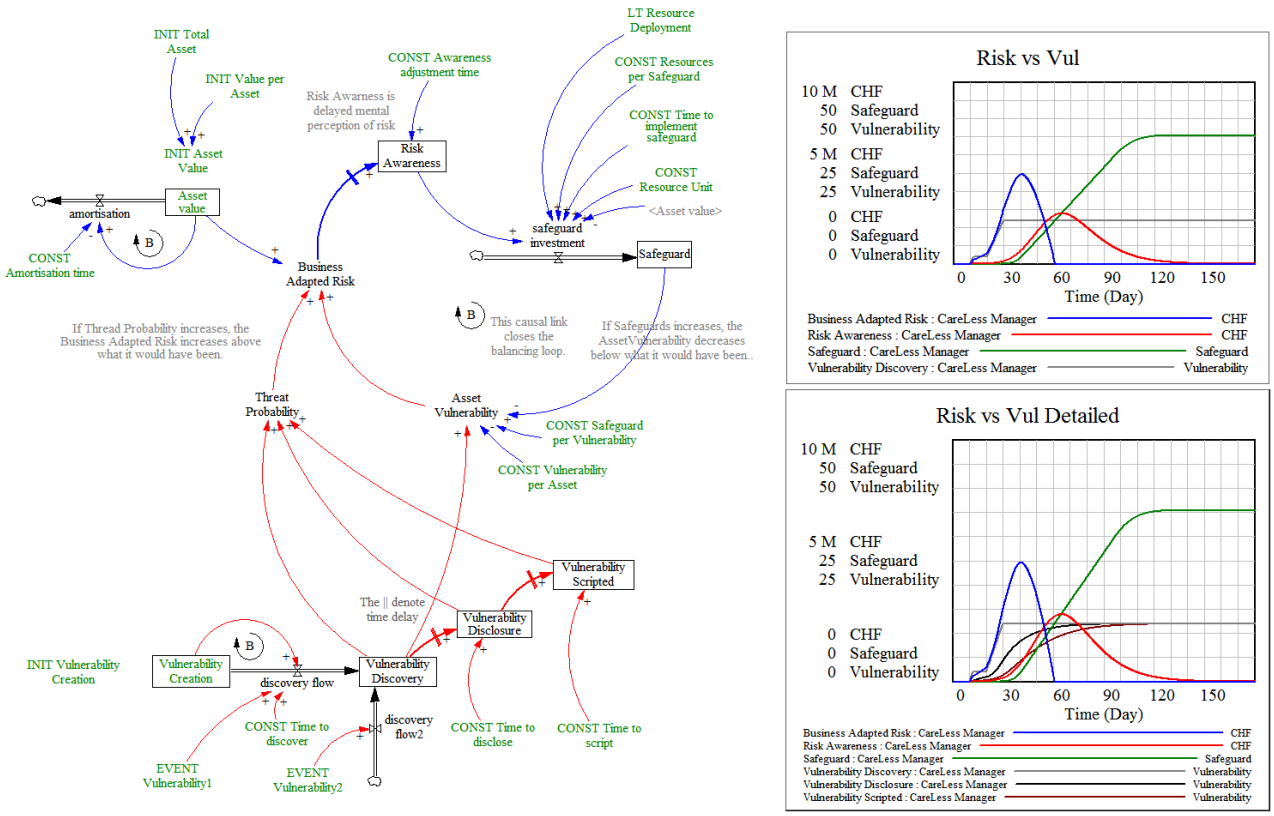


Figure 2: Executable Presentation Model: Implementation of GIT-RM

The basic concept of quantitative risk management can be explained from the figure 1. To show more than just a structure but also behaviour over time an executable model (see the figure 2) was created during the STSM.

This executable model has four scenarios in which risk awareness mental perception is set as: high awareness, average awareness low awareness and the last, careless manager which has the worst reaction time for risk adjustment. In the figure above, the careless manager scenario is presented.

However, we agreed that the implementation of the GIT-RM model above is not accurate enough to capture and be able to reproduce real word behaviour due to the made-up vulnerability data. Vulnerability variables in the lower portion of the figure above are endogenous (endogenous variables have causal link leading to them and are defined by equation).

