DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF TORONTO

TECHNICAL REPORT #CSRG-614

Released October, 2011

Submitted April, 2007

Modeling and Analyzing Technology Strategies

Jennifer Horkoff
Department of Computer Science,
University of Toronto
40 St. George St.,
Toronto, Ontario, Candada
+1 416-978-3107
Jenhork @ cs.utoronto.ca

Eric Yu
Faculty of Information Studies,
University of Toronto
140 St. George St.,
Toronto, Ontario, Canada
+1 416-978-3107
Yu @ fis.utoronto.ca

ABSTRACT

As technology design becomes increasingly motivated by business strategy, technology users become wary of vendor intentions. Conversely, technology producers must discover strategies to gain the trust of consumers. Both parties have a need to understand how business strategies shape technology design, and how such designs alter relationships among stakeholders. In this work, Trusted Computing technology, part of a potential infrastructure for E-Business Services, is used as an example. Can consumers trust the advertised intentions of Trusted Computing? Can technology producers gain the trust of consumers? We propose the use of the i* Modeling Framework and the qualitative i* evaluation procedure to analyze the links between strategies and technologies in terms of a network of social intentional relationships.

KEYWORDS

Trust, Trusted Computing, Business Strategies, The i Framework, Model Evaluation.*

1. INTRODUCTION

As technology becomes progressively more difficult to understand and increasingly entwined with product marketing, our concern for personal security and autonomy in the use of technology grows, and our trust in technology providers is put at increasing risk. When the motivations and intentions behind technological products become murky, there is an increased need for individual consumers and businesses to understand these motivations and their effects, in order to protect their interests. Customer lock-in, misrepresentation of functionality and diminished compatibility with competitors' products are examples of some of the strategies that may influence technology. Such strategies may affect the ability of technology to provide effective support for interoperable web-based applications. Further complicating the situation is the varying and contrasting reports concerning the intention of technologies. The vendor may paint one picture of a product while a competitor paints another, and a third party analyst may offer a different opinion yet again. How can the consumer digest and analyze information from all these viewpoints? Conversely, product success relies on consumer confidence. In an atmosphere of increased suspicion, how can the vendor win the consumer's trust?

This situation calls for a method to analyze technology designs in relation to business strategies, including the influence of trust. We need a way to analyze how a particular design contributes positively or negatively to the strategic interests of consumers and technology vendors. If a clearer picture of contradicting information concerning technology implications

is constructed, facilitating the communication of different points of view, an informed debate may be provoked, and a consumer or business may use their increased knowledge to make better-informed decisions.

In this work, we facilitate the needed understanding and analysis by modelling the intentions and social relationships among stakeholders involved in technological systems. We analyze the trust that stakeholders have in each other in terms of contributing factors such as security and privacy. The models are created using the i* Modeling Framework, introduced by Yu in [31]. Unlike other common modeling notations used in software engineering such as the Unified Modeling Language (UML), the i* Framework is intended to explicitly represent the intentions of domain entities in a social network, represented as actors. Such models represent not only how things occur in a domain, but also why they occur.

The outline of this work is as follows. We begin by arguing the need for a systematic approach to consider the relationships between business strategies and technology, with an emphasis on the role of trust. After pointing to several example domains, we focus on the issues surrounding Trusted Computing. We briefly introduce our approach: the i* Framework using a qualitative evaluation procedure. We provide a detailed walk-through of our analysis of the Trusted Computing domain, depicting the major controversies in the domain. In order to introduce the material gradually, some technical details are postponed to later sections. Finally, we review related research, discuss the contributions and limitations of our approach, and outline future work.

2. SYSTEMATIC ANALYSIS OF TRUST IN TECHNOLOGY STRATEGIES

With the introduction of a multitude of new technologies with impressive functionality, often the focus is placed on the specifics of what the technology can do and not on why the consumer needs the technology, or why the producer has chosen to sell a particular technology. Although consumer demand certainly plays a role in motivating new product development, the strategies behind the production of specific technology and product features are often far more complex. One could even argue that demand for products is often created by marketing and media instead of being driven by real needs. Embedded in this situation is the role of trust. The effectiveness of product marketing and other business strategies relies on some level of trust, either explicit or implicit, of consumers on the technology producers. Producers, in turn, employ strategies in order to gain this trust,

although their consideration of consumer trust may also be performed implicitly.

The situation calls for a way to explicitly consider the effects of trust in technology strategies, both from the point of view of the technology producer and the consumer. We would like to be able to answer questions such as:

(i). What are the goals of each stakeholder? What do they want to achieve?

(ii). Can the goals of stakeholders be met?

(iii). What are the business strategies underlying the introduction of certain technologies? How do these strategies achieve the goals of the technology producers?

(iv). How does the technology implement such business strategies?

(v). Is the trust of the consumer necessary in order for such strategies to be successful?

(vi). Is consumer trust effectively gained? Through what means is trust gained or lost?

Finding the answers to such questions will aid the technology consumer in making informed decisions concerning their purchase and use of technology, and will aid the technology producer in creating effective strategies to acquire and retain consumer business.

We can think of various domains in which this type of analysis can prove useful. Consider the use of smartcards. Ostensibly, the role of such technology is to store information such as a monetary balance, allowing for easy transactions. However, one can question the existence of underlying business strategies involving the collection or distribution of transaction information, perhaps for marketing purposes. Thus, the role of the user's trust in card providers and accepting businesses becomes important. Can users trust smartcard participants? What strategies do participating businesses use to gain the trust of card users? How do these strategies affect the goals of all parties involved?

Further examples of domains where strategy and trust analysis would prove useful include online shopping involving the disclosure of consumer information, the use of technology in healthcare (e-health situations), and the interoperable applications used for business cooperation.

Previous studies have considered the nature and potential representations of trust. For instance, Gambetta [8] considers trust as reaching a particular threshold over the subjective probability of an action being performed. Castelfranchi and Falcone [7] expand on the quantitative treatment of trust by suggesting the

explicit consideration of the necessary mental ingredients of trust such as beliefs, goals, and delegation decisions.

However, such approaches do not explicitly consider the relationship between trust and technology strategies. Furthermore, when dealing with high-level social concepts such as business strategies, it can be difficult to find and use quantitative measures which are based on accurate domain data.

We approach the analysis of trust in technology strategies by applying socio-technical modeling and reasoning. By explicitly modeling trust, domain actors, their intentions, and the relationship between these elements, we are able to elucidate the role of trust in technology strategies. Our work with the i* modeling framework differs from other approaches to trust in that we treat the trust that one actor has in another actor as a goal to be achieved. We evaluate whether the goal is achieved by evaluating contributing factors such as the achievement of security and privacy. The trust goal, in turn, contributes to other goals such as purchasing technology. If trust is not achieved, we conclude that purchasing technology is not viable.

We make the claim that by applying intentional modeling to domains involving trust and technology strategies, we are able to effectively answer the questions outlined above. By explicitly modeling the intentions of technology producers, we can gain an understanding of the business strategies employed. With the inclusion of concrete technological operationalizations of those strategies, we can clarify and pinpoint the specific links between technology and strategies. By capturing the implementation of such strategies, we can analyze whether or not the acquisition of consumer trust is necessary for the success of technology producers. Through model evaluation, we can determine the achievement of stakeholder goals including trust, and analyze how the implementation of certain strategies via the introduction of specific technologies affects the goals of all parties involved. We demonstrate our claims by applying i* to the issues surrounding Trusted Computing.

3. TRUSTED COMPUTING

Trusted Computing (TC) refers to technology, applicable to personal computers and other personal electronic devices, which has been proposed by a set of technology vendors, now represented by the Trusted Computing Group (TCG) [29]. Such technology has the potential to play a pivotal role in the emerging area of E-Business Services, acting as a crucial part of the supporting infrastructure. The demand for such services makes the issues surrounding trust, privacy and security prominent. From the point

of view of Trusted Computing Proponents, the technology is being introduced as a means to address such issues. For instance, proponents of TC have claimed that it will promote security for the average user while not preventing the use of pirated content. However, the parties who are opposed to the technology claim that it will in fact give control of technology to technology vendors, effectively threatening security. Trusted Computing opponents claim that the primary motivation for the technology is to combat software piracy and further implement digital rights management (DRM).

The Trusted Computing context serves as an interesting case study to illustrate our modelling technique due to the presence of multiple viewpoints concerning technology strategies, and the resulting uncertainty surrounding trust, privacy, and security.

In analyzing the issues surrounding Trusted Computing we would like to answer the following questions:

(i). What are the goals of the Technology Producer? Technology User? Other relevant stakeholders?

(ii). Can these goals be achieved? In what situations?

(iii). What are the business strategies underlying the implementation of TC?

(iv). How are these strategies implemented by TC Technology?

(v). Is the trust of the consumer necessary in order for the underlying strategies to be successful?

(vi). Can TC producers gain the trust of the consumer? Through what means is trust gained or lost?

Can intentional modeling effectively answer these questions? Due to the presence of conflicting viewpoints, our analysis produces several answers to each question, from the point of view of TC proponents and opponents.

4. THE i* FRAMEWORK

In order to answer the questions outlined in section 3, we identify and model domain actors, such as the technology user and provider, and represent their needs and wants, as well as the relationships among them. Figure 1 shows a simplified example of such a model, depicting the internal motivations and the relationship between the Technology Provider and the Technology User in the Trusted Computing domain.

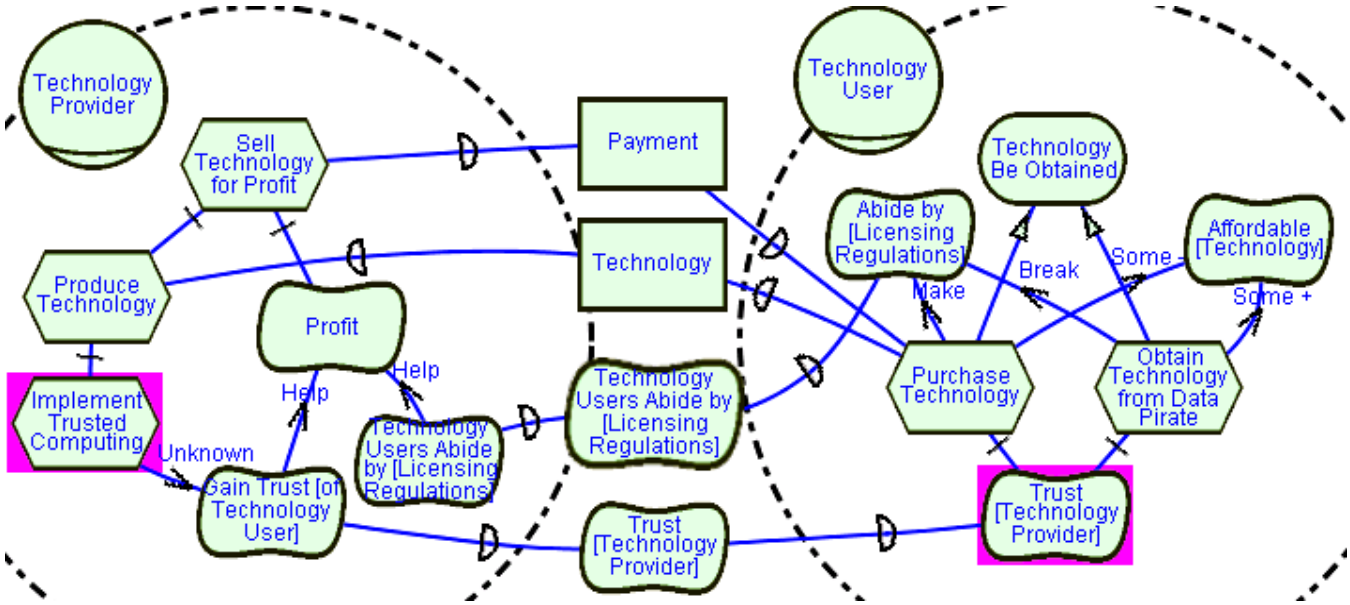

Figure 1. Simplified TC Model

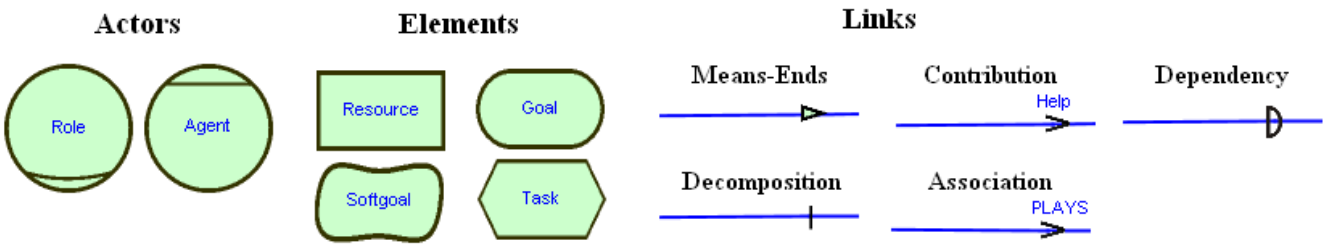

Figure 2. Legend of i* Constructs

The i* Framework, (i* for distributed intentionality), depicts the intentional relationships between actors using elements, links between elements, actors, and actor association links. As the high-level, social analysis for which i* is intended involves many uncertainties in a wide variety of potential situations, strictly determining the steps of a modeling process is thought to be too restrictive. As a result, the Framework leaves the specifics of a formalized modeling method open.

