Analyzing Trust in Technology Strategies

Jennifer Horkoff
Department of Computer Science,
University of Toronto
jenhork @ cs.utoronto.ca

Eric Yu
Faculty of Information Studies,
University of Toronto
yu @ fis.utoronto.ca

Lin Liu
School of Software,
Tsinghua University, Beijing
linliu @ tsinghua.edu.cn

Abstract

As technology design becomes increasingly motivated by business strategy, technology users become wary of vendor intentions. Conversely, technology producers must determine what strategies they can employ to gain the trust of consumers in order to acquire and retain their business. As a result, both parties have a need to understand how business strategies shape technology design, and how such designs alter relationships among stakeholders. In this work, we use the Trusted Computing domain as an example. Can the technology consumer trust the advertised intentions of Trusted Computing Technology? Can the providers of Trusted Computing gain the trust of consumers? We use the i Modeling Framework to analyze the links between strategies and technologies in terms of a network of social intentional relationships. By applying the qualitative i* evaluation procedure, we probe the intentions behind the strategies of technology providers, facilitating an analysis of trust.*

Keywords: Trust, Business Strategies, The i* Framework, Goal Modeling, 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, diminished compatibility with competitors' products and misrepresentation of functionality are examples of some of the strategies that may influence technology. 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. 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 [1]. Unlike other common modeling notations 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.

Our work with the i* Framework differs from other approaches to trust (e.g. [2, 3]) 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. 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.

Specifically, trust is modelled as a *softgoal*, a goal without a clear-cut definition of satisfaction, as introduced in the NFR Framework [4], effectively treating trust as a non-functional requirement (NFR). The achievement of trust for one actor of another actor is assessed from the point of view of an actor in the domain.

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

Consider the issues surrounding 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). The proponents of this technology 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 apply our ideas due to the presence of multiple viewpoints concerning technology intentions, and the resulting uncertainty surrounding trust, privacy, and security.

Can an intentional modeling approach help shed light on the controversies surrounding Trusted Computing? Can we make the link between business strategies and the implementation of TC technology?

In this work, we briefly introduce the i* Framework and its evaluation procedure. In order to demonstrate the use of i* in analyzing the effects of technology motivated by business strategy, we walk through part of our TC analysis, depicting the major controversies in the domain. In the interest of space, some details are omitted.

2. The i* Framework and Evaluation Procedure

In analyzing the TC domain, the technology user wants to know: “Is Trusted Computing good for me?” and “Can I trust the technology and the technology provider?” The technology provider would like to know: “How can I make TC technology attractive to users?” and “If I do not gain the trust of the user, how will this affect profit?” In order to answer these questions, we identify domain actors, such as the technology user and provider, and represent their needs, wants and the relationships between them. What makes technology “good” for the user? How can the technology provider gain the trust of the user? We use a model such as Figure 1 to answer these types of questions.

The i* Framework, (i* for distributed intentionality), depicts such information using intentional 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** and **softgoals**, representing stakeholder desires which can be precisely and vaguely defined, respectively. **Tasks** are used to represent the desire for a specific action, and **resources** are used to represent desired entities.

