predict
prioritise
prevent

TRESPASS

Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

Deliverable D4.3.3

Visualisations of socio-technical dimensions of information security risks

Project:	TRE$_S$PASS
Project Number:	ICT-318003
Deliverable:	D4.3.3
Title:	Visualisations of socio-technical dimensions of information security risks
Version:	1.0
Confidentiality:	Public
Editor:	Peter Hall
Cont. Authors:	C. Heath, L. Coles-Kemp
Date:	2016-10-31

Part of the Seventh Framework Programme
Funded by the EC-DG CONNECT

Members of the TRESPASS Consortium

1.	University of Twente	UT	The Netherlands
2.	Technical University of Denmark	DTU	Denmark
3.	Cybernetica	CYB	Estonia
4.	GMV Portugal	GMVP	Portugal
5.	GMV Spain	GMVS	Spain
6.	Royal Holloway University of London	RHUL	United Kingdom
7.	itrust consulting	ITR	Luxembourg
8.	Goethe University Frankfurt	GUF	Germany
9.	IBM Research	IBM	Switzerland
10.	Delft University of Technology	TUD	The Netherlands
11.	Hamburg University of Technology	TUHH	Germany
12.	University of Luxembourg	UL	Luxembourg
13.	Aalborg University	AAU	Denmark
14.	Consult Hyperion	CHYP	United Kingdom
15.	BizzDesign	BD	The Netherlands
16.	Deloitte	DELO	The Netherlands
17.	Lust	LUST	The Netherlands

Document History

Authors		
Partner	Name	Chapters
RHUL	Claude Heath, Lizzie Coles-Kemp	All

Quality assurance		
Role	Name	Date
Editor	Peter Hall	2016-09-30
Reviewer	Marlon Fraile	2016-09-30
Reviewer	Lars Wolos	2016-10-15
Task leader	Claude Heath	2016-09-30
WP leader	Lizzie Coles-Kemp	2016-09-30
Coordinator	Pieter Hartel	2016-10-15

Circulation	
Recipient	Date of submission
Project Partners	2016-09-30
European Commission	2016-10-31

Acknowledgement: *The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRESPASS). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained herein.*

Contents

List of Figures

List of Tables

Management Summary

In conjunction with (The TRESPASS Project, D4.2.2, 2016), this deliverable addresses Task 4.3 which is defined in the Description of Work as: '"One strand aims at visualising complex technical information in an easy to understand way. The goal is to provide sufficient information to allow users to find, assess, and mitigate risks while maintaining ease of use and simplicity. The second strand will track the development of the socio-technical security model and develop tools to articulate the organisational and social dimensions that affect the likelihood of a successful attack. It will also develop attack/defence trees as a tool to visualise the logic of the model's calculations. These tools are expected to make the model and its calculation much easier to understand for practitioners."

Whereas (The TRESPASS Project, D4.2.2, 2016) presents our work to visualise the logic of the model's calculations, the visualisation of attacker profiles and the socio-technical calculations within the attack tree analysis, the work presented in this deliverable shows our work with the LEGO™ method to allow users to find, assess, and mitigate risks while maintaining ease of use and simplicity. In addition this deliverable presents the *InterActor* prototype which provides a means to transcribe social data gathered from the WP2 social data extraction tools. We demonstrate using the LEGO™ modeling process how this can be done. *InterActor* enables users to visualise the social networks within this data and to export elements of this data into the ANM, thus providing a bridge between the analogue, qualitative data and the digitised, quantitative data of the Attack Navigator and underlying model.

Key takeaways: In order to complete our work in socio-technical risk visualisations, we have complemented the work in (The TRESPASS Project, D4.2.2, 2016) by developing a means of capturing social data and passing it to the ANM. The means of achieving this can be described in the following three aspects of our work:

- The development of a process and framework for taking as input the qualitative social data gathered, such as the LEGO™ physical modelling process, and converting such data into output that can be consumed by the ANM.
- The development of an prototype called *InterActor* designed to instantiate the framework mentioned above, as supported by industry feedback we have gathered.
- The development of visualisations that articulate the communities of practice within a given risk scenario, that is: representing those groups of people who share security practices, and articulating the relationships between social actors therein.

By concentrating on the visualisation of the social dimensions of risk, we have sought to redress the general trend observed in the current state of the art that favours the visualisation of the technical over the visualisation of the social. Moreover, we have sought to create visualisations of these social practices that will enhance the technical risk representations that have been developed in TRE$_S$PASS, as seen in (The TRE$_S$PASS Project, D4.2.2, 2016), with the aim that social and technical visualisations will mutually support one another.