Elements in i*. i* elements include goals, tasks, resources, and softgoals. These elements are intentional in that they represent an actor's desires. A **goal** is a desired state in the world. **Tasks** and **resources** are needed for achieving goals. **Softgoals** are goals whose criteria of attainment are not precisely defined, thus requiring further interpretation and elaboration.

A model is evaluated by associating each element with a value (or label) indicating whether the element is achievable. The value for an element

is computed from values contributed by other elements, starting from inputs provided by the modeller. As softgoals do not have precise criteria for determining their satisfaction, we used the term "satisficed", to refer to a judgment of sufficient satisfaction, following Simon [26]. This notion of softgoal was introduced in the NFR framework [4] to deal with non-functional requirements in software engineering. In our approach, we model trust as a *softgoal*, effectively treating trust as a non-functional requirement (NFR) alongside other NFRs such as usability and extensibility. The achievement of trust of one actor by another actor is assessed from the point of view of some (possibly third) actor in the domain.

Links in i*. Elements are connected by links. A **decomposition link** between a task and its sub-elements is used to represent the elements which must be accomplished in order for a task to be accomplished. Sub-elements can include a mix of goals, softgoals, resources, as well as tasks. A **means-ends link** from a task to a goal represents one way to achieve that goal. Modellers are encouraged to find and represent multiple means or alternatives to accomplish any given goal. A **dependency link** states that an actor (the depender) depends on another actor (the dependee) for something (the dependum). A **Contribution link** from an element (of any type) to a softgoal indicates a qualitative contribution effect. When the contribution is strong enough to satisfice or deny the softgoal, we call it a *Make* or *Break* link, respectively. If we know that the contribution is not strong enough to satisfice or deny the softgoal, we call it a *Help* or *Hurt* link. When positive or negative contributions exist and we are unsure of whether or not they are strong enough to satisfice or deny a softgoal, we call it a *Some+* or *Some-* link. When a contribution exists which is not known to be positive or negative, we use an *Unknown* contribution link.

Actors in i*. Elements in i* are either inside an **actor boundary** – (represented as a dashed circle which contains elements) or appear as dependum between actors. Placing an element within an actor boundary indicates that the element is desired by that actor, although this desire may be indirect as a means to achieve another desired element. An **actor** can be a **role**, representing an abstract set of duties, or an **agent**, representing concrete people or systems. The relationships between actors are described by **association links**, such as the **PLAYS** link, indicating that an agent plays a role. See Figure 2 for a legend of i* constructs.

When analyzing the business strategies underlying technology, i* models may be created by analysts who are assessing a technology, such as commentators or researchers, or by business

insiders, who are aiming to find technology designs which will be effective in satisfying their business goals without alienating consumers.

5. THE i* EVALUATION PROCEDURE

Constructing an i* model showing relationships among goals and how they are achieved can provide valuable insights about the domain, helping to facilitate understanding and communication. However, to facilitate further analysis, a qualitative reasoning method is provided to evaluate whether goals can indeed be achieved. The i* evaluation procedure, detailed in [13], is adapted from a procedure originating the NFR Framework [4]. In this section, we explain the evaluation procedure, using the simplified Trusted Computing model in Figure 1 for illustration.

The i* evaluation procedure facilitates analysis by applying labels representing the level of evidence towards the qualitative satisfaction or denial of model elements. These labels represent evidence which is sufficient to satisfy or deny an element (**satisficed/denied**), evidence which is positive but not in itself sufficient to satisfy or deny an element (**partially satisficed/denied**), evidence with an unknown effect (**unknown**), and the presence of both positive and negative evidence which are judged to be roughly equivalent (**conflict**). Here, the term "satisficed" is used to mean sufficiently satisfied.

Concerning the use of partial labels (partially satisficed, partially denied), typically, one would think of the partial labels as being applied only to qualitative softgoals, with the "full" labels (satisficed, denied, unknown, conflict) applied to "hard" elements (goals, tasks, and resources). However, in this work we use qualitative partial labels for such "hard" elements as well, in order to increase the expressive power of the evaluation. Otherwise partial labels would often have to be "rounded off" to full labels, losing potentially valuable evaluation results. See Figure 3 for an example.

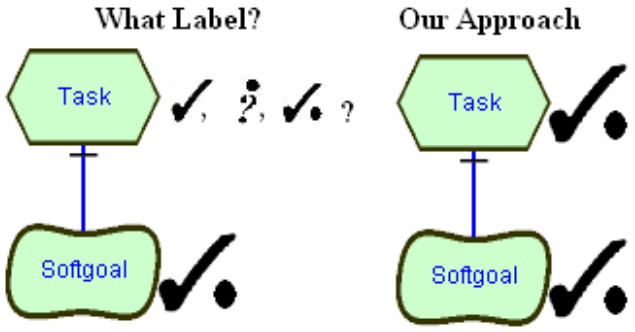

Figure 3. Partial Labels to Hard Elements

Initial Labels. The procedure starts with a set of initial labels given to "leaf elements" in the graph, i.e., elements having no input links. As a visual aid these are highlighted with a rectangular block background. In Figure 1, for example, there are two leaf elements, the Implement Trusted

Computing task and the Trust [Technology Provider] softgoal. Initial labels are selected by posing an analysis question. For example, in Figure 1, the analyst may ask: "If the Technology Provider chooses to Implement Trusted Computing, but the Technology User does not Trust the Technology Provider, how will this affect the goals of both actors?" In this case the evaluation would be started with initial labels of satisficed for Implemented Trusted Computing and denied for Trust [Technology Provider].

Initial labels can, less commonly, be given to elements which are not leaf elements, if the analyst wants to explore the propagation of specific labels from these elements. For example, an analyst might want to know the effect of Obtain Technology from Data Pirate, regardless of the effects of Trust on this task, and will therefore place an initial label of satisficed on this task. The initial labels discussed have been placed on the Figure 4 model.

Step 1. In the first step of the procedure, after initial labels have been placed, a set of propagation rules are used to propagate evaluation labels from elements to other elements via the model links. The propagation rules for contribution links as well as the graphical representation of element labels are shown in Table 1. These rules reflect the semantics of the contribution links. The Make link propagates the evidence it receives without modification. The Break link propagates the inverse of the evidence it receives, with the exception of a denied label, which is propagated as partially denied with the idea that the denial of a break is not strong enough to produce a satisficed value. Help/Some+ and Hurt/Some- links are similar to Make and Break links, respectively, except that sufficient evidence is weakened to partial evidence, taking the pessimistic interpretation of Some+ and Some-. Unknown links and unknown values always propagate unknown values, and conflict values are propagated as conflict values, unless through an Unknown link. As softgoals may be affected by multiple contribution links, multiple labels may be received. These labels are stored with the element in a bag of labels until resolution in step 2.

Table 1. Propagation Rules Showing Resulting Labels for Contribution Links

Originating Label		**Contribution Link Type**						
Label	Name	Make	Break	Help	Hurt	Some+	Some-	Unknown
✓	Satisficed	✓	✗	✓.	✗.	✓.	✗.	?
✓.	Partially Satisficed	✓.	✗.	✓.	✗.	✓.	✗.	?
↯	Conflict	↯	↯	↯	↯	↯	↯	?

?	Unknown	?	?	?	?	?	?	?
✗?	Partially Denied	✗?	✓?	✗?	✓?	✗?	✓?	?
✗	Denied	✗	✓?	✗?	✓?	✗?	✓?	?

Evaluation values in decomposition links are propagated as-is from dependee to dependum to depender. In means-ends links, the propagation is treated as an OR relationship, taking the maximum value of the contribution elements.

In decomposition links propagation is treated as an AND relationship, taking the minimum value. The maximum and minimum labels are determined by an ordering of most positive to most negative, as follows:

✓ > ✓? > ⚡ > ? > ✗? > ✗

Step 2 continues until the queue of labels to propagate, initially populated by initial labels, is empty.

Step 2. In the second step of the procedure, the labels in the bag of labels received by each element are combined to produce an overall label for each element. In some cases, such as when there is only one label, or when combining full and partial positive evidence, the final label for an element can be determined automatically. For example, the combined label of an element receiving the labels {✓, ✓?} can be set automatically to ✓, as the qualitative evidence is viewed as roughly cumulative.

In other cases, such as when an element has received both positive and negative evidence, or when there is no source of sufficient evidence, human judgement based on contextual knowledge is used to determine an overall element label. As i* models represent social, and intentional aspects of the domain, often expressing the complex needs of people, such models are typically incomplete, in the sense that further detail could always be added. In practice, we aim to produce models which are sufficiently complete to facilitate useful analysis and insight, and to encourage clarification of understanding and communication, possibly provoking further inquiry. In this light, there is a continual trade-off between completeness and complexity.

The intrinsic incompleteness of i* models makes it necessary, in some cases, to supplement the model with tacit knowledge from the modeller, in order to determine the satisfaction of model elements. The need for such intervention likely indicates areas where elements or contributions are missing from the model, or where there are subtleties that are difficult for the modelling notation to capture. In some cases, the tacit knowledge could be made explicit by expanding

or modifying the model. In other cases, one might opt for simplicity and readability at the expense of completeness.

In Figure 4, we have completed the evaluation by propagating the effects of the initial labels discussed previously. Areas requiring human intervention are highlighted with a green circle. For example, the Affordable [Technology] softgoal receives two partially satisficed labels in its bag ({✓, ✓}). We determine that the effects of Obtaining Technology from the Data Pirate without Purchasing Technology are sufficient to mark Affordable as satisficed. This decision is made based on the context of the model, the identity and meaning of contributing and recipient elements. The Gain Trust [of Technology User] softgoal contained labels of denied and unknown in its label bag ({✗, ?}). We decide to emphasize the unknown effects of Implement Trusted Computing by marking this softgoal as unknown. We make a similar choice for the Profit softgoal, having a label bag of {✗, ?}.

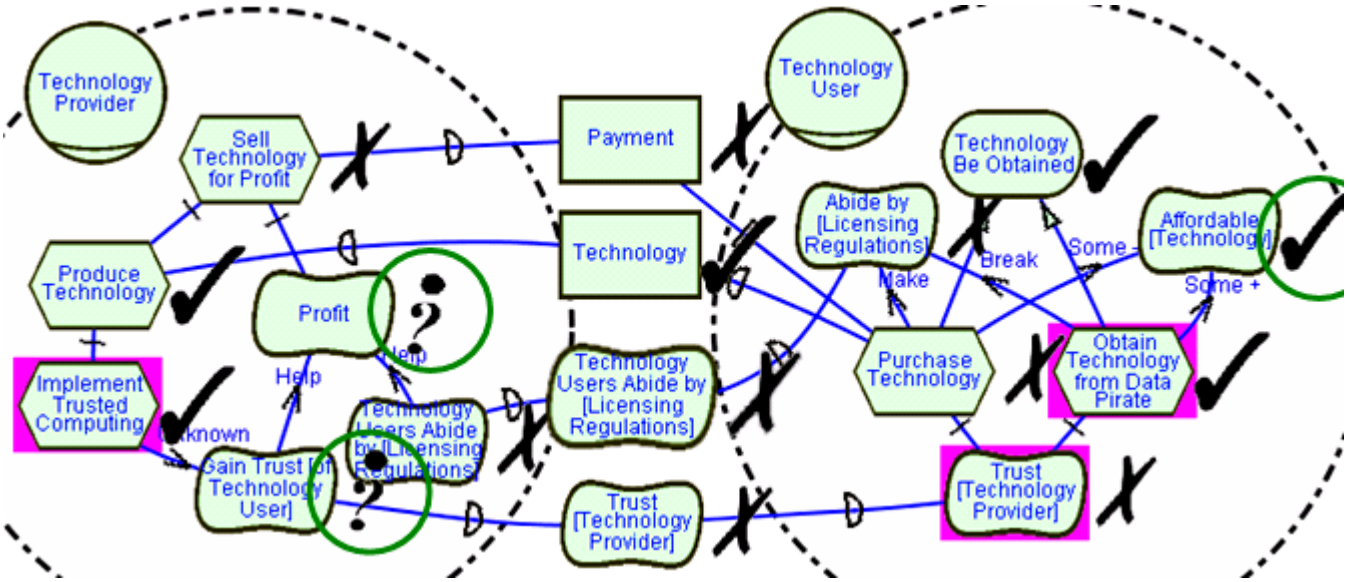

Figure 4. Simplified TC Model with Example Evaluation

Once a label bag has been resolved, the resulting label is placed in the queue of labels to be propagated. When all label bags are resolved, step 1 begins again, propagating the new labels in the queue. The algorithm alternates between step 1 and 2 until all label bags have been resolved and the queue of labels to propagate is empty. As i* models often contain cycles, it is possible that situations may arise where the labels do not converge. However, this will only occur in a cycle which involves human intervention to resolve a label, allowing the loop to be detected and terminated. More detail concerning the evaluation algorithm, including the checks to

ensure this level of convergence and termination, can be found in [13].