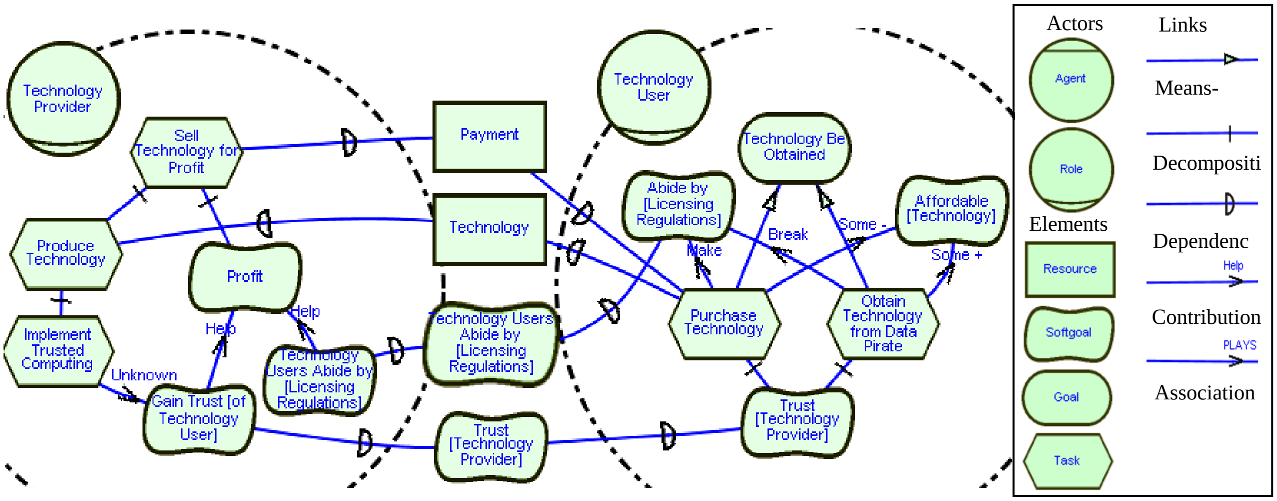

Technology Provider
Sell Technology for Profit
Payment
Produce Technology
Technology
Profit
Implement Trusted Computing
Help
Help
Unknown
Gain Trust [of Technology User]
Technology Users Abide by [Licensing Regulations]
Technology Users Abide by [Licensing Regulations]
Trust [Technology Provider]
Technology User
Technology Be Obtained
Abide by [Licensing Regulations]
Affordable [Technology]
Make
Break
Some -
Some +
Purchase Technology
Obtain Technology from Data Pirate
Trust [Technology Provider]
Actors
Agent
Role
Elements
Resource
Softgoal
Goal
Task
Links
Means-
Decompositi
Dependenc
Help
Contribution
PLAYS
Association

Figure 1. Simplified TC Example with Legend of i* Constructs

Associated with each element is the notion of satisfaction or denial, whether or not the element is accomplished given the set of satisfaction or denial values in the rest of the model, or given the input of the modeller. As softgoals do not have a precise definition of satisfaction, we used the term “satisficed”, to refer to a judgment of sufficient satisfaction.

Links in i*. 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, potentially including other tasks, goals, softgoals and resources.

A **means-ends link** from a task to a goal represents one way for achieving that goal. A **dependency link** states that an actor (the depender) depends on another actor (the dependee) for something (the dependum). **Contribution links** from any element to a softgoal indicate a qualitative effect. This effect can be sufficient to satisfice/deny a softgoal (make/break), can have a positive/negative contribution which is in itself not sufficient to satisfice/deny a softgoal (help/hurt), can have a positive/negative contribution of unknown strength (some+/some-), or can have an unknown effect (unknown).

Actors in i*. Elements in i* are associated with actors via an **actor boundary** - a dashed circle which contains elements. 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.

The i* evaluation procedure. Constructing an i* model showing relationships among goals and how they are achieved can provide valuable insights about the domain. However, to facilitate further analysis, a qualitative reasoning method is provided to evaluate whether goals are indeed achieved. The i* evaluation procedure, detailed in [5], is based on a procedure included with the NFR Framework [4].

The i* evaluation procedure facilitates analysis by applying labels representing the level of evidence towards the qualitative satisfaction and denial of model elements. These labels represent evidence which is sufficient to satisfy/deny an element (**satisficed/denied**), evidence which is positive but not in itself sufficient to satisfy/deny an element (**partially satisficed/denied**), evidence with an unknown effect (**unknown**), and the presence of both positive and negative evidence (**conflict**). In this work we use the qualitative partial labels for “hard” elements (goals, tasks, and resources) as well as for softgoals, in order to increase the expressive power of the evaluation.

The procedure starts with a set of initial labels given to graph “leaf elements”, elements having no input links, indicated via a highlighted square. These initial labels are chosen based on an analysis question.

In the first step of the procedure, a set of propagation rules are used to propagate present 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 pessimist 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 in a label bag until resolution in step 2.

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.

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	✗	✓•	✗•	✓•	✗•	✓•	?

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:

✓ > ✓• > ⚡ > ? > ✗• > ✗

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, it is unreasonable and impractical to expect such models to be complete. Instead we aim to produce models which are complete enough to facilitate useful analysis and communication. 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 evaluate the satisfaction of model elements.

For instance, in the case when an element receives both positive and negative evidence, such as in {✓•, ✗•}, the evaluator can decide that the overall evidence for the element is either positive or negative, or can decide that the evidence is of comparable strength, and give the element a conflict evaluation label. When multiple sources of only positive or only negative partial evidence is present, such as in {✗•, ✗•}, the evaluator can decide if this evidence is strong enough to satisfice or deny an element, combining the evidence to produce a value of satisficed or denied.

3. Analyzing Trusted Computing

In order to understand the players and relationships involved in Trusted Computing, to form the foundation for the exploration of business strategies, 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 by including elements which are likely not 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 divide our attention to two viewpoints, the proponents and the opponents of trusted computing.

For this study, the primary sources of information on the proponents side of Trusted Computing are technical reports and FAQ's of the TCG or TCG members such as [6, 7]. The information source for the opponent viewpoint has come from a FAQ written by Ross Anderson [8]. 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 following sections are simplified versions of the models originally created for the study.