For the model to reproduce real word behaviour, vulnerability variables should be exogenous (which is complementary concept of endogenous) and should be acquired using either vulnerability database or/and feed from local area network.

To close this gap, vulnerability data acquisition architecture has to be defined, implemented and connected with the model and finally tested to validate the model's behaviour over time. The definition of the vulnerability data acquisition architecture was one of the objectives of the STSM.

To develop this subject further, a notation and simulation System Dynamics [2] tutorial was shown to the group using IPv4 to IPv6 adoption model as a case study (see the figure below). It is based on Bass diffusion model. Three different scenarios were used to demonstrate basic concepts. Some advanced concepts such as sensitivity analysis, optimisation and games were presented as well.

IPv4--2--IPv6 ADOPTION MODEL

MOTIVATION

IPv4 addresses will deplete and Internet will have to migrate to IPv6 eventually. We are interested in dynamics behavior of this IPv6 adoption process.

SENSITIVITY ANALYSIS

A policy maker might ask: "What is the sensitivity of IPv6 and Subsidy Total Cost for HiSubsidy Scenario if CONST Absolute Satisfaction Norm is uncertain?

OPTIMISATION

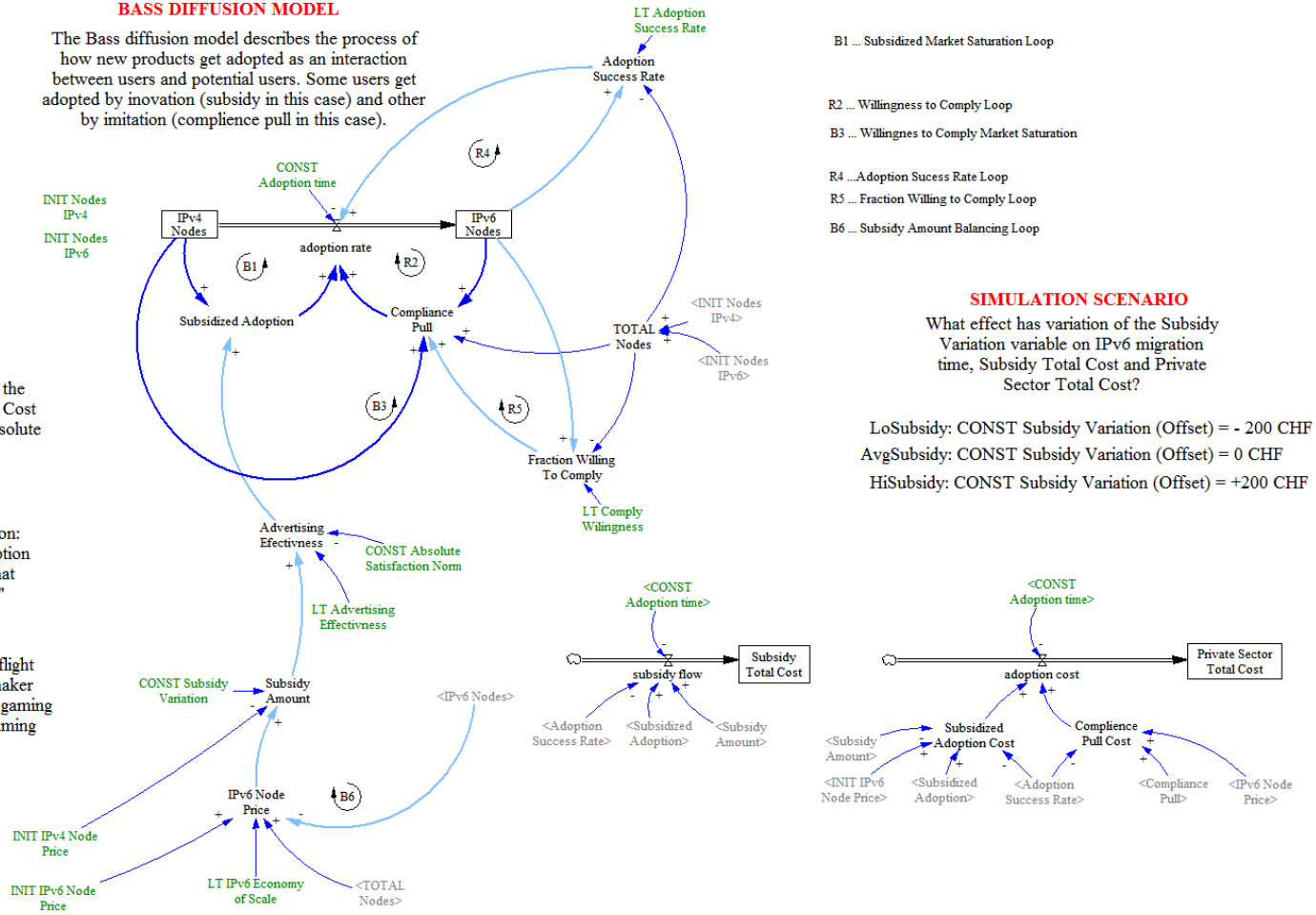
A policy maker might raise a question: "We would like to achieve IPv6 adoption with the following dynamics ... What subsidy amount should we offer?"