Once the evaluation algorithm has completed, the results can be analyzed in light of the question posed. In this case, if the Technology User does not Trust the Technology Provider, but Obtains Technology from the Data Pirate anyway, the Technology User obtains Affordable technology, and the Technology Provider does not Sell Technology for Profit, regardless of the Implementation of Trusted Computing. From this analysis we can derive several interesting results. First, according to this simple model, the Implementation of Trusted Computing will not help the cause of the Technology Provider unless it can sway the Technology User towards Purchasing Technology Legally. Secondly, such influence may not be accurately reflected in the model, as the Technology User's Trust is not dependent on the Technology Provider. Finally, in order to better understand the effects of Trusted Computing, the model must be elaborated in an attempt to replace the unknown effect with more specific contributions.

Overall, this evaluation helps us to learn more about the context of trusted computing and can lead us to iterate and expand on our simple model, as is illustrated in the next sections. The value of qualitative model evaluation is as much in this process of learning, exploration, and iteration as it is in the evaluation results.

6. ANALYZING TRUSTED COMPUTING

In order to understand the players and relationships involved in Trusted Computing and to form the foundation to answer the questions posed in Section 3, we will explore the domain incrementally. First we will focus on the background of the business of technology, creating models representing a single shared viewpoint, deferring consideration of elements which are potentially controversial. In this shared viewpoint we explore the actors in the business of technology; next, we see how the addition of malicious parties affects this domain. We then direct our attention to two competing viewpoints, representing the proponents and the opponents of trusted computing.

For this study, the primary sources of information on the proponent's side of Trusted Computing are technical reports and FAQ's of the TCG or TCG members such as [18, 30]. The information source for the opponent viewpoint has come from a FAQ written by Ross Anderson [1]. These sources were accessed for model creation from May of 2003 to June of 2004.

We recognize that these parties do not necessarily represent a united front. Within each camp there are varying opinions concerning the effects of the technology. Here, we attempt to represent the

most prevalent proponent and opponent viewpoints based on our sources.

The models presented in the Sections 6.1 to 6.4 are simplified versions of the models originally created for the study. We start our analysis with the simplified models in order to avoid overwhelming the reader with technical detail. In section 6.5 we shall briefly introduce some of the omitted technical details.

6.1 The Business of Content and Technology

We start by examining four roles: the Technology User, the Technology Provider, the License/Copyright Owner, and the Licensed/Copyrighted Content User shown in Figure 5. Such models can initially appear quite complex, but can be navigated effectively by examining the reasoning structure within one actor at a time. Then, focus can shift to the relationships between actors.

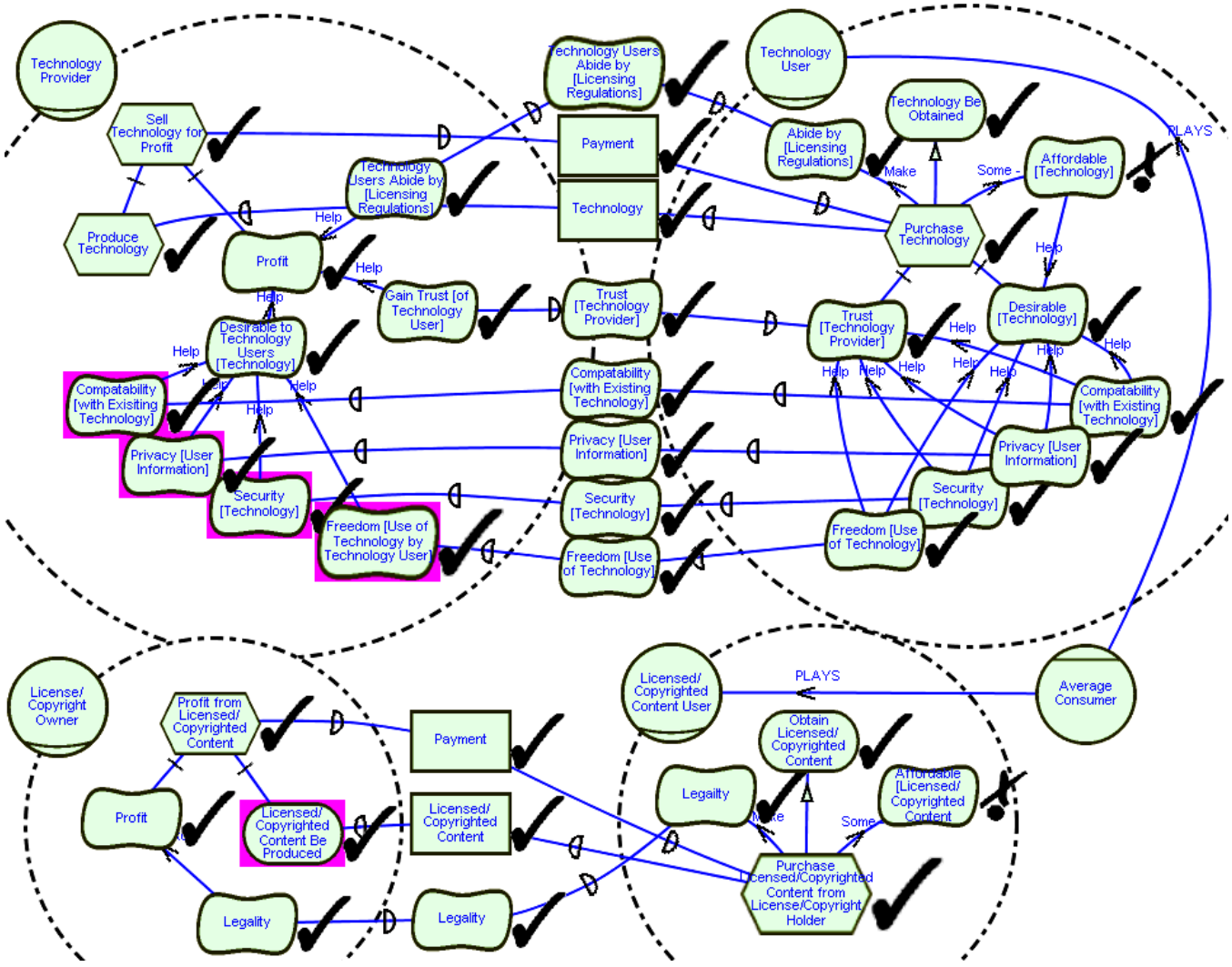

Figure 5. The Business of Content Technology, before considering Malicious Parties

What does the Technology User want? The Technology User role represents the user of personal technology devices such as PCs, cell phones, and PDAs, for various personal or professional tasks. The main goal of this role is for Technology to be Obtained. The Technology User would like these products to be Affordable, and would also like to Abide by Licensing Regulations. In order to Purchase Technology, it must be Desirable and the User must Trust the Technology Provider. Here, we do not distinguish between trust in the Technology Provider and trust in the technology itself. We assume that if the Technology User trusts the Technology Provider, they are likely to trust the technology.

We have included Compatibility, Security, Privacy, Affordability and Freedom of Use, (lack of restrictions) as the criteria for Desirable technology that are most relevant to the Trusted Computing issues. The Technology User depends on the Technology Provider for the satisfaction of these intentional elements, satisficed during the production of technology.

What makes technology trustworthy? We have included the notions of Privacy, Security, and Trust as desired elements of the Technology User. These concerns are treated here as softgoals as they are unlikely to be completely satisfied. The qualitative reasoning approach leads the analyst to determine ways in which the softgoal can be sufficiently met (i.e. satisficed).

The inclusion of Trust as a softgoal prompts us to ask: what makes the technology trustworthy? We see that many of the same elements that make a product Desirable, such as Compatibility, Security, Privacy and Freedom of Use, can also help Trust. If the model was further expanded, one could include other elements that help Trust but not Desirability, such as a security feature which may disable certain functionality, helping to distinguish between the meanings of the two concepts. For the sake of simplicity such elements are omitted from the current model.

What does the Technology Provider do? The Technology Provider is meant to represent the role played by companies such as members of the TCG, companies that create technology in various forms, and then sell it to Technology Users. The primary task of this role is to Sell Technology Products for Profit, requiring Products to be Produced and Profit to be made. In order to make Profit, Technology Users must Abide by Licensing Regulations by making legal purchases. Here we again include Privacy and Security as intentional softgoals, needed by the Technology Provider as a means to make Technology Desirable to Technology Users in order to make a Profit. Note that the inclusion of these elements within the Technology Provider does not prevent the modeller

from including additional intentional elements within this role which conflict with these desires. The power of i* lies in part in depicting and exploring such conflicting intentions.

In the Technology Provider we have added a softgoal representing this role's desire to Gain the Trust of the Technology User, as the Technology Provider believes the User's Trust will encourage the User to purchase products, helping increase the Profit of the Technology Provider. From this relatively simple model, we can see that the Technology Provider is employing the strategy of providing Compatibility, Privacy, Security, and Freedom of Use in its products in order to attract the business of the consumer and produce a Profit.

How does this relate to Licensed/Copyrighted Content? The roles of the Technology User and the Licensed/Copyrighted Content User are often played by the same individual, the Average Consumer. The Licensed/Copyrighted Content User wants to obtain such content for use. In order to do so it can Purchase Licensed/Copyrighted Content, ensuring that it follows various regulations and thereby ensuring Legality.

How is Licensed/Copyrighted Content provided? The License/Copyright Owner role is played by companies who own licensed or copyrighted material such as movies, music and software. Their main task is to Profit from Licensed/Copyrighted Content, requiring them to Produce and Sell such content. The License/Copyright Owner depends on Legality from the Licensed/Copyrighted Content User, in order to help make a Profit.

What can evaluation tell us? We initiate the i* evaluation procedure by marking the leaf elements as satisficed, meant to represent a positive situation, where all possible qualities of technology such as Security, Privacy, Compatibility and Freedom of Use are satisficed (in more detailed models these elements can be decomposed to depict precisely *how* they are satisficed). In Figure 2 we can see that if these technology qualities are satisfied, and Technology and Content are Produced, the major desires of all four roles are satisficed, with the exception of the Affordable goals for the Technology and Content Users. Concerning the questions raised in Section 3, by explicitly capturing the goals of stakeholders we have answered question (i) and by evaluating the achievement of these goals, we have addressed question (ii).

The result of the evaluation raises an interesting question: with the conflicting desires of the Technology and Content Providers to maximize profit, and the Technology and Content Users to minimize expenses, is it ever possible to achieve a compromise where all goals are sufficiently satisfied? Or will each role continually search for ways to satisfy their goals at the expense of

the others? Market forces often work to produce a balance between cost and profit, but either role may look for ways to circumvent these effects. This sort of insatiable desire creates opportunities for malicious parties, who satisfy the goals of some actors while creating adverse effects for others.

6.2 Introducing Malicious Parties

To explore the effects of malicious parties on the situation described in Section 4.1, we introduce the roles of the Data Pirate and the Hacker/Malicious User in Figure 6.