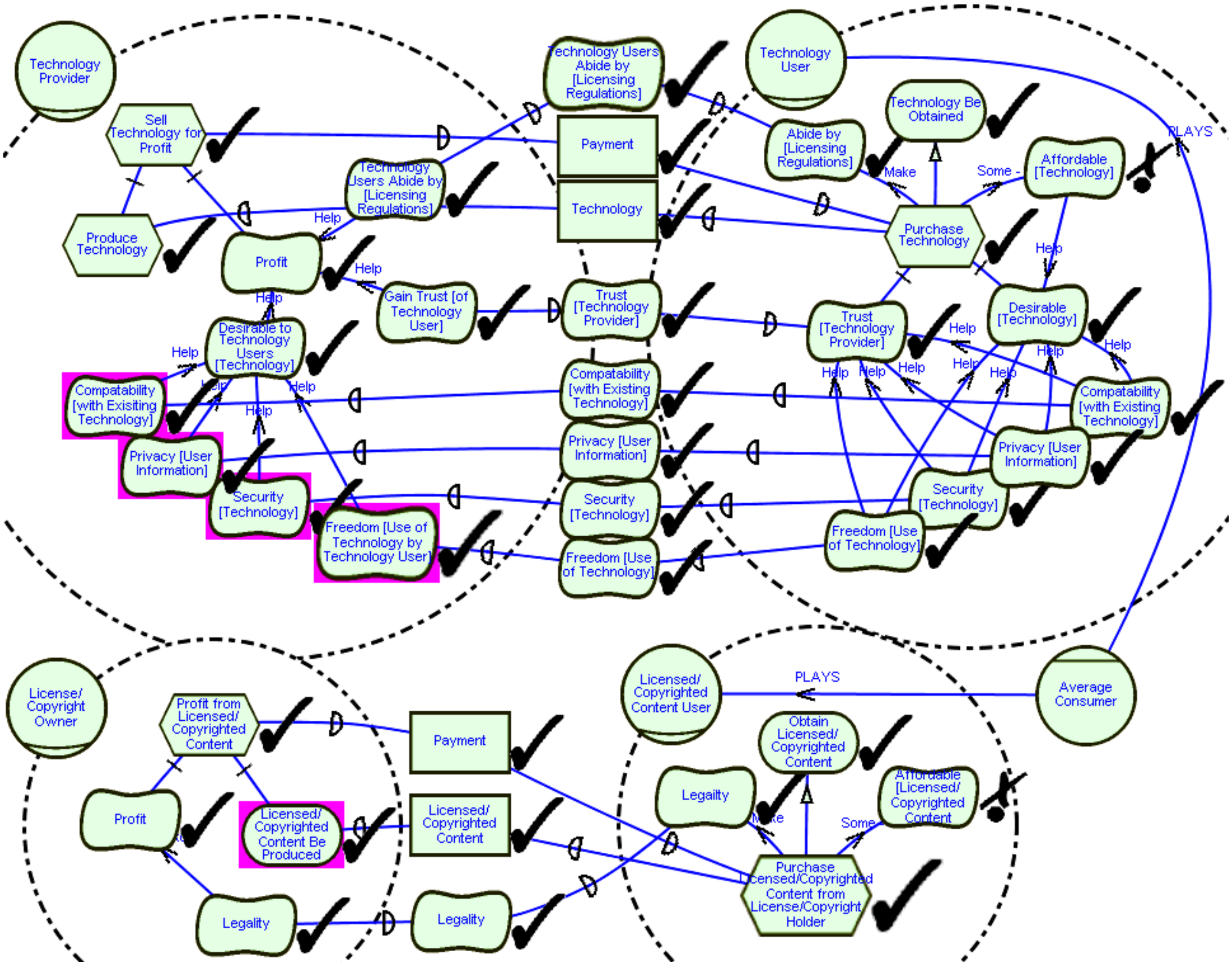
3.1 The Business of Content and Technology

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 2. 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.

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, as if the Technology User trusts the Technology Provider, they are likely to trust the technology.

We have included Compatibility, Security, Privacy and Freedom of Use, (lack of restrictions) as the criteria for Desirable technology which 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 since they are unlikely to be completely satisfied.



Technology Provider
Sell Technology for Profit
Produce Technology
Profit
Technology Users Abide by [Licensing Regulations]
Gain Trust [of Technology User]
Desirable to Technology Users [Technology]
Compatability [with Exisiting Technology]
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology by Technology User]
Help
Technology Users Abide by [Licensing Regulations]
Payment
Technology
Trust [Technology Provider]
Compatability [with Existing Technology]
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology]
Technology User
Abide by [Licensing Regulations]
Technology Be Obtained
Affordable [Technology]
Purchase Technology
Make
Some -
PLAYS
Trust [Technology Provider]
Desirable [Technology]
Compatability [with Existing Technology]
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology]
License/ Copyright Owner
Profit from Licensed/ Copyrighted Content
Profit
Licensed/ Copyrighted Content Be Produced
Legality
Payment
Licensed/ Copyrighted Content
Legality
Licensed/ Copyrighted Content User
PLAYS
Average Consumer
Obtain Licensed/ Copyrighted Content
Legality
Affordable [Licensed/ Copyrighted Content
Make
Some
Purchase Licensed/Copyrighted Content from License/Copyright Holder

Figure 2. The Business of Content Technology, before considering Malicious Parties

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 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 likely include other elements that help Desirability but not Trust, such as providing useful functionality. 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 which create technology in various forms, 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 satisfied (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.