As the reader will see, the digital prototype *InterActor* supplies visualisations of communities of practice and some of the social attributes of risk. This is our contribution to extending the state of the art, by synthesising the technical and the social into truly socio-technical visualisations of risk.

1 Introduction

In this final report on visualisations of socio-technical dimensions, the focus is the prototype for articulating some of the social dimensions, not addressed in the visualisations in (The TRESPASS Project, D4.2.2, 2016) and the written report to illustrate and explain the prototype produced.

1.1 Goals

The main goal of this deliverable is to present the prototype that we have developed to enable security practitioners to produce visual representations of some of the social aspects of cyber security risk.

The specific aims of this deliverable are to:

- Present the *InterActor* prototype, which is designed to visually present some of the social aspects of risk;
- Explain the prototype's design philosophy and how it relates to the Attack Navigator Map (ANM);
- Give an overview of the prototype's functionality; and
- Describe the evaluation process and explain how the target user community engaged with and fed back into the prototype design process.

.

1.2 Choices made

The development of the *InterActor* prototype was directly influenced by the participatory nature of the engagement with the target user community. Eighteen months of engagement was conducted using physical modelling techniques (primarily LEGO™) in order to develop a clear understanding of what was required from the prototype and how such a technology might be used. The prototype design choices made that stemmed from these engagements are documented in this deliverable.

1.3 Foreground and background

As regards Intellectual Property (IP), the following elements of the visualisation platform are foregrounded:

1. Attack Navigator Map.
2. The visualisation toolkit.
3. The Attack Tree visualisation.
4. The *InterActor* prototype.

The current prototypes of the TRE$_S$PASS user interface, namely the Attack Navigator and one of its main tools, the Attack Navigator Map, are foreground to the project. Early versions of some TRE$_S$PASS tools (ADTool (v1.1), DFTCalc, Approxtree etc.) are background of the project. The individual tools have been improved by their development teams and constitute foreground of the project. TREsPASS.js is foreground to the project, other libraries are background to their respective developers (d3, angular, react, bootstrap, keystone). Everything else in this document and on the prototype website[1] is foreground.

1.4 How to access the prototypes

Prototypes are at the core of the three final deliverables from WP4. There are several ways to access these prototypes.

1. Via the visualisation prototypes, tools and methods showcase:
   https://visualisation.trespass-project.eu (no log-in needed).
   This showcase includes:
   - Publications
     - Book series '"Picturing Risk":
       https://visualisation.trespass-project.eu/?cat=69
   - Methods for visualising security risks
     - Attack Tree component visualiser (XML to Attack Tree):
       https://visualisation.trespass-project.eu/?p=409
     - Visualisation Atlas:
       https://visualisation.trespass-project.eu/?p=122
     - Attack Cloud visualisation:
       https://visualisation.trespass-project.eu/?p=236
     - Attack Tree visualisations:
       https://visualisation.trespass-project.eu/?cat=5

[1] demo environment at http.trespass.lustlab.net

  - TRESPASS security visualisation methods:
    https://visualisation.trespass-project.eu/?cat=12
  - ATM case study visualisation:
    https://visualisation.trespass-project.eu/?p=117
  - DBIR Attack Graphs 2015 visualisation:
    https://visualisation.trespass-project.eu/?p=275

- Complexity prototypes
  - Time-Containment Visualiser (TiCoVis):
    https://visualisation.trespass-project.eu/?p=55 (no log-in) or
    https://trespass.itrust.lu/tkb/tkb/TiCoVis (log-in at the TRESPASS portal required - see below)
  - Complexity prototype Cloud Environment Actor Visualiser (CEAV):
    https://visualisation.trespass-project.eu/?p=216 (no log-in) or
    https://trespass.itrust.lu/tkb/tkb/CEAV (log-in at the TRESPASS portal required - see below)

- Social-technical visualisations
  - *InterActor*:
    https://visualisation.trespass-project.eu/?p=482
    The above page on the showcase includes a link to the prototype itself [2]:
    InterActor
  - Paper Prototyping:
    https://visualisation.trespass-project.eu/?cat=14
  - Lego methods:
    https://visualisation.trespass-project.eu/?cat=18

2. Via the TRESPASS portal:
   https://trespass.itrust.lu/login.
   First time log-in: Click on Sign-up, you will receive a confirmation email, you need to click on it to acknowledge the registration. The itrust ICT administrator will have to personally validate your account. Once you receive the validation email, you will be able to access with the same credentials:
   - The individual tools
   - The Attack Navigator
   - The Attack Navigator Map
   - The SVN repository for the update of programs

[2] Please note that isolated issues have been reported accessing the prototype using *Eduroam* wifi in certain institutions, due to local access rules at host institution sites.