What does the Data Pirate **have to offer?** The Data Pirate wants to facilitate the Free Exchange and Use of Licensed/Copyrighted Content. In order to facilitate this, the Data Pirate depends on the Technology Provider for Freedom of Use, allowing actions such as copying, ripping, uploading, downloading and using licensed/copyrighted content through various technologies such as Peer-to-Peer technology and CD/DVD ripping software. With the inclusion of this role, the Technology User can now Obtain Technology from the Data Pirate, and the Content User can now obtain Licensed/Copyrighted Content from the Data Pirate.

What is the effect of Hacker/Malicious Users**?** The Hacker/Malicious User role causes harm or annoyance to others. We have identified the primary goals for this role as Profit and Notoriety. We have included a few of the actions that a Hacker/Malicious User might take to accomplish these softgoals, such as the Spreading of Viruses or the Accessing of Stored Data. Such data may contain personal information allowing for some form of theft. Further detail for this actor is explored in Section 4.5. We use contribution links across actor boundaries to represent the detrimental affects of these actions on the Privacy and Security provided by technology.

The effects of Malicious Parties, represented by contribution links in Figure 6, are summarized in Table 2. Such tables can be seen as alternate user interfaces to the graph-based models. The use of tool support, potentially facilitating such views of the model, is further discussed in Section 7.

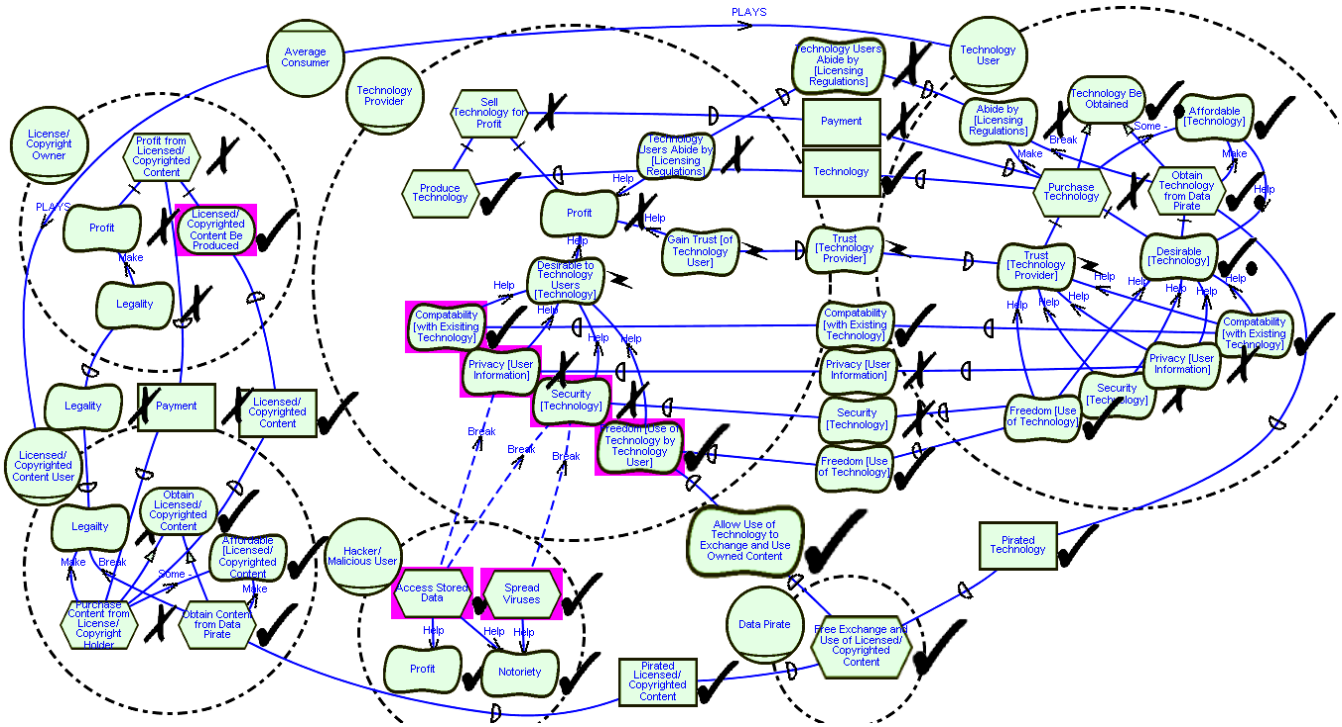

Figure 6. The Business of Technology with Malicious Parties

Table 2: Summary of the Effects of Malicious Parties Shown in Figure 6. Each row can be read as a paraphrased statement, such as "Access(ing) Stored Data IN Hacker/Malicious User BREAKS (the softgoal) Privacy [User Information] IN Technology Provider."

Contributing Element	Contributing Actor	Contribution	Recipient Element	Recipient Actor
Access Stored Data	Hacker/Malicious User	Break	Privacy [User Information]	Technology Provider
Access Stored Data	Hacker/Malicious User	Break	Security [Technology]	Technology Provider
Spread Viruses	Hacker/Malicious User	Break	Security [Technology]	Technology Provider

How do malicious parties affect the evaluation? We apply the evaluation procedure to Figure 6, assuming a worst-case scenario where the Hacker is able to perform all possible actions, and the Content User is able to Exchange and Use Licensed/Copyrighted Content. In this case Privacy and Security are broken by the actions of the Hacker. The evaluator makes a judgment, supplementing the model with additional knowledge about the domain, that this will result in a conflicting value for Trust in the Technology Provider, as technology is Compatible and provides Freedom of Use, but is not Secure and does not provide Privacy. These same criteria, along with

the Affordability of Technology, are used to determine the Desirability of Technology. Desirability is judged to be partially satisficed due to the positive contribution of Affordability, despite the denial of Privacy and Security. The evaluator judges that the Content User and the Technology User will choose to obtain content illegally due to the Affordability of illegally acquired content and technology. In the case of the Technology User, the reduced Trust and Desirability of the technology contributes to this decision. Although these actors also have a desire to Abide by Licensing Regulations and follow Legality, a pessimistic view is taken, using tacit domain knowledge to determine that these desires are less important to these roles than the desire to save money, especially as the model does not represent the consequences of breaking copyright laws (as for many, the consequences are negligible). The use of this tacit knowledge brings to light a potential area of model expansion or iteration. However, for the sake of simplicity, we choose not to expand the model in this case.

Obviously, this situation is detrimental for the Technology Provider and the License/Copyright Owner. Their desire for Profit is judged to be denied as a result of the illegal content acquisition, as well as the reduced Desirability and Trust of the consumer. Although this model helps to further address questions (i) and (ii) by including further relevant stakeholders, it does not yet depict the business strategies employed by these actors to deal with the threats of the Malicious Actors. The nature of these strategies and their effects are controversial. We shall attempt to capture a high-level view of these controversies in the models that follow.

6.3 The Effects of Trusted Computing According to Proponents

So far we have analyzed the Trusted Computing background from a single viewpoint. Now we elaborate the models to consider the effects of TC on this situation according to the technology's proponents (Figure 7). From this viewpoint, using the models and model analysis, we intend to answer the questions posed in Section 3.

How does Trusted Computing help? TC proponents describe various aspects of TC technology which affect the ability of the Hacker/Malicious User to perform certain actions. Here we provide examples of some of these aspects and their effects on Security and Privacy. For instance, according to proponents, the isolation of applications and checking of the platform configuration hurts the Hacker/Malicious User's ability to gain control of technology and Access Stored Data. Furthermore, proponents have claimed that protection profiles and endorsement keys reduce the ability of malicious users to Spread Viruses. The counter-measures

offered by the capabilities of TC are shown in the model by hurt links to actions of the Hacker/Malicious User's. Further aspects and effects of TC technology can be found in section 4.5.

Various sources have addressed the inclusion of Digital Rights Management (DRM) features in TC technology. DRM has the potential to affect Freedom of Use, possibly reducing the user's freedom to possess/play certain files or programs.

In the proponent sources examined for this study, the DRM features provided by TC are emphasized as optional, requiring user permission. However, the consequences of denying this permission are often not explained. When modelling the technology and its effects, omissions such as this become clearer. What happens if TC's DRM capabilities are refused by the user? How does this affect the functionality of TC components and the trusted status of TC users? If users are compelled to activate DRM components, how does this affect the interactions between the Technology Provider and User, or between the License/Copyright Owner and Technology Provider? Further developing and evaluating the models in this study could help to conceptualize and propose answers to questions such as these. In this simple model, the uncertainty concerning the effects of TC technology on Freedom of Use is depicted by an unknown contribution link.

The simplified view of the effects of Trusted Computing according to proponents represented in Figure 7 is summarized in Table 3.

Will TC Work? Through our steps of modeling and analysis we are now in a position to continue to answer the questions posed in Section 3.

(ii) By performing an evaluation assuming that all aspects of TC are implemented and distributed with the technology, we can see that the actions of the Hacker/Malicious User are now harmed, resulting in partially denied values. Therefore their effects on Security and Privacy are lessened, and these softgoals are now partially satisfied. As a result, the Desirability of technology is judged to be partially satisficed, and the amount of content acquired legally is perceived to rise. This is depicted by the partially satisficed value for Purchase Technology, having a value of denied in the previous model.

Consequently, the Technology Provider has partially satisfied value for Profit, but the situation for the License/Copyright Owner, (not shown due to space constraints), has changed little, coinciding with the claims of proponents that the overall intention of TC technology is not to fight piracy.

(iii) By examining the model we can perceive that the overall strategy behind Trusted

Computing technology is to improve the security of technology, improving its desirability to users, and consequently improving sales. (iv) The fundamental means of implementing this strategy is through the introduction of TC. More detail concerning precisely how TC implements the business strategies is contained in Section 6.5. (v) The strategy requires the achievement of the Trust of the consumer, in order to fully achieve Profit. (v, vi) However, in this situation the Trust of Technology Users is only partially achieved due to contributing factors such as Compatibility, Security, Privacy and Freedom of Use.

In addition, one can question the logic of the strategies employed by the Technology Provider. Will the heightened desirability of technology provided by TC mean that more people will purchase it legally and not illegally? And if not, why are Technology Providers Implementing TC?

6.4 The Effects of Trusted Computing According to Opponents

What do opponents say about Trusted Computing? Opponents of Trusted Computing have a different view of the elements contained within its design [1]. We have taken the shared viewpoint model in Figure 6 and added the effects of Trusted Computing according to this viewpoint, producing Figure 8.

Currently, when modeling two different viewpoints concerning the same subject matter, in this case the effect of TC technology, the i* Framework does not specify conventions for identifying conflicts across viewpoints. These types of conflicts are in contrast to conflicts in the evaluation sense, the presence of both positive and negative evidence. In this study viewpoint conflicts are represented implicitly in the differences between models, in this case the differences between Figure 7 and 8.

In the opponents view, one of the main intentions of TC is to Protect Licensed/Copyrighted Content. This is a required component of Sell Licensed/Copyrighted Content Online, which is depended on by the License/Copyright Owner in order to Sell Profit Safely Online and increase Profit. As a result of the need to Protect Licensed/Copyrighted Content, the support of DRM within Implement TC is not optional, causing Implement TC to break Freedom of Use.

Opponents claim that TC will make it more difficult for consumers to switch to alternative products, hurting Compatibility and effectively locking customers into their products. This is represented by the softgoal Lock-in Customers within the Technology Provider, and the dangling dependency of Avoid Lock-in within the Technology User.

Lock-in Customers forces the consumer to continue to Purchase the Technology, represented by links breaking the effects of Desirability and Trust on

Purchase Technology within the Technology User and Profit within the Technology Provider. In other words, when locked-in, it does not matter if the consumer no longer desires the product, or trusts the vendor; they are forced to purchase the product regardless.

In addition, opponents describe other uses and intentions of TC such as potential remote censorship, remote access to personal documents, greater controls on document access, and providing back-door access to authorities. These elements have negative effects on both Privacy and Security.

Opponents claim that TC technology is not effective in protecting against various actions of the Hacker/Malicious User, such as Spreading Viruses. This is shown by the removal of the counter-measure links, when compared to the links present in Figure 7. As opponents of TC do not seem to discount its ability to help prevent Access to Stored Data, this link is retained.

The simplified view of the effects of Trusted Computing and related elements according to opponents is summarized in Table 4. The similarities between Table 3 and Table 4 are highlighted in italics.