This result 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.

3.2 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 3.

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.

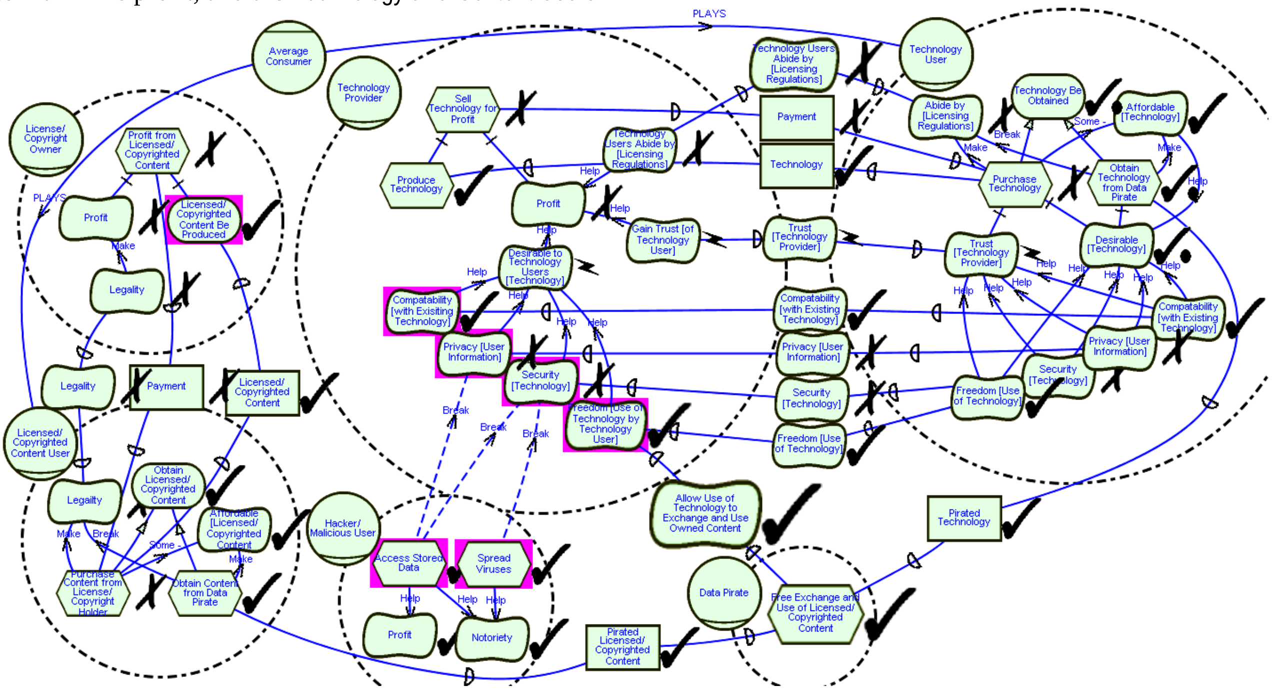

PLAYS
Average Consumer
Technology Provider
Technology User
License/ Copyright Owner
PLAYS
Profit from Licensed/ Copyrighted Content
Profit
Make
Licensed/ Copyrighted Content Be Produced
Legality
Sell Technology for Profit
Produce Technology
Profit
Help
Technology Users Abide by [Licensing Regulations]
Gain Trust [of Technology User]
Desirable to Technology Users [Technology]
Compatability [with Exisiting Technology]
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology by Technology User]
Break
Payment
Technology
Trust [Technology Provider]
Compatability [with Existing Technology]
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology]
Abide by [Licensing Regulations]
Technology Be Obtained
Affordable [Technology]
Some -
Make
Purchase Technology
Obtain Technology from Data Pirate
Trust [Technology Provider]
Desirable [Technology]
Compatability [with Existing Technology]
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology]
Legality
Payment
Licensed/ Copyrighted Content
Licensed/ Copyrighted Content User
Legaity
Obtain Licensed/ Copyrighted Content
Affordable [Licensed/ Copyrighted Content
Purchase Content from License/ Copyright Holder
Obtain Content from Data Pirate
Hacker/ Malicious User
Access Stored Data
Spread Viruses
Profit
Notoriety
Allow Use of Technology to Exchange and Use Owned Content
Pirated Technology
Data Pirate
Free Exchange and Use of Licensed/ Copyrighted Content
Pirated Licensed/ Copyrighted Content

Figure 3. The Business of Technology with Malicious Parties

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. We use contribution links across actor boundaries to represent the detrimental affects of these actions on the Privacy and Security provided by technology.