GAME

In order to train decision makers, a flight simulator is created. The decision maker interact with the simulator and adjusts gaming variable values to compensate the gaming behavior.

BASS DIFFUSION MODEL

The Bass diffusion model describes the process of how new products get adopted as an interaction between users and potential users. Some users get adopted by inovation (subsidy in this case) and other by imitation (complience pull in this case).



B1 ... Subsidized Market Saturation Loop

R2 ... Willingness to Comply Loop

B3 ... Willingnes to Comply Market Saturation

R4 ...Adoption Sucess Rate Loop

R5 ... Fraction Willing to Comply Loop

B6 ... Subsidy Amount Balancing Loop

SIMULATION SCENARIO

What effect has variation of the Subsidy Variation variable on IPv6 migration time, Subsidy Total Cost and Private Sector Total Cost?

LoSubsidy: CONST Subsidy Variation (Offset) = - 200 CHF

AvgSubsidy: CONST Subsidy Variation (Offset) = 0 CHF

HiSubsidy: CONST Subsidy Variation (Offset) = +200 CHF

Figure 3: Introduction to System Dynamics notation, simulation and advanced concepts such as Sensitivity Analysis, Optimisation and Games using an executable IPv4 to IPv6 adoption model as a case study

During the last two weeks of the STSM, a vulnerability data acquisition architecture for a local area network was defined (see the figure below) and can be explained in the following way. Each device has its own auditing agent that measures the impact factor in real-time and submits vulnerability data using SNMP protocol to a central network monitoring tool like Nagios or OpenNMS. Collected data of all agents is used (and transformed) to calculate system impact factor for a given scenario [4]. This data is fed to the GIT-RM model to enable pro-active risk treatment. This satisfies the objectives of the STSM.