What are the overall effects of Trusted Computing? Our modeling and analysis allows us to answer the questions posed in Section 3 from the point of view of TC opponents.

(ii) From the evaluation of the TC opponent model we can see that the Hacker/Malicious User is still able to execute some malicious actions. However, due to the harmful effect of TC components on Freedom of Use we can see that the Data Pirate is no longer able to satisfy its main task of Free Exchange and Use of Licensed/Copyrighted Content.

Examining the Technology Provider, we can see that Security and Privacy for the Technology User is denied. This, in conjunction with the denial of Compatibility and Freedom of Use, results in the denial of Desirability and Trust in the Technology Provider. However, the dependency on Avoiding Lock-In is unfulfilled, and this has a negative effect on the links which make Desirability and Trust necessary in order to Purchase Technology. These effects, along with the unavailability of pirated content, force the consumer to Purchase Technology legally from TC providing vendors. Likewise, the Licensed/Copyrighted Content User is forced to Purchase Content from the License/Copyright Owner. As a result, Profit for both the Technology Provider and the Licensed/Copyright Owner is satisficed.

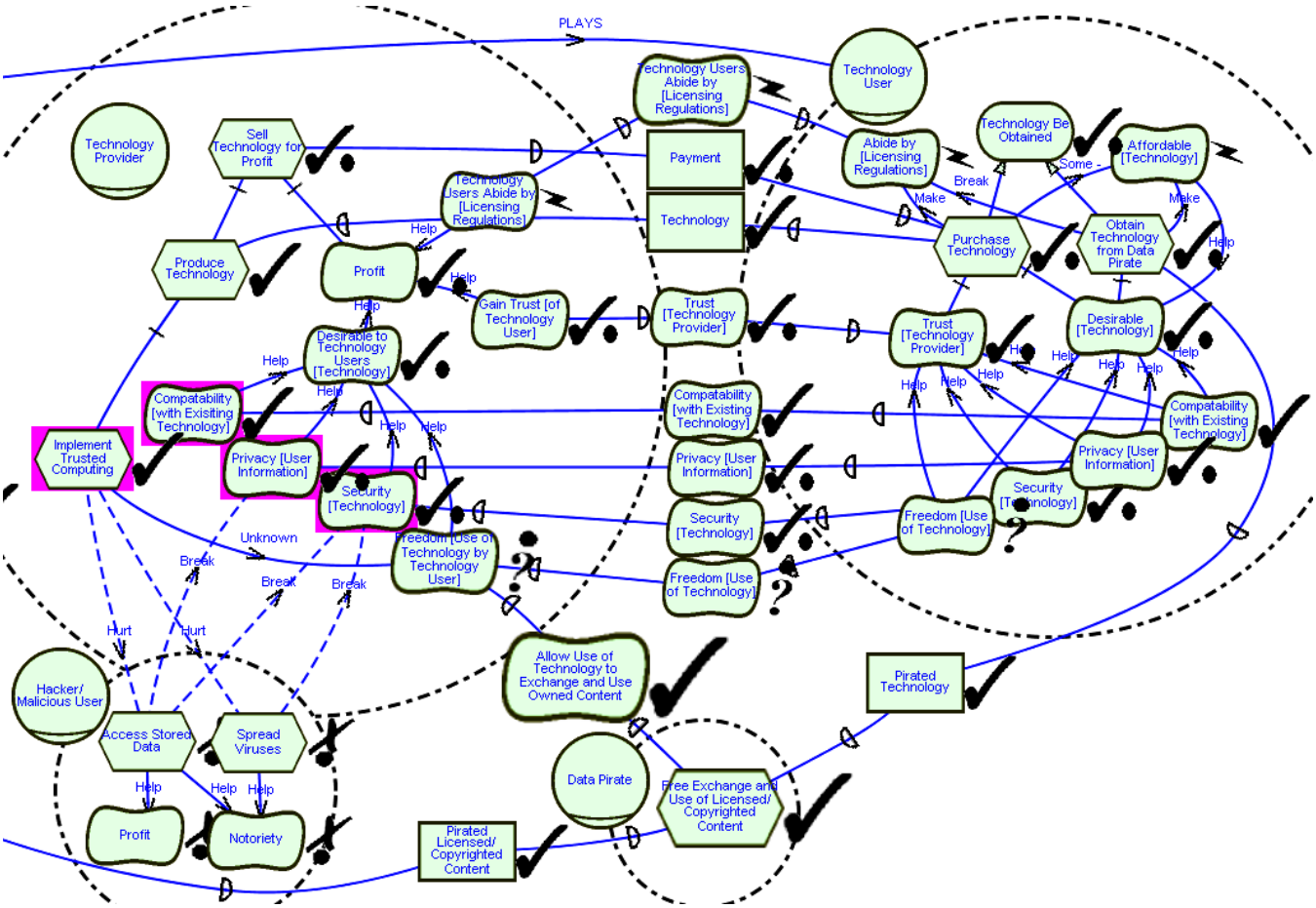

Figure 7. The Effects of Trusted Computing According to Proponents

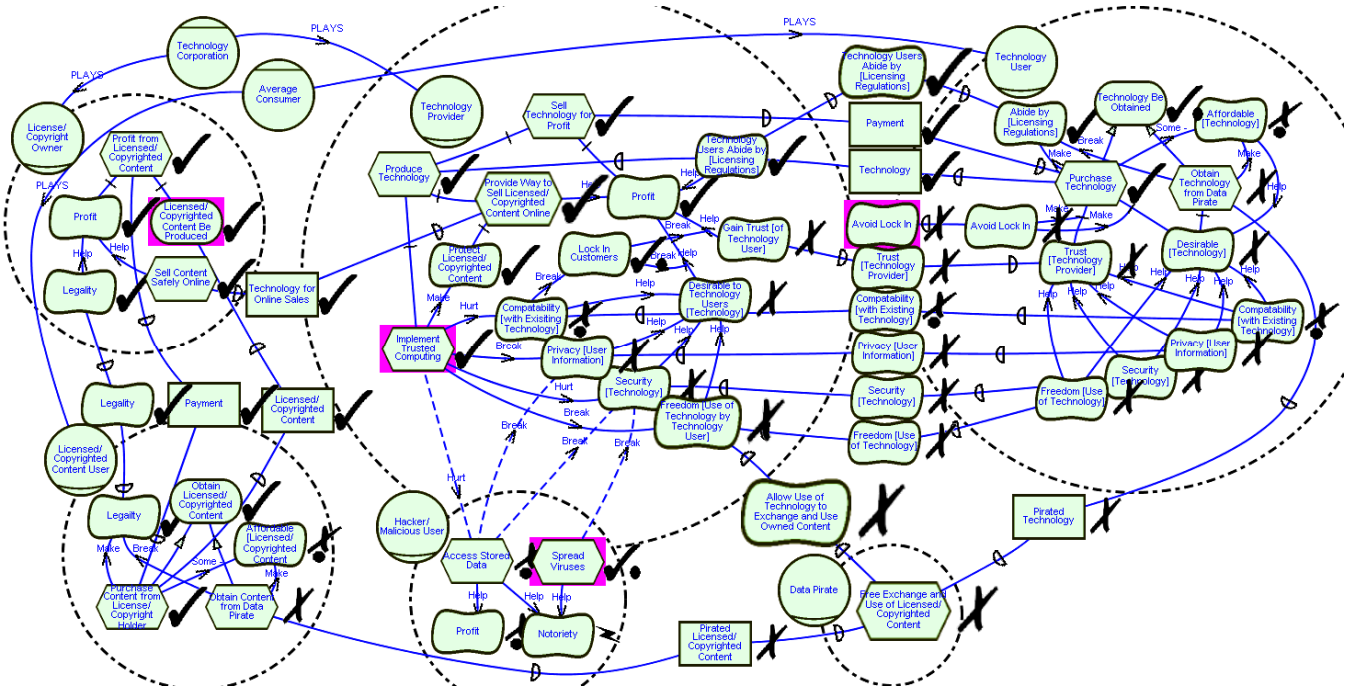

Figure 8. The Effects of Trusted Computing According to Opponents

Table 3: Summary of the Effects of Trusted Computing Shown in Figure 7 (Proponents).

Contributing Element	Contributing Actor	Contribution	Recipient Element	Recipient Actor
Implement Trusted Computing	*Technology Provider*	*Hurt*	*Access Stored Data*	*Hacker/Malicious User*
Implement Trusted Computing	Technology Provider	Hurt	Spread Viruses	Hacker/Malicious User
Implement Trusted Computing	Technology Provider	Unknown	Freedom [Use of Technology by Technology User]	Technology Provider

Table 4: Summary of the Effects of Trusted Computing and Related Elements Shown in Figure 8 (Opponents)

Contributing Element	Contributing Actor	Contribution	Recipient Element	Recipient Actor
Implement Trusted Computing	*Technology Provider*	*Hurt*	*Access Stored Data*	*Hacker/Malicious User*
Implement Trusted Computing	Technology Provider	Make	Protect [Licensed/ Copyrighted Content]	Technology Provider
Implement Trusted Computing	Technology Provider	Hurt	Compatibility [with Existing Technology]	Technology Provider
Implement Trusted Computing	Technology Provider	Break	Privacy [User Information]	Technology Provider
Implement Trusted Computing	Technology Provider	Hurt	Security [Technology]	Technology Provider
Implement Trusted Computing	*Technology Provider*	Break	*Freedom [Use of Technology by Technology User]*	*Technology Provider*
Compatibility [with Existing Technology]	Technology Provider	Break	Lock in Customers	Technology Provider
Lock in Customers	Technology Provider	Break	Help Contribution from Desirable to Technology Users [Technology] to Profit	Technology Provider
Lock in Customers	Technology Provider	Break	Help Contribution from Gain Trust of Technology Users to Profit	Technology Provider
Avoid Lock-In	Technology User	Make	Decomposition Link from Purchase Technology to Trust [Technology Provider]	Technology User
Avoid Lock-In	Technology User	Make	Decomposition Link from Purchase Technology to Desirable [Technology]	Technology User

(iii) Overall, from the point of view of TC opponents, the business strategy motivating the production of TC involves increasing profit by gaining control of technology and thwarting the actions of the Data Pirate. (iv) Not only is security and privacy not effectively protected from the actions of the Hacker/Malicious User, but elements within TC itself, such as remote access, will harm these concerns, providing the technical control necessary for the Technology Producers to

fight Piracy. (v) In this strategy, the role of Trust is mitigated by consumer Lock-In, (vi) allowing the Technology Producer to deny trust by denying Compatibility, Security, Privacy and Freedom of Use.

TC opponents rationalize this strategy by pointing out that the same agents who play the role of the Technology Provider, producing TC, also play the role of the License/Copyright Owner, as producers of licensed software. This relationship, shown in Figure 5 via PLAYS links between agents and roles, is not emphasized in the proponent sources. Generally, from the point of view of opponents, TC is a malicious component similar to the Data Pirate, satisfying insatiable goals of some actors, (Profit for Providers/Owners), while bringing adverse effects to others (Users).

6.5 Trusted Computing Elaborated

By elaborating on the models presented in this study, a more detailed picture of the elements involved in the business strategies fueling technology can be derived. Figure 9 and 10 show high-level views of detailed proponent and opponent models, respectively. Figure 9 additionally demonstrates the interface of the OME application [22]. These models provide an overview of the level of complexity involved in the expanded models. They include more detail on the actions of the malicious parties, and contain the decomposition of the Implementation of TC from both viewpoints, showing the effects of individual TC components on elaborated components of privacy and security.

In Figures 11 and 12, we enlarge comparable portions of Figures 9 and 10 to highlight the interaction between the Technology Provider and the Hacker/Malicious User, from the point of view of TC proponents and opponents, respectively. The extra detail included in these views can be summarized in tabular form. Figure 13 lists the detailed elements contributing positively to Security and Figure 14 lists the decomposition elements of Freedom [Use of Technology by Technology User]. In Table 6 we list the effects of the expanded actions Hacker/Malicious User on elements pertaining to Security and Privacy. These details are shared between viewpoints.

In Table 7 we summarize the detailed effects of Trusted Computing according to proponents. The equivalent table for proponents is provided in Table 8. The similarities between these two viewpoints are highlighted in italics.