How do malicious parties affect the evaluation? We apply the evaluation procedure to Figure 3, 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).

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. This model 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 which follow.

3.3 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 4).

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. Further aspects and effects of TC technology described by proponents have been considered in a more detailed analysis, omitted here for simplicity.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.

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 this. In this simple model, the uncertainty concerning the effects of TC technology on Freedom of Use is depicted by an unknown contribution link. The overall effects of Implementing TC are highlighted by dashed circle (i).

Will TC Work? 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.

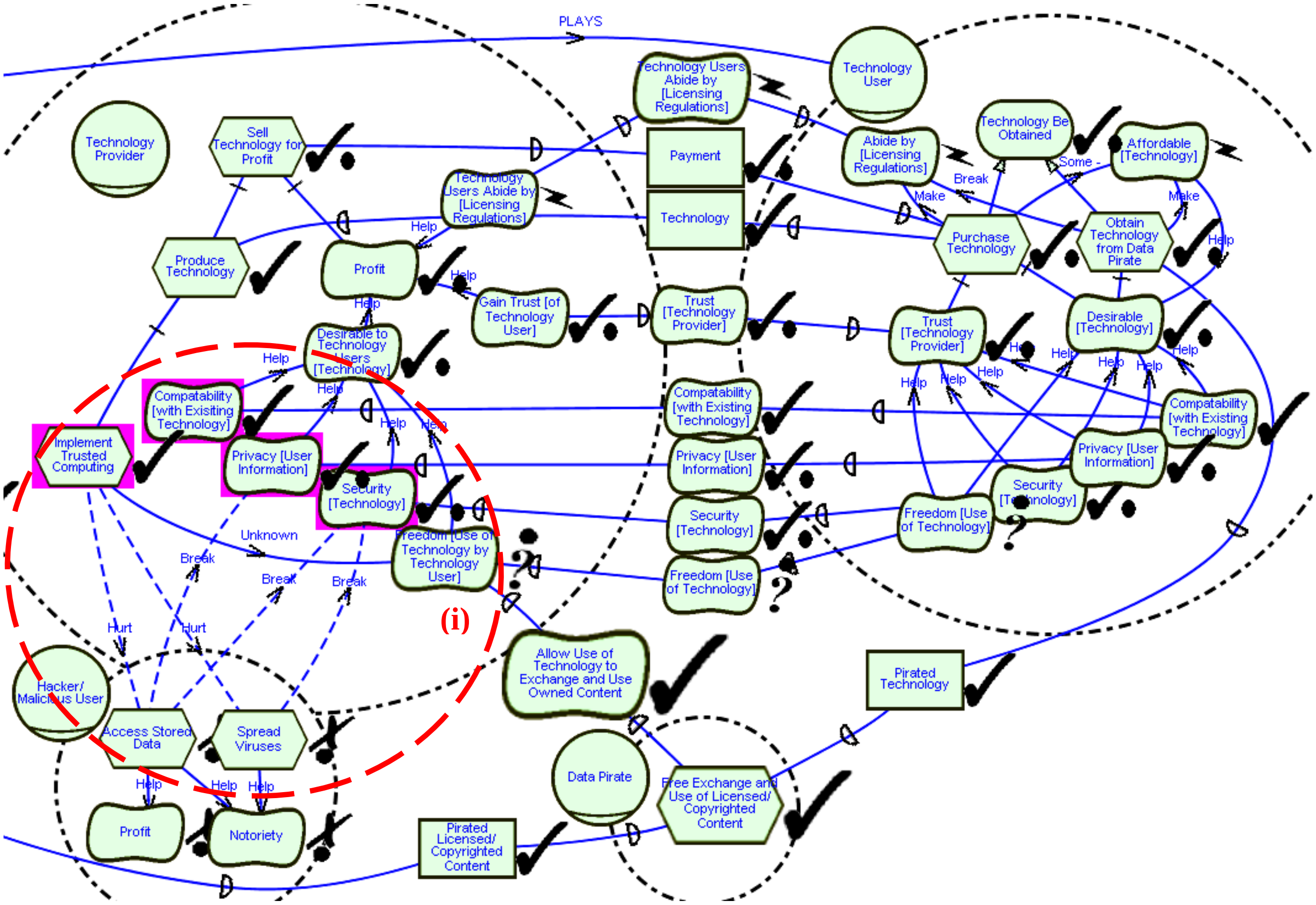

PLAYS
Technology Provider
Sell Technology for Profit
Technology Users Abide by [Licensing Regulations]
Payment
Technology
Technology User
Abide by [Licensing Regulations]
Technology Be Obtained
Affordable [Technology]
Some -
Break
Make
Purchase Technology
Obtain Technology from Data Pirate
Produce Technology
Profit
Gain Trust [of Technology User]
Trust [Technology Provider]
Desirable [Technology]
Desirable to Technology Users [Technology]
Compatability [with Existing Technology]
Implement Trusted Computing
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology by Technology User]
Freedom [Use of Technology]
Unknown
Help
Hurt
(i)
Allow Use of Technology to Exchange and Use Owned Content
Pirated Technology
Hacker/ Malicious User
Access Stored Data