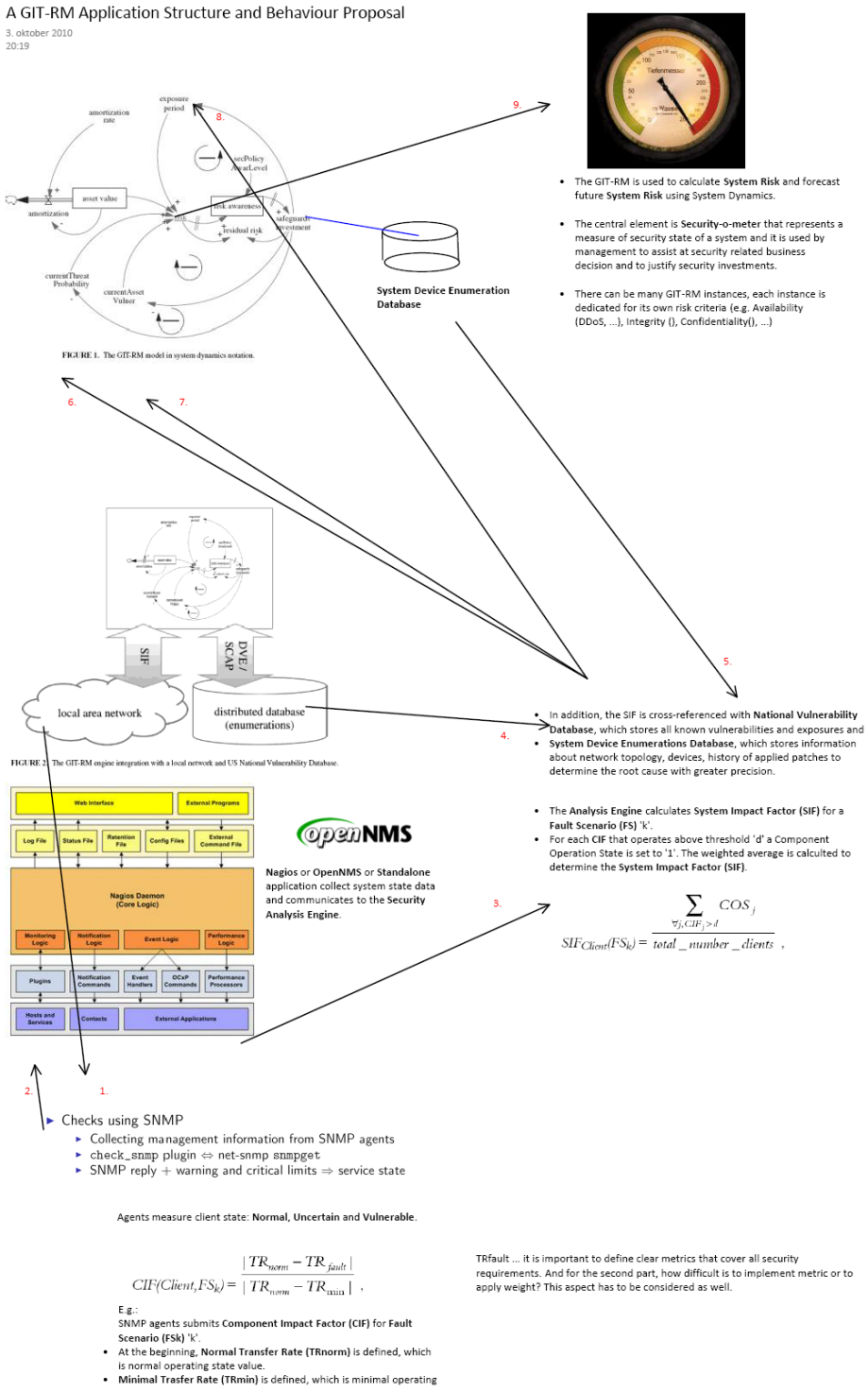


Figure 4: GIT-RM and Local Area Network Data Acquisition Architecture Concept Model

Modelling implications of internet jurisdiction

In addition, we figured out that System Dynamics could be applied to another interesting research area - Internet jurisdiction. Even though it was out of the scope of the STSM objectives, this topic remains within interests of the COST Econ@Tel.

In particular, during the last week we collaborated on policy implication of a transition to harmonized private international law for electronic business. In other words, long-term transition from a private international law (PIL) was investigated, from a point where each state defines its own PIL law, towards single, harmonized PIL for electronic business in the Internet using System Dynamics as a holistic approach to understand this complex (feedback) system. For boundary articulation and model development a conference paper of Waldburger, Macri and Stiller [5] was used. Our objective was:

- To provide insight in the root of problem for a given scenario;
- To improve system behaviour using different policies, which are designed, tested and optimised.

Stake- and shareholders were identified and classified. Associations between stake- and shareholders were mapped. Basic indicators for each stake- or shareholders were defined. On a basis of this information a non-executable baby model was created (see figure below) and an extended abstract for EuroCPR 2011 conference paper was written, submitted but sadly, not accepted (see Appendix A).