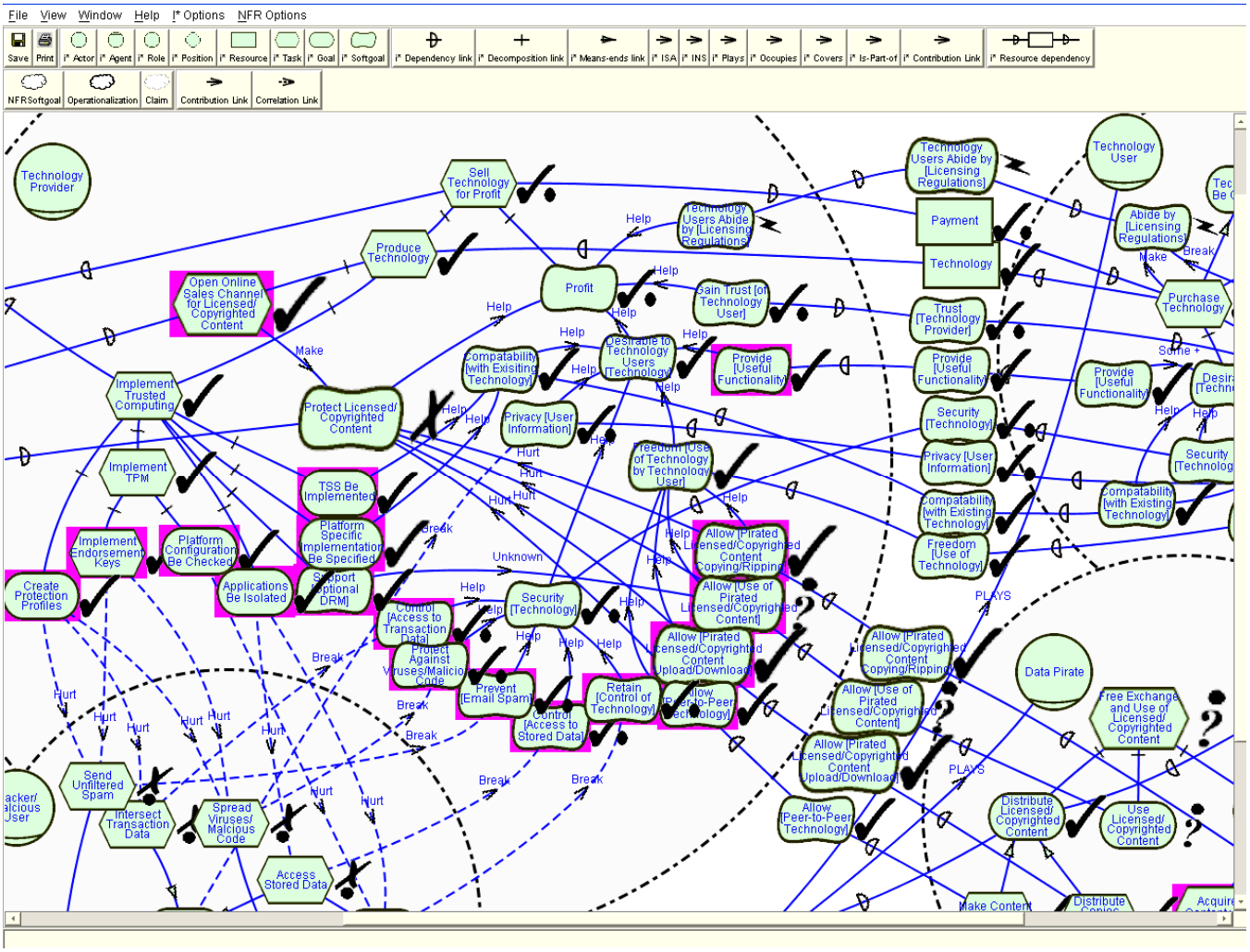

Figure 9. Screenshot of the OME Tool displaying the Trusted Computing Domain in Detail According to Proponents

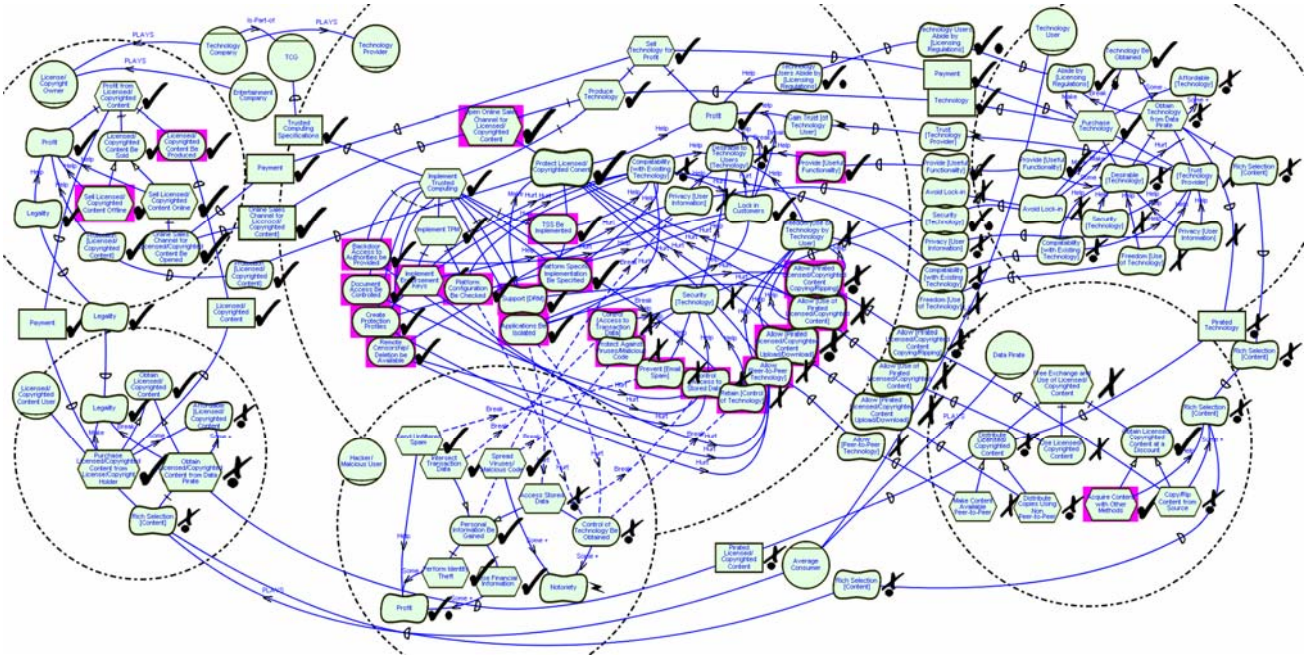

Figure 10. The Trusted Computing Domain in Detail According to Opponents

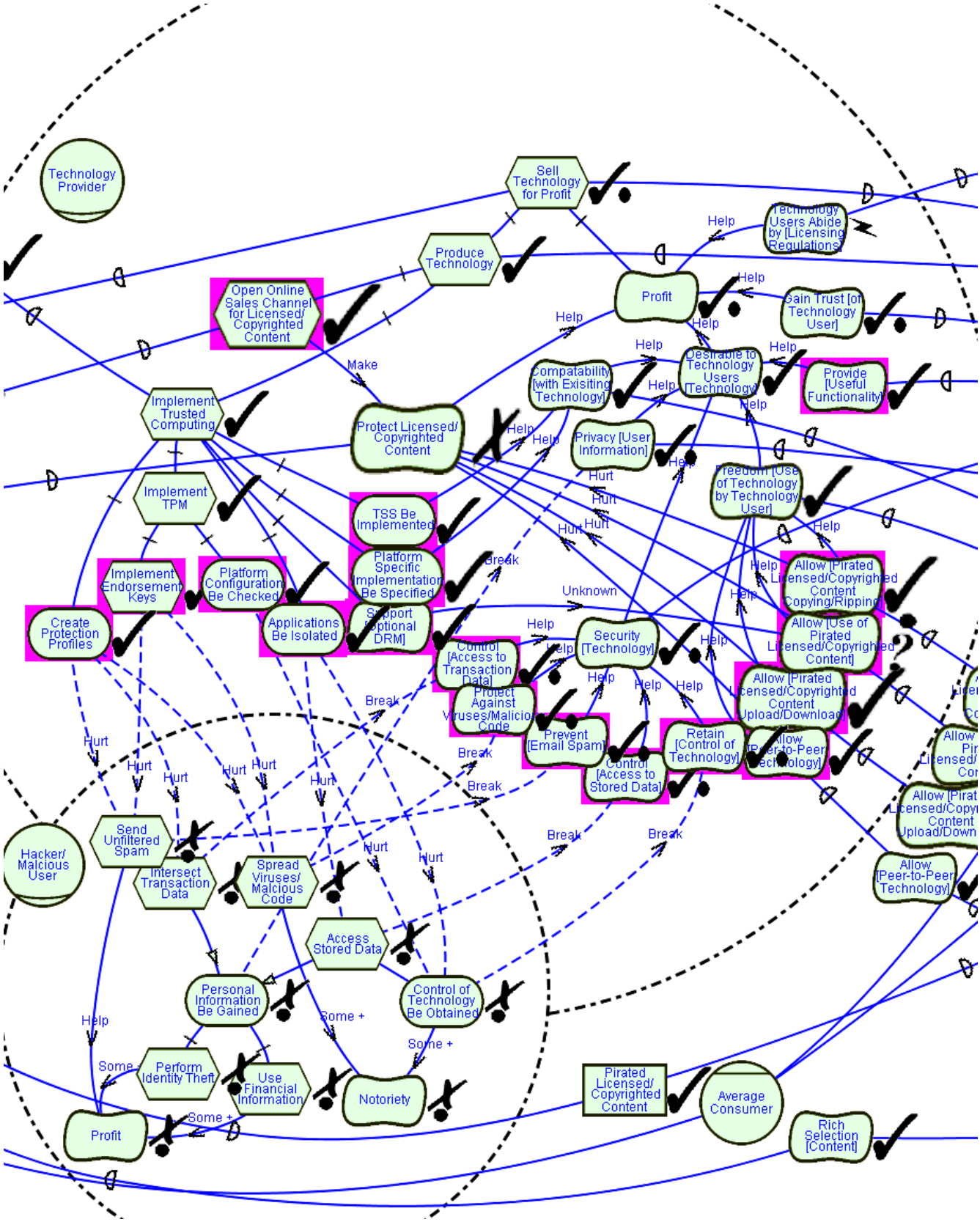

Figure 11. Technology Producer and Hacker/Malicious User in Detail According to Proponents