- Visualisation components (directly accessible at https://trespass.itrust.lu/visualizations)

1.4.1 Getting started with the prototypes

- Downloadable demo file: ATM case study XML (can for instance be used in the Attack Tree component visualiser (XML to Attack Tree): https://visualisation.trespass-project.eu/?p=409
- Github repositories where visualisation code is hosted: https://github.com/trespass-project
- The manual to the Attack Navigator Map: *ANM Manual*

1.5 Document structure

We start this document with an overview of the general approach being taken by WP4 towards visualising socio-technical dimensions. Initially we assert and describe a number of general design principles, techniques, and processes to be taken from our work. Particular reference is made, throughout, to the way in which constructed narratives can be used to represent the socio-technical data that has emerged from case studies. Throughout this Deliverable, the IPTV home-banking case study is used as a common thread in order to illustrate the action of these principles and techniques (The TRESPASS Project, D4.3.1, 2014).

Following this, the prototype instantiations of our work are described, in the form of our LEGO™ scoping methodology, a paper prototyping method of risk assessment, and the *InterActor* prototype to record and visualise data gathered from physical and other modelling interactions with stakeholders and security practitioners. These prototypes are all concerned with how to elicit and record social data, and they also address the question of how to integrate this data into the TRESPASS platform and into the ANM in particular.

Finally, we summarise how our prototypes and visualisations have been evaluated, based upon typical user-journeys that can be made with the tools, and we provide excerpts of feedback from users who have provided high degree of satisfaction with the tools and recommend their use within the field (Chap. 6). We conclude with some observations how TRESPASS visualisations have advanced the state of the art, and reflect the potential for exploitation of our work.

2 General visualisation principles and techniques

A socio-technical system is a system consisting of human behaviour, technology and the policies that influence human behaviour. The key properties in the socio-technical system are entities, interaction possibilities, and quantitative and qualitative properties associated with interactions. Our socio-technical visualisations therefore focus on the interaction possibilities and the presentation of the quantitative and qualitative properties of those interactions. Primarily, the input for these socio-technical visualisations came from the analysis techniques developed in WP3 and the results of the physical modelling techniques developed in WP2.

The physical modelling sessions reflected the importance of understanding interactions between elements from the point of view of relationships between social actors and the communities of practice that are sustained by those relationships.

In order to develop the socio-technical visualisations we have deployed a number of general visualisation principles and techniques that have been deployed across WP4 (full details can be found in (The TRESPASS Project, D4.2.2, 2016)):

Similarity concerns things that share visual characteristics such as shape, size, colour, texture, value or orientation which will be seen as belonging together.

Continuation predicts the preference for continuous figures.

Closure applies when viewers tend to see complete figures even if part of the information is missing.

Proximity and contiguity states that things which are closer together will be seen as belonging together.

Figure and Ground elements of the scene which are similar in appearance and shape are grouped together to be seen as a whole.

Pre-attentive Variables and Layering Pre-attentive variables operate mostly at a 'subconscious' level. Well designed pre-attentive factors like shape, color hue, brightness, saturation, position, orientation, texture, and size (Tidwell, 2005), cause the appropriate visual elements to perceptually 'pop out,' and similarity causes them to be seen as connected to one another. This segments data, while relationships among the whole are preserved.

In concert with these principles and techniques we use others that organise our approach to the specifically non-visual complexities of socio-technical systems:

- *Ashby's Law of Requisite Variety* states that, paradoxically, complexity is needed in order to tackle the challenges posed by complexity: "variety absorbs variety, defines the minimum number of states necessary for a controller to control a system of a given number of states." (see, WR Ashby, "An Introduction to Cybernetics", London, Chapman and Hall, 1956).
- Complex systems have a high number of variables and a high level of interdependence, such that linear models do not account for transitions between states (Flach, 2012). To draw from classical organisational theory (Thompson, 1967), complex systems are characterised by *reciprocal interdependence*. As complexity increases, Ashby's Law suggests that the demand increases for distributed, flexible forms of control like this process of mutual adjustment (Flach, 2012). Ideally, security visualisation tools should support this distributed form of control.
- An analogy can be made with navigation, which, while it may be guided by a map, is never an entirely cognitive process, but is embodied, situated, and subject to change.
- Given Ashby's Law, security visualisation tools need to support feedback loops. "Feedback changes the behaviour of the system, making it impossible to understand the whole through understanding each of its parts." (Norman & Stappers, 2015).
- The importance of visual notation to explicitly cope with the complexity of the described system. "Physics of Notation" (Moody, 2009).