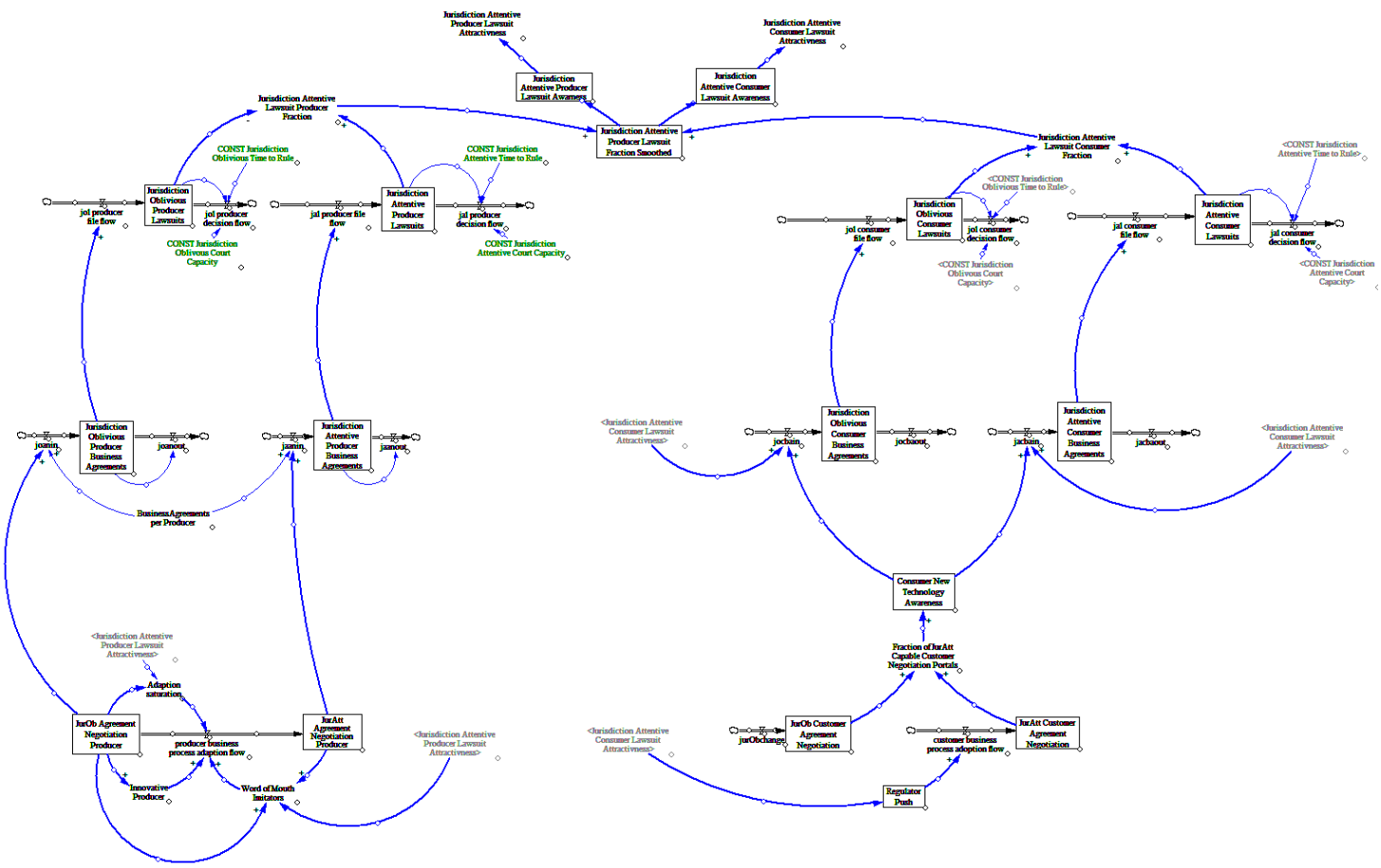


Figure 5: System Dynamics baby model: Transition to harmonized PIL model

Description of the main results obtained

The following main results were obtained:

1. The vulnerability data acquisition architecture for a local area network was defined for the general information technology risk management model.
2. For a purpose of vulnerability data collection, Nagios and OpenNMS, open source and industry standard network monitoring tools, were identified.

3. Extended abstract for EUROCPR 2011 conference was written.

Foreseen publications resulting or to result from the STSM

Extended abstract for EUROCPR 2011 conference was submitted but unfortunately rejected.

Future collaboration with the host institution

In the year 2011 we are planning for a second exchange to intensively collaborate and finish the model development. We aim to further develop the “Transition to harmonized PIL” baby model in a full grown model as well as improve the paper and publish it.

Acknowledgement

I am grateful to the Management Committee of the Econ@Tel COST Action IS 0605, especially to Chair Prof. Dr. Burkhard Stiller and Co-chair Prof. Dr. Louis-Francois Pau for granting the funding of this STSM.