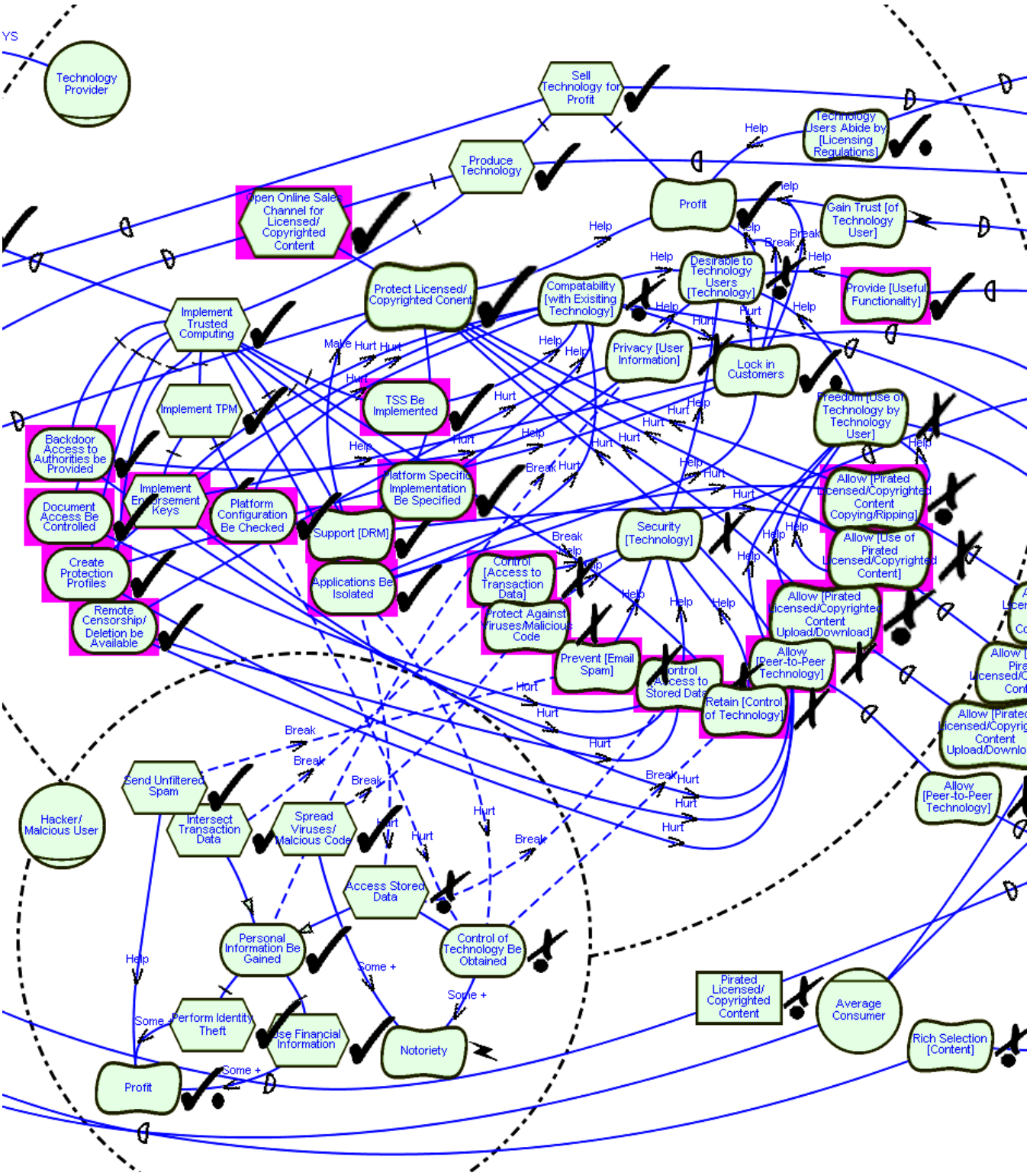

Figure 12. Technology Producer and Hacker/Malicious User in Detail According to Opponents

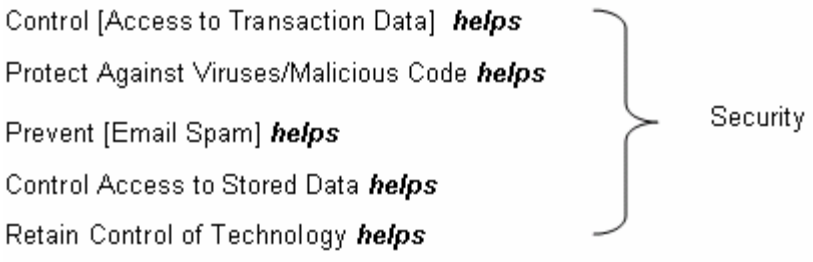

Figure 13: Security Decompositions

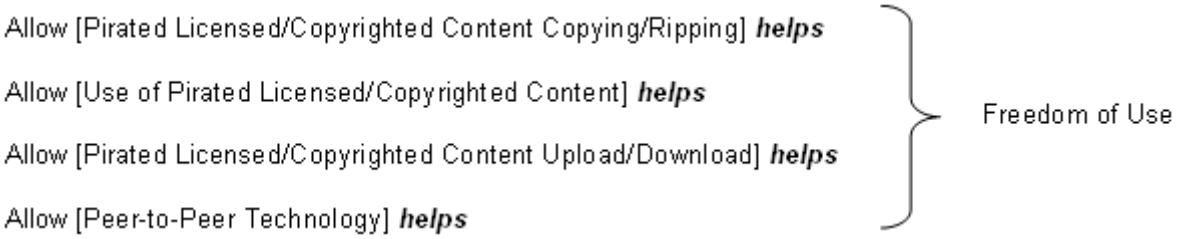

Figure 14: Freedom of Use Decompositions

Table 6: Effects of the expanded actions of the Hacker/Malicious User

Contributing Element	Contributing Actor	Contribution	Recipient Element	Recipient Actor
Send Unfiltered Spam	Hacker/Malicious User	Break	Prevent [Email Spam]	Technology Producer
Intersect Transaction Data	Hacker/Malicious User	Break	Control [Access to Transaction Data]	Technology Producer
Spread Viruses/Malicious Code	Hacker/Malicious User	Break	Protect Against Viruses/Malicious Code	Technology Producer
Access Stored Data	Hacker/Malicious User	Break	Control Access to Stored Data	Technology Producer
Control of Technology Be Obtained	Hacker/Malicious User	Break	Retain [Control of Technology]	Technology Producer
Personal Information be Gained	Hacker/Malicious User	Break	Privacy [User Information]	Technology Producer

Table 7: The Effects of Trusted Computing According to Proponents

Contributing Element	Contributing Actor	Contribution	Recipient Element	Recipient Actor
Create Protection Profiles	Technology Producer	Hurt	Send Unfiltered Spam	Hacker/Malicious User
Create Protection Profiles	Technology Producer	Hurt	Intersect Transaction Data	Hacker/Malicious User
Create Protection Profiles	Technology Producer	Hurt	Spread Viruses/Malicious Code	Hacker/Malicious User
Implement Endorsement Keys	Technology Producer	Hurt	Send Unfiltered Spam	Hacker/Malicious User
Implement Endorsement	Technology	Hurt	Spread Viruses/Malicious	Hacker/Malicious

Keys	Producer		Code	User
Platform Configuration Be Checked	*Technology Producer*	*Hurt*	*Control of Technology Be Obtained*	*Hacker/Malicious User*
Applications Be Isolated	*Technology Producer*	*Hurt*	*Access Stored Data*	*Hacker/Malicious User*
Applications Be Isolated	*Technology Producer*	*Hurt*	*Control of Technology Be Obtained*	*Hacker/Malicious User*
Support DRM	*Technology Producer*	Unknown	*Allow [Use of Pirated Licensed/Copyrighted Content]*	*Technology Producer*
Platform Specific Implementation Be Specified	*Technology Producer*	*Help*	*Compatibility [with Existing Technology]*	*Technology Producer*
TSS Be Implemented	*Technology Producer*	*Help*	*Compatibility [with Existing Technology]*	*Technology Producer*

Table 8: The Effects of Trusted Computing According to Opponents

Contributing Element	**Contributing Actor**	**Contribution**	**Recipient Element**	**Recipient Actor**
Backdoor Access to Authorities be Provided	Technology Producer	Hurt	Privacy [User Information]	Technology Producer
Backdoor Access to Authorities be Provided	Technology Producer	Hurt	Control [Access to Stored Data]	Technology Producer
Document Access be Controlled	Technology Producer	Hurt	Control [Access to Stored Data]	Technology Producer
Create Protection Profiles	Technology Producer	Hurt	Compatibility [with Existing Technology]	Technology Producer
Create Protection Profiles	Technology Producer	Hurt	Allow [Peer-to-peer Technology]	Technology Producer
Remote Censorship/Deletion be Available	Technology Producer	Hurt	Privacy [User Information]	Technology Producer
Remote Censorship/Deletion be Available	Technology Producer	Hurt	Allow [Peer-to-peer Technology]	Technology Producer
Remote Censorship/Deletion be Available	Technology Producer	Hurt	Control [Access to Stored Data]	Technology Producer
Implement Endorsement Keys	Technology Producer	Hurt	Compatibility [with Existing Technology]	Technology Producer
Implement Endorsement Keys	Technology Producer	Help	Lock-in Customers	Technology Producer
Implement Endorsement Keys	Technology Producer	Help	Allow [Peer-to-peer Technology]	Technology Producer
Platform Configuration Be Checked	Technology Producer	Hurt	Compatibility [with Existing Technology]	Technology Producer
Platform Configuration Be Checked	*Technology Producer*	*Hurt*	*Control of Technology Be Obtained*	*Hacker/Malicious User*
Applications Be Isolated	*Technology Producer*	*Hurt*	*Access Stored Data*	*Hacker/Malicious User*
Applications Be Isolated	*Technology Producer*	*Hurt*	*Control of Technology Be Obtained*	*Hacker/Malicious User*
Applications Be Isolated	Technology	Hurt	Compatibility [with Existing	Technology Producer

	Producer		Technology]	
Applications Be Isolated	Technology Producer	Help	Lock-in Customers	Technology Producer
Applications Be Isolated	Technology Producer	Hurt	Allow [Pirated Licensed/Copyrighted Content Copying/Ripping]	Technology Producer
Applications Be Isolated	Technology Producer	Help	Protect Licensed/Copyrighted Content	Technology Producer
Support DRM	*Technology Producer*	Hurt	*Allow [Use of Pirated Licensed/Copyrighted Content]*	*Technology Producer*
Support DRM	Technology Producer	Make	Protect Licensed/Copyrighted Content	Technology Producer
Platform Specific Implementation Be Specified	*Technology Producer*	*Help*	*Compatibility [with Existing Technology]*	*Technology Producer*
TSS Be Implemented	*Technology Producer*	*Help*	*Compatibility [with Existing Technology]*	*Technology Producer*
Implement Trusted Computing	Technology Producer	Break	Retain [Control of Technology]	Technology Producer

The addition of the detail described in these tables better supports the claims made by our models concerning the effects of Trusted Computing, giving a more detailed answer to question (ii). As the simplified models were extracted from these more complex models, the overall results demonstrated by evaluation, including the answers to the Section 3 questions, are consistent between the different model versions. If, instead, our modeling process had taken us from the simpler models to the more complex, the discoveries prompted by the addition of the extra detail would likely have led us to modify our models and make changes to our analysis.

7. DISCUSSION

Our use of i* has enabled us to answer the analysis questions posed in Section 3 from the point of view of TC proponents and opponents. By doing so, differences between viewpoints have been brought to light. (i) We have explicitly captured a subset of the goals of relevant stakeholders enabling useful analysis. (ii) The application of the evaluation procedure has allowed us to determine whether or not these goals could be achieved in certain situations, examining the differences between goal achievement from each point of view. Although the evaluation procedure has been used effectively to help answers these questions, the procedure could be used more extensively to answer additional analysis questions. For example, from the proponent's point of view, if DRM features were no longer optional, would users still purchase TC laden technology?

(iii) From the point of view of TC proponents, we have shown the Technology Provider's strategy of gaining the trust of users by providing security and privacy. From the opponent point of view, we have shown a different strategy: increasing profit by hindering the actions of the Data Pirate while locking the user into their technology.

(iv) By presenting specific details of TC implementation in Section 6.5, we were able to show how the implementation of TC achieved the strategies of the Technology Producer. (v) We were able to examine the role of trust from both viewpoints, seen as either an essential ingredient for success, or mitigated through product lock-in. (vi) Finally, by applying the evaluation procedure we were able to determine the achievement or denial of trust in certain situations, determining how trust was achieved or denied by examining contributing factors in the model.

Using i* to model the TC domain revealed insights which were not immediately obvious. For example, the success of piracy depends on a decision of the Technology Provider to allow for freedom of technology use, which the provider may allow in order to please consumers. Intentions and relationships became apparent when we had to rationalize stakeholder actions in order to express them in our models. For instance, why do Technology Producers implement TC if it makes technology less desirable to users? By exploring the intent to stop piracy, and the relationships between lock-in, trust, and desirability, we have rationalized this strategy from the point of view of TC opponents. Gaps or flaws in arguments became apparent when they were modelled in the context of all affected stakeholders. For example, what are the consequences of refusing DRM functionality for the Technology User? In addition, our models helped us to explore the meaning of multi-faceted terms, such as trust.

This study makes use of ongoing work to address and improve the visualization of i* models, making use of interactive tools which allow one to view, manipulate, and evaluate models. For instance, the OME (Organization Modeling Environment) Tool was created to allow the construction and analysis of goal modeling frameworks such as i* and the NFR Framework [22]. OME allows users to insert i* notation including elements and links and to perform a version of the qualitative evaluation procedure described in this work. Models created in OME are represented in the Telos conceptual modeling language [20]. Recently, OME has been expanded and modified to create OpenOME [23], an open-sourced version integrated with the Eclipse Development Platform [6]. The application includes an interface to the Protégé Ontology tool [24], developed as an Eclipse plug-

in. Active development of OpenOME includes implementation of qualitative and quantitative evaluation procedures and integration with the Eclipse GMF [11].

Furthermore, as part of the previous work involving i*, multiple software tools have been built in order to support additional i* aspects or extensions. A summary and comparison of these tools can be found on the i* Collaborative Wiki [12].