Spread Viruses
Notoriety
Data Pirate
Free Exchange and Use of Licensed/ Copyrighted Content
Pirated Licensed/ Copyrighted Content

Figure 4. The Effects of Trusted Computing According to Proponents

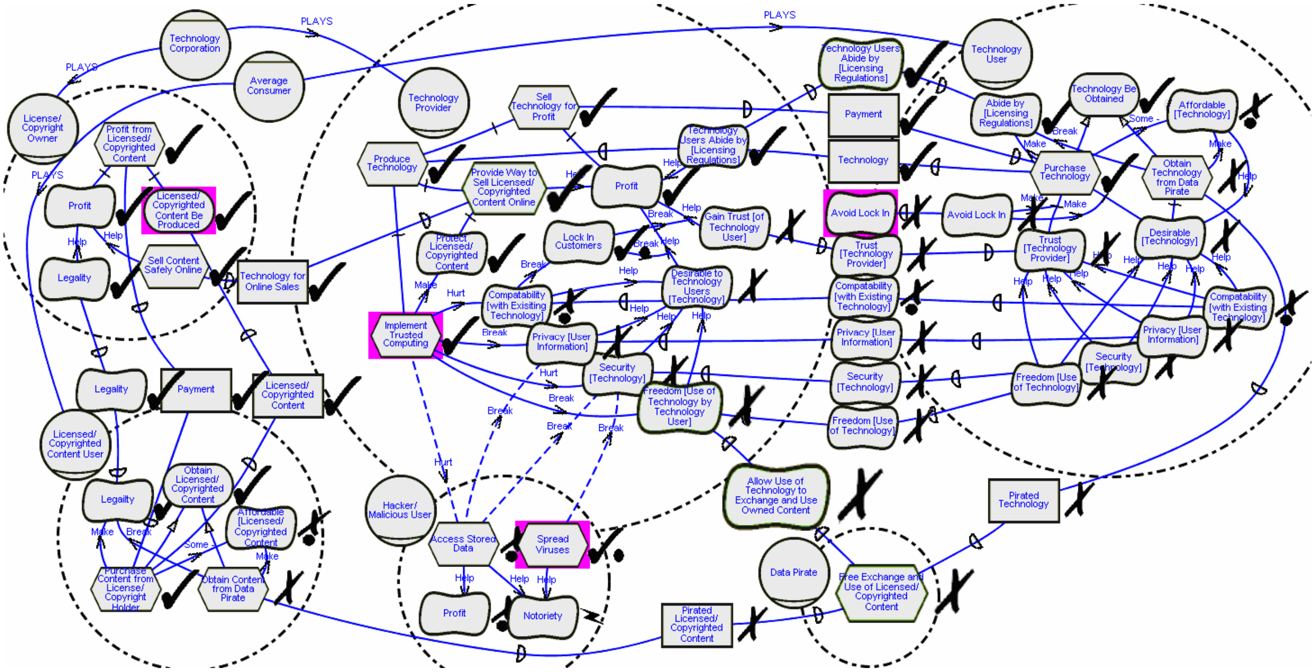

PLAYS
Technology Corporation
Average Consumer
License/ Copyright Owner
Profit from Licensed/ Copyrighted Content
Profit
Licensed/ Copyrighted Content Be Produced
Legality
Sell Content Safely Online
Technology for Online Sales
Payment
Licensed/ Copyrighted Content
Licensed/ Copyrighted Content User
Legailty
Obtain Licensed/ Copyrighted Content
Affordable [Licensed/ Copyrighted Content]
Purchase Content from License/ Copyright Holder
Obtain Content from Data Pirate
Make
Break
Some -
Help
Hurt
Technology Provider
Sell Technology for Profit
Produce Technology
Provide Way to Sell Licensed/ Copyrighted Content Online
Protect Licensed/ Copyrighted Content
Lock In Customers
Technology Users Abide by [Licensing Regulations]
Gain Trust [of Technology User]
Desirable to Technology Users [Technology]
Compatability [with Exisiting Technology]
Implement Trusted Computing
Privacy [User Information]
Security [Technology]
Freedom [Use of Technology by Technology User]
Hacker/ Malicious User
Access Stored Data
Spread Viruses
Notoriety
Avoid Lock In
Trust [Technology Provider]
Compatability [with Existing Technology]
Freedom [Use of Technology]
Technology User
Abide by [Licensing Regulations]
Technology Be Obtained
Affordable [Technology]
Purchase Technology
Obtain Technology from Data Pirate
Desirable [Technology]
Allow Use of Technology to Exchange and Use Owned Content
Pirated Technology
Data Pirate
Free Exchange and Use of Licensed/ Copyrighted Content
Pirated Licensed/ Copyrighted Content