3 Visualisation principles and techniques applied to TRESPASS

We have taken the general principles described in the previous chapter and made them core to the ANM to respond to the challenge of visualising socio-technical systems:

1. Filtering/highlighting/sorting.
2. Exploiting visual form through iconography and abstraction.
3. Overview and drill-down.
4. Multiple views.

These techniques are discussed in other Deliverables (The TRESPASS Project, D4.2.2, 2016).

In addition, to these general principles the following visualisation principles have been used to visualise the interactions between elements, interactions which define a socio-technical system:

- **Proximity or contiguity** refers to things which are closer together will be seen as belonging together.
- **Pre-attentive variables** refer to the way in which the organisation is depicted and described influences how users frame the data about that organisation.
- **Spatial and cultural regimes**.
- **Collapse and expand: Technical** Users can unfold technical and spatial dimensions at will, in order to make a closer inspection of the individual infrastructural units (servers, or computers, and so on). This is an apparent **'curling up' or compressing of highly complex technical dimensions** within the representation of the social dimensions - the way in which digital infrastructure can be viewed in a compressed form, as groups clearly linked to specific organisational spaces.
- **Collapse and expand: Social** The actors in a given scenario are treated in a similar way, reducing the complexity of the representation via quickly comprehensible iconic visual forms that are designed to summarise the key intrinsic attributes of the actors. These **actor icons are dynamic and responsive**, and are tightly connected to the surrounding mapping by colour-coded lines that lead to specific organisational/hierarchical spaces, according to their business roles and professional relationships.

- **Closer inspection and editing** Actors can also be selected by users and queried in order to find more detail about how and where linear connections lead (a visual and manual operation), to examine and edit their profiles and persona traits (a primarily textual operation that is carried out manually).

Figure 3.1: A digital collage summarising the relationships within communities of practice and relative scale of items built into a LEGO™ model of a scenario.

Beyond this several of WP1 model concepts have been referenced as we have developed specific socio-technical visualisation techniques:

- **Adjacency** allows us to represent neighbouring relationships between objects such as a floor that has neighbouring rooms or networks separated by a firewall's **containment**.
- **Locations** refers to the set of locations and (neighbouring) connections. A location relation between, for example, rooms in a spatial environment.
- **Infrastructure** refers to the set of locations and (neighbouring) connections. A location - relation between, for example, rooms in a spatial environment.

- **Interaction and Transition Social Role** From the social aspect we are interested in the transition of one role to another, as well as the interaction between roles. Through role interaction and role transition we can represent the impersonation of an adversary and adversary's direct interaction with an employee.
- **Relation Change** refers to the possibility to change the relation between two entities.

The visualisation techniques for socio-technical systems described in this chapter were prototyped graphically in the first instance (Fig. 3.1). This image, while unlabelled, shows one way in which several techniques can be combined. The grouping of elements suggests a overall gestalt or 'visual thinking' equivalent of the raw relationships and properties of such systems. Using a combination of abstraction and iconography a mapping such as this should also be able to represent narrative flow, when interacted with by a user. An interactive force directed graph should have layers of data accessible via semantic zooming, contextual awareness, and highlighting methods. Finally, a way to access multiple views upon the system should provide users with a dynamically framed overview.

4 Visualisation processes

Visualisation processes relate to the systematic way that WP4 has organised the general principles, methods and libraries, such that they fit together to respond to the stated problem space.

The process for developing socio-technical risk visualisations developed in WP4 is as follows:

- Characterise the socio-technical system to understand the elements within the risk assessment and the interactions and relationships between those elements.
- Identify the patterns of interactions between social elements and group these patterns into communities of practice that reflect the different risk positions in operation within a socio-technical system.
- Identify the control strengths and pathways to attack within and between each of the communities of practice.

4.1 Characterising socio-technical systems

The visualisation work of WP4 has been guided by a definition of the term 'socio-technical' that is given below. The basic assumption in the TRE_SPASS modelling framework is that there are systems that can be represented in models, which have states representing properties that can change over time:

A socio-technical system is a system consisting of human behaviour, technology and the policies that influence human behaviour. The key properties in the socio-technical system are entities, interaction possibilities, and quantifiable properties associated with interactions. The quantifiable properties include difficulty, risk for attacker, rewards, and visibility, for example. The quantitative values attributed to these properties, however, need to be complemented with an understanding of the relationships and interactions between entities. Such an understanding is emergent from the particular risk situation and from the data that is fluid and often ephemeral.