Our work is a first attempt to use early requirements modelling techniques to analyze the link between stakeholder interests and technology strategies, opening up a vast area for further research. Although we have focused on the Trusted Computing example, we believe that our approach could be used successfully to answer analysis questions such as those posed in Section 3 for multiple domains involving trust and technology strategies. Such modelling techniques can be used to take vendor strategies into account when guiding system design or procurement decisions. Considering of the effects of trust on technology strategies can be made explicit, facilitating a more effective achievement of the goals of both the consumers and producers of technology.

8. RELATED WORK

In this work, we test the ability of i* to assist in the analysis of trust in technology strategies. The intention of this approach is to explicitly reason about trust at an early stage in strategy analysis, when quantitative information is often difficult to obtain. Therefore, our analysis uses a qualitative method to represent the satisfaction of trust, as well as the satisfaction of intentional desires. However, our approach does not exclude the possibility of extension for quantitative analysis if detailed numerical information is available from the domain. For instance, in the work of Gans et al. [9], the Trust-Confidence-Distrust (TCD) method uses quantitative utility functions to evaluate trust and distrust in social networks expressed in the i* Framework. A quantitative approach such as this would be complementary to our qualitative approach.

The softgoal construct in the i* Framework has been used previously to explore trust, [35, 36], in the context of system design. In this study, our models contain additional subtleties in the notion of trust, as we examine trust from conflicting viewpoints, and explore dependencies on trust by the trusted parties.

Similar to our treatment of trust as a non-functional softgoal, we are able to reason about additional non-functional system desires such as security and privacy by the same means. Here, we consider these aspects in relation to our focus on trust, but previous work with the i*

Framework has focused specifically on these concerns [36, 15].

Our work using i* to represent multiple viewpoints contains similarities to the work in [14], where the TCD method is used with multiple i* viewpoints in the healthcare network domain. Similarly, i* and its evaluation procedure have been used to explore the benefits of viewpoint modeling in [5].

The i* Framework has been previously applied in several other fields. In the context of Requirements Engineering i* has been used to focus specifically on the phase of Early Requirements Engineering [34]. In the RESCUE method, system requirements are developed using parallel streams of modeling, including i* [16]. In the work of Sutcliffe and Minocha, i* has been used in combination with cost and workflow analysis to analyze system requirements [28]. Santander and Castro have proposed a method for deriving use cases, a common modeling notation used in requirements elicitation, from i* models [25]. Martinez et al. have developed a methodology to transform constructs of an i* model into formalized requirement specification statements [17].

In the context of system development, the i* framework has been incorporated into the Tropos software design processes, described in [21]. This methodology has been extended to consider trust and security requirements [10]. Furthermore, i* has be used in the analysis and design of software processes, as described in [32] and as demonstrated in [3].

The i* Framework has also been applied in the context of Business Process design and redesign [33]. Additionally, previous work has applied i* in the field of knowledge management, [19, 27].

Generally, the approach taken in this paper to analyze trust at the technology strategy level can be viewed as part of an overall methodology for system and software development that connects strategy analysis with technical system development.

9. LIMITATIONS AND FUTURE WORK

Despite the success of our analysis, we can see a number of limitations to our approach. As mentioned, due to the complex nature of real-world domains, it is clear that models depicting social situations can never be entirely complete or fully accurate. Thus there is a continual trade-off between the inclusion of potential information, and model size and readability, as demonstrated by the complexity of Figures 9 through 12. Despite scalability issues, i* modeling has been successfully applied to complex, real-life applications [5].

The TC example used in this paper is based purely on document sources. As a consequence,

it is difficult to validate the correctness of the resulting models beyond the knowledge acquired by the modellers. In other studies, models have been constructed based on interviews with stakeholders [5].

The use of i* for depicting viewpoints raises the need for more specific methods and tools to deal with alternative viewpoints in i* models. It would be useful to indicate precisely which elements represent agreement or conflict, and to provide tools which highlight and emphasize such differences.

In this work, we have presented i* modeling as a modeling technique without prescribing a specific methodology, therefore, there is an opportunity to develop a systematic methodology which would better enable business and technology strategy analysis. In addition, we have shown the relationships among trust, security, and privacy in only a rudimentary way, treating security and privacy as contributing factors for trust. The relationships among privacy, security, and trust can be explored in greater depth in future work.

Regarding the coverage of the domain complexity in this study, we have only modelled and analyzed two opposing viewpoints at a particular stage in the development of a technology. We could further exploit the capabilities of the i* Framework to seek alternative technological solutions which sufficiently satisfy the goals of all stakeholders while thwarting malicious parties. The scope of our models could be expanded to explore additional related actors, such as the role of governmental parties, who may depend on TC to provide a Backdoor Access to Technology, or the role of technology producers who do not implement TC, examining the effects of competition in technology production. In addition, there are many intermediate viewpoints concerning the effects of TC beyond the two explored in this work. For example, Arbaugh [2] has looked at TC from both a positive and a negative view, and suggests ways in which TC could be adjusted to produce technology which is more acceptable to stakeholders. It would be interesting to apply these suggestions to our models and evaluate whether they offer an adequate alternative.

10. REFERENCES

[1] Anderson, R., “Trusted Computing' Frequently Asked Questions”, Retrieved July 2004 from www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[2] Arbaugh, W. A., “Improving the TCPA”, *IEEE Computer*, vol. 35, August, 2002, pp. 77 – 79.

[3] Briand, L., Kim, Y., Melo, W., Seaman, C., Basili, V., "Q_MOPP: Qualitative Evaluation

of Maintenance Organizations, Processes, and Products", *Journal of Software Maintenance: Research and Practice*, 1998.

[4] Chung, L., Nixon, B.A., Yu, E., Mylopoulos, J., *Non-Functional Requirements in Software Engineering*, Kluwer Academic Publishers, 2000.

[5] Easterbrook, S. M., Yu, E., Aranda, J., Fan, Y., Horkoff, J., Leica, M., Qadir, R. A, "Do Viewpoints Lead to Better Conceptual Models? An Exploratory Case Study", In *Proceedings of 13th IEEE International Requirements Engineering Conference (RE'05)*, Paris, France, 2005, pp. 199- 208.

[6] "Eclipse - an open development platform",Retrieved January 2007 from http://www.eclipse.org/

[7] Falcone, R., Castelfranchi, C., "Social trust: a cognitive approach", In C. Castelfranchi and Y.-H. Tan (ed.), *Trust and Deception in Virtual Societies*, Kluwer Academic Publishers, 2001, pp. 55-90.

[8] Gambetta, D. (ed.), *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, New York, 1988.

[9] Gans, G., Jarke, M., Kethers, S., Lakemeyer, G., "Continuous requirements management for organization networks: a (dis)trust-based approach", *Requirements Engineering Journal, Special Issue RE'01*, Springer 8, 2003, pp. 4-22.

[10] Giorgini, P., Massacci, F., Mylopoulos, J., "Requirement Engineering meets Security: A Case Study on Modelling Secure Electronic Transactions by VISA and Mastercard", *Proceedings of the 22nd International Conference on Conceptual Modeling (ER 2003)*, October 13-16, 2003, pp. 263-276.

[11] "Graphical Modeling Framework", Retrieved January 2007 from http://protege.stanford.edu/

[12] Grau,Gemma, "Comparing the i* Tools", Retrieved January 2007 from http://istar.rwth-aachen.de/tiki-index.php?page=Comparing+the+i%2A+Tools

[13] Horkoff, J., *Using i* Models for Evaluation*, Masters Thesis, University of Toronto, Department of Computer Science, 2006.

[14] Kethers, S., Gans, G., Schmitz, D., Sier, D., "Modelling Trust Relationships in a Healthcare Network: Experiences with the TCD Framework", In *Proceedings of the Thirteenth European Conference on Information Systems*, Regensburg, Germany, 2005.

[15] Liu, L., Yu, E., and Mylopoulos, J., "Security and Privacy Requirements Analysis within a Social Setting", In *Proceedings of the 11th IEEE international Conference on Requirements Engineering*, RE. IEEE

Computer Society, Washington, DC, 2003, pp. 151-161.

[16] Maiden, N.A.M, Jones, S.V., Manning, S., Greenwood, J., & Renou., L., "Model-Driven Requirements Engineering: Synchronising Models in an Air Traffic Management Case Study", *Proceedings of 16th International Conference (CAiSE 2004)*, June 7-11, 2004, pp. 368-383.

[17] Martínez, A., Pastor, O., & Estrada, H., "Isolating and Specifying the Relevant Information of an Organizational Model: A Process Oriented Towards Information System Generation", *Lecture Notes in Computer Science, 3046*, 2004, pp. 783-790.

[18] "Microsoft Next-Generation Secure Computing Base - Technical FAQ", Retrieved July 2004 from www.microsoft.com/technet/Security/news/ngscb.mspx.

[19] Molani, A., Perini, A., Yu, E., Bresciani, P., "Analyzing the Requirements for Knowledge Management using Intentional Analysis.", *Proceedings of AAAI Spring Symposium on Agent-Mediated Knowledge Management (AMKM-03)*, March 24-26, Stanford University, 2003.

[20] Mylopoulos, J., Borgida, A., Jarke, M., Koubarakis, M., "Telos: Representing knowledge about information systems", *ACM Trans. on Information Systems. vol. 8(4)*, 1990.

[21] Mylopoulos, J., & Castro, J., "Tropos: A Framework for Requirements-Driven Software Development.", J. Brinkkemper & A. Solvberg (Eds), *Information Systems Engineering: State of the Art and Research Themes, Lecture Notes in Computer Science*, 2000, pp. 261-273.

[22] "OME, Organizational Modeling Environment", Retrieved January 2007 from http://www.cs.toronto.edu/km/ome/.

[23] "OpenOME, an open-source requirements engineering tool", Retrieved November 2005 from www.cs.toronto.edu/km/openome

[24] "The Protégé Ontology Editor and Knowledge Acquisition System", Retrieved January 2007 from http://protege.stanford.edu/

[25] Santander, V. F., & Castro, J., "Deriving Use Cases from Organizational Modeling", *Proceedings of the 10th Anniversary IEEE Joint International Conference on Requirements Engineering*, September 9 -13, 2002, pp. 32-42.

[26] Simon, Herbert A., *Models of man - social and rational*, New York, John Wiley and Sons, 1957.

[27] Strohmaier, M., Yu, E., Horkoff, J., Aranda, J., Easterbrook, S., "Analyzing Knowledge Transfer Effectiveness - An Agent-Oriented

Approach", *40th Hawaii International Conference on Systems Science (HICSS-40 2007)*, HI, USA., 2007.

[28] Sutcliffe, G. A., & Minocha, S., "Linking Business Modelling to Socio-technical System Design", *Proceedings CAiSE'99*, June 14 – 18, 1999, pp. 73-87.

[29] "Trusted Computing Group", Retrieved January 2007 from https://www.trustedcomputinggroup.org

[30] "Trusted Computing Group Backgrounder", Retrieved July 2004 from https://www.trustedcomputinggroup.org/.

[31] Yu, E., "Modeling Organizations for Information Systems Requirements Engineering", *Proc. 1st IEEE International Symposium on Requirements Engineering*, San Diego, California, USA, 1993, pp. 34-41.

[32] Yu, E. S. K., Mylopoulos, J., "Understanding 'Why' in Software Process Modelling, Analysis, and Design", *Proceedings of 16th International Conference on Software Engineering*, May 16-21, 1994, pp. 159-168.

[33] Yu, Eric S.K., Mylopoulos, J., "Using Goals, Rules and Methods to Support Reasoning in Business Process Reengineering", *International Journal of Intelligent Systems in Accounting, Finance, and Management*, John Wiley & Sons, 5(1), March 1996, pp. 1-13.

[34] Yu, E., "Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering", In *Proceedings of the 3rd IEEE Int. Symp. on Requirements Engineering (RE'97)*, 1997, Washington D.C., USA, pp. 226-235.

[35] Yu, E., Liu, L., "Modelling Trust for System Design Using the i* Strategic Actors Framework", In R. Falcone, M. Singh, Y.H. Tan (eds.), *Trust in Cyber-Societies - Integrating the Human and Artificial Perspectives*, Springer Verlag, 2001, pp. 175-194.

[36] Yu, E., Cysneiros, L.M., "Designing for Privacy in a Multi-Agent World", In R. Falcone, S. Barber, L. Korba and M. Singh (eds.): *Trust, Reputation and Security: Theories and Practice*, Springer-Verlag, 2003, pp. 209-223.