Figure 5. The Effects of Trusted Computing According to Opponents

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.By modeling the point of view of proponents 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. However, one can question the logic of this strategy. 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?

3.4 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 [8]. We have taken the shared viewpoint model in Figure 3 and added the effects of Trusted Computing according to this viewpoint, producing Figure 5.

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 4 and 5.

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 4. As opponents of TC do not seem to discount its ability to help prevent Access to Stored Data, this link is retained.

What are the overall effects of Trusted Computing? 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.

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. 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. 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).

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. To demonstrate this, in Figure 6 we have included a part of an elaborated version of Figure 5. Here, we have included more detail on the actions of the malicious parties, and have decomposed the Implementation of TC, showing the effects of individual TC components.

4. Related Work and Discussion

The i* Framework has been explored in a requirements engineering and system development context [9]. In this work, as well as further demonstrating the domain knowledge gained by i* modeling, we test the ability of i* to assist in the analysis of technology strategies.

The intention of this approach is to explicitly reason about trust at an early, high-level of abstraction, when specific 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. [10], 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, [11, 12], 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 [12, 13].

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 [15].

Our use of i* has enabled us to depict and evaluate the motivations and strategies behind the implementation of Trusted Computing. We have shown the effects of implementing TC on trust, security, privacy, and have been able to analyze how these effects change when looking at the domain from different viewpoints. Differences between viewpoints concerning the intentions behind and effects of technology have been brought to light. 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.

The evaluation procedure has been used to make such overall conclusions on the domain, but could be used more extensively to answer a variety of intermediate 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?

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.

5. Conclusions and Future Work

Despite the success of our analysis, we can see some limitations of our modeling. 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 Figure 6. There is ongoing work to address this difficulty via the visualization of i* models, creating interactive tools which allow one to view, manipulate, and evaluate models [16]. Despite scalability issues, i* modeling has been successfully applied to complex, real-life applications [15].

This particular example is based purely on text based sources. As a consequence, it is difficult to validate the correctness of the resulting models beyond the knowledge acquired by the modellers. In future studies, we will aim to have direct involvement of stakeholders in constructing and verifying the models.

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.

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. Such modelling techniques can be used to take vendor strategies into account when guiding system design or procurement decisions.

In this work, we have presented i* modeling as a tool without a defined 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 are likely more complex, and can be explored in greater depth in future work.

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 the effects of competition in technology production, including technology producers who do not implement TC. In addition, there are many intermediate viewpoints concerning the effects of TC beyond the two explored in this work. For example, Arbaugh [17] 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.

References

[1] 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.

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

[3] 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.

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

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

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

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

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[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] 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.