For the purposes of WP4's work and for this Deliverable, we can assume that as well as quantitative there will also be qualitative 'properties associated with interactions'. It is these that the visualisation methods most often seek to represent, alongside quantitative properties. It might well be argued that qualitative dimensions of these interactions cannot be reduced to or even mapped directly onto quantitative properties. This Deliverable does not assume that this is the case, but rather we set out to demonstrate that an analyst is

capable of using our tools to assist them in selecting which social and which technical data to strongly associate in practical terms.

A socio-technical security model is a model of a socio-technical system specifically focused on security risks in such systems, consisting of (1). a specification of objects, relations, and capabilities, (2). a specification of possible transformations, and (3). a specification of what constitutes an attack.

The socio-technical security model is made up of several types of components: **Spatial components** (refers to the geometric representation of its shape in some coordinate space, or its 'geometry'); **Social components** (a human as an entity that interacts in the model, can change location between rooms for example, and can have relations with entities, and actors can interact with each other); **Locations** (entities in the spatial component); **Object component** (the set of all objects); **Objects** (entities that can be moved around through the spatial component); **Digital component** (this concerns all programs and data that are present in objects supporting digital data storage, processing and communication); **Action** (a change to the state of the socio-technical system as represented in the socio-technical security model); **Actor** (an (in)animate object that executes actions).

4.2 Visualising socio-technical patterns

Above and beyond this description of what constitutes a socio-technical model, WP4 has identified the importance of visualising larger patterns of social behaviour. There is potential for highly effective graphical expression of data that relates to such larger patterns of behaviour, repeated over spatial and temporal locations. This potential has been noted by some practitioners (see Chap. 5).

4.2.1 Stage-Zero risk modelling

In (The TRE$_S$PASS Project, D2.3.2, 2015) we described the importance of brainstorming and scenario setting in the risk assessment process. As part of our WP2 work, we presented the brainstorming process as a type of "Stage-Zero" risk assessment stage. In this deliverable we have used this stage as the basis from which we have modeled our prototype, *InterActor*, that visualises the some social aspects of a risk scenario.

In this sub-section we describe the types of data that are extracted from Stage-Zero participatory physical modelling engagements. The central purpose is to show how this data arising from the brainstorming stage can be used to identify and visualise the key narratives emerging from these sessions. In doing so, the aim is to take account of the different actor perspectives inherent in the data, using these to pattern the resulting visualisations (Heath, Coles-Kemp, Hall, et al., 2014).

Table 4.1 shows a selection of the many data parameters that can be taken from TRE$_S$-PASS LEGO^{TM} models. Previous experiments with interactive data visualisations using existing tools (Excel, RAW, Tableau, VISMIO) have shown that this data can be harnessed

NO.	VISUALISATION	ASSOCIATED DATA	TYPE
1	**Visual size**	*Scale* for each element	Network map
2	**Line weight/colour**	*Negative/positive keyword freq*	Network map
3	**Clustering**	*Grouping and social practices*	Map/Actors
4	**Location**	Relationship btwn items on model	Map/Narrative view
5	**Grouping**	*Sets of related actors*	Map/Narrative view
6	**Highlights**	Keywords/Transcript	Actor details

Table 4.1: Summary of the ways in which the participatory data can be combined in visualisations.

to generate informative visualisations suitable to this domain (Fig. 4.1). The metrics associated with these data types relate to ordinal measurements or simple relational properties taken from the physical outputs from the sessions.

The interactive features of these trial visualisations do not elicit all of the aspects of the social data gathered by TRE$_S$PASS methods. They do not sufficiently illustrate the varied nature of connections between actors, or even the basic 'properties associated with interactions' which have been identified above as key to socio-technical systems. This has prompted the design of a prototype tool, *InterActor*, to manage how data is structured for visualisation.

For the purposes of gathering and modelling social aspects of risk scenarios, The TRE$_S$-PASS tool set includes the analogue data-gathering kit (in particular the LEGO^{TM} data gathering methodology) and the *InterActor* prototype. In addition, other techniques described in (The TRE$_S$PASS Project, D2.3.2, 2015) could be included as elements of this tool set, if they were so developed. Within TRE$_S$PASS, the LEGO^