I would like to thank my host Prof.Dr. Burkhard Stiller for all the time and effort put in organizing this STSM as well as Mrs Evelyne Berger for her help in finding accommodation in Zürich.

Special thanks go to Martin Waldburger and Prof.Dr. Burkahrad Stiller for their warm welcome, hosting and providing help and guidance during my stay in Zürich.

Finally, many thanks (alphabetical order) go to Andrei Vancea, Prof. Dr. Burkahrad Stiller, Fabio Hecht, Guilherme Machado, Hasan and Martin Waldburger for all enlightened discussions, feedback, friendly advices and cooperation. Thank you!

Literature

[1] D. Trček, “Security Metrics Foundations for Computer Security,” *The Computer Journal*, Nov. 2009.

[2] J.W. Forrester, *Industrial Dynamics*, Pegasus Communications, 1961.

[3] J. McHugh, W.L. Fithen, and W.A. Arbaugh, “Windows of vulnerability: a case study analysis,” *Computer*, vol. 33, 2000, pp. 52-59.

[4] S. Hariri, T. Dharmagadda, M. Ramkishore, and C.S. Raghavendra, “Impact analysis of faults and attacks in large-scale networks,” *IEEE Security & Privacy Magazine*, vol. 1, Sep. 2003, pp. 49-54.

[5] Martin Waldburger, Alessandra Macri, Burkhard Stiller: Service Provider Market Activities Constituting Jurisdiction for International Service Contracts—A Structuring Approach and Techno-legal Implications. 21st European Regional ITS Conference, published by the ITS 2010 conference, pages 1-22, Copenhagen, Denmark, September 2010.

Appendix A

Policy Implications of a Transition to Harmonized Private International Law for Electronic Business

Martin Waldburger[1], Iztok Starc[2], Burkhard Stiller[1], Denis Trček[2]

[1]*University of Zürich, Department of Informatics (IFI), Communication Systems Group (CSG)*
Binzmühlestrasse 14, CH–8050 Zürich, Switzerland, [waldburger\|stiller]@ifi.uzh.ch
[2]*University of Ljubljana, Faculty of Computer and Information Science,*
Tržaška c. 25, SI-1000 Ljubljana, Slovenia, [iztok.starc\|denis.trcek]@fri.uni-lj.si

Extended Abstract

THE set of available dispute resolution means determines a key contractual parameter in any type of contract. Dispute resolution provisions embrace typically questions of jurisdiction and applicable law. In cross-border business transactions, jurisdiction and applicable law are of special importance as jurisdiction refers to which state's courts have authority to hear and decide a dispute, while applicable law refers to which state's law is to be used in order to come to a decision.

Due to the principle of state sovereignty, each state may define its own Private International Law (PIL) governing the state-specific set of connecting factors based on which own or foreign jurisdiction is established, application of own or foreign law is substantiated, and recognition of foreign decisions is granted or denied. This territorial approach to dispute resolution makes PIL a highly complex field of law, in particular in an increasingly international and digital economy.

This is why several efforts in harmonizing PIL have appeared. For member states of the European Union (EU), for instance, the two main harmonized PIL instruments are the Brussels I regulation [1] (for questions of jurisdiction) and the Rome I regulation [2] (for questions of applicable law). Despite ongoing harmonization endeavors in different regions and in different bodies, previous research reveals that fundamental challenges in handling dispute resolution remain essentially unaddressed in market places which are border-less, *a priori* — the Internet being a prominent example.

On the one hand, a system to produce in an automated manner a list of recommended jurisdictions for a contract of an electronic service in the Internet — *e.g.*, a content service — was designed and prototypically implemented [4, 6]. To this aim, a method to formally model PILs in a machine-executable way, and to implement the respective jurisdiction-oriented reasoning was determined. In order to show the feasibility of this approach, as well as its limitations, the Brussels I regulation was modeled and implemented [4]. The approach has proven fully functional, *per se*, but even with regionally harmonized PILs like the Brussels I regulation in place, scalability on a global scale remains challenging due to a considerable modeling and implementation effort for each PIL to be covered. In addition, questions of conflicting recommendations and mutual recognition among modeled PILs have not been addressed. In essence, this approach shows that the territoriality principle of PIL may be supported in the Internet to some extent, while it would clearly suffer from severe issues had PILs of as many states to be modeled and implemented as exist to date.