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

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

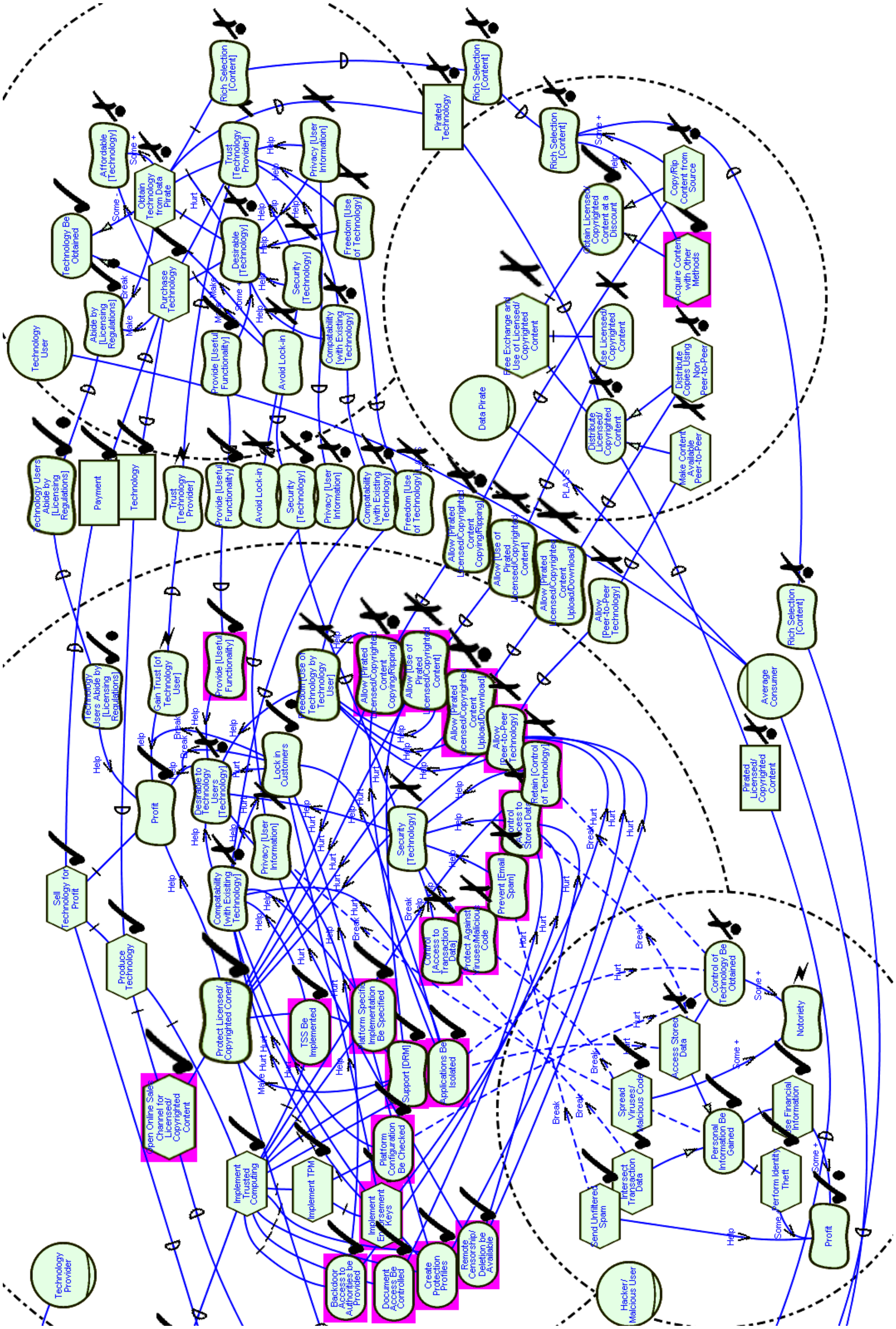

Technology User
Technology Provider
Data Pirate
Average Consumer
Hacker/ Malicious User
Rich Selection [Content]
Affordable [Technology]
Obtain Technology from Data Pirate
Technology Be Obtained
Purchase Technology
Abide by [Licensing Regulations]
Trust [Technology Provider]
Privacy [User Information]
Freedom [Use of Technology]
Desirable [Technology]
Security [Technology]
Compatability [with Existing Technology]
Provide [Useful Functionality]
Avoid Lock-in
Pirated Technology
Copy/Rip Content from Source
Obtain Licensed/ Copyrighted Content at a Discount
Acquire Content with Other Methods
Free Exchange and Use of Licensed/ Copyrighted Content
Use Licensed/ Copyrighted Content
Distribute Copies Using Non Peer-to-Peer
Distribute Licensed/ Copyrighted Content
Make Content Available Peer-to-Peer
Technology Users Abide by [Licensing Regulations]
Payment
Technology
Allow [Pirated Licensed/Copyrighted Content Copying/Ripping]
Allow [Use of Pirated Licensed/Copyrighted Content]
Allow [Pirated Licensed/Copyrighted Content Upload/Download]
Allow [Peer-to-Peer Technology]
Pirated Licensed/ Copyrighted Content
Gain Trust [of Technology User]
Freedom [Use of Technology by User]
Lock in Customers
Desirable to Technology Users [Technology]
Profit
Sell Technology for Profit
Produce Technology
Retain [Control of Technology]
Control Access to Stored Data
Prevent [Email Spam]
Protect Against Viruses/Malicious Code
Control [Access to Transaction Data]
Protect Licensed/ Copyrighted Content
TSS Be Implemented
Platform Specific Implementation Be Specified
Support [DRM]
Applications Be Isolated
Open Online Sales Channel for Licensed/ Copyrighted Content
Implement Trusted Computing
Implement TPM
Platform Configuration Be Checked
Implement Endorsement Keys
Backdoor Access to Authorities be Provided
Document Access Be Controlled
Create Protection Profiles
Remote Censorship/ Deletion be Available
Control of Technology Be Obtained
Notoriety
Access Stored Data
Spread Viruses/ Malicious Code
Personal Information Be Gained
Use Financial Information
Perform Identity Theft
Intersect Transaction Data
Send Unfiltered Spam
Help
Hurt
Break
Make
Some +
Some -
PLAYS

Figure 6. The Elaborated Effects of Trusted Computing According to Opponents