On the other hand, an embracing comparative analysis of the PIL situation in the USA, the EU, and in China resulted in the identification of service provider market activities that may constitute jurisdiction in these regions investigated [5]. To that aim, the set of region-specific connecting factors was compiled and assessed based on a common frame for comparison developed. Connecting factors were mapped to service provider market activities in the Internet (*e.g.*, targeted on-line advertisements) and the real world (*e.g.*, presence by means of distrainable property). The accordingly conducted assessment of techno-legal implications revealed that both, service providers and service customers, are confronted with a high level of jurisdictional risk and uncertainty in dispute resolution when doing international electronic business in the Internet. In essence, this research effort shows that the current approach to cross-border dispute resolution as reflected by PIL of today fails for international electronic business in the Internet.

Therefore, a transition towards a single, internationally harmonized PIL for electronic business in the Internet is perceived as the dominant long-term strategy in order to foster certainty and trust in international electronic business substantially. Such transition needs time as it involves a large number of stakeholders which may have differing agendas, interests, and objectives. Accordingly, this paper is concerned with the following research question: Which policy implications for different policy proposals under changed scenario assumptions result form a long-term transition to a harmonized, electronic service provisioning-adapted PIL in an interconnected system of service providers, service customers, courts, lawyers, and policy makers?

The policy implications result from complex system behavior. In order to understand the modeling method System Dynamics [3] is used. System Dynamics was founded in 1960. It is a well established modeling methodology used to address business, social, socio-technical, and dynamic decision

making problems. System Dynamics is a holistic approach to understand a complex feedback system that is comprised of interacting parts. Feedback describes a specific situation of interacting parts that form a causal loop. *E.g.*, policy makers affect service providers which in turn affect policy makers through a sequence of causes and effects.

This holistic approach to complex feedback system understanding is especially important to determine the correct behavior of the system, because studying single cause and effect relations in isolation would lead only to partial results and could miss some of the behavior that might arise. Furthermore, the model structure is mathematically formalized by describing the structure with a set of difference equations, and a computer-aided approach is used to simulate the model using numerical methods to determine system behavior. The model is tested and refined in iterative processes to reproduce real-world behavior. Finally, policies are designed and evaluated for real-world improvement.

This paper provides a number of results in relation to the simulated long-term transition to a harmonized PIL for electronic business in the Internet:

- The model structure provides insight in the root of problems of this complex feedback system.
- Behavior over time for key indicators and variables is presented for different scenarios.
- Policies are designed, tested, and optimized for these scenarios to improve system behavior.

Since no empirical historical data set is known for model validation at this point (the simulated transition has not happened yet), expert opinion is used to build confidence in the model. This model is perceived as an input to trigger awareness and discussion among policy makers and other influencing stakeholders.

References

[1] Council of the European Union. *Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters*. *Official Journal of the European Communities*, L12:1–23, Jan. 2001.

[2] European Parliament and the Council of the European Union. *Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I)*. *Official Journal of the European Union*, L177:6–16, July 2008.

[3] Forrester J. W. *Industrial Dynamics*. Productivity Press, Cambridge (MA), USA, pages 1–479, 1961.

[4] Waldburger M., Charalambides M., Schaaf T., and Stiller B. *Automated Determination of Jurisdiction and Applicable Law for International Service Contracts: Modeling Method, Information Model, and Implementation*. In 18th Biennial and Silver Anniversary International Telecommunications Society Conference (ITS 2010), pages 1–31, Tokyo, Japan, June 2010.

[5] Waldburger M., Macri A., and Stiller B. *Service Provider Market Activities Constituting Jurisdiction for International Service Contracts—A Structuring Approach and Techno-legal Implications*. In 21st European Regional ITS Conference (ITS 2010), pages 1–22, Copenhagen, Denmark, Sept. 2010.

[6] Waldburger M. and Stiller B. *Automated Contract Formation for Electronic Value-added Services in the Internet—The Case of Bandwidth-on-Demand Contracts in Europe*. In 37th Research Conference on Communication, Information and Internet Policy (TPRC 2009), pages 1–30, Arlington (VA), USA, Sept. 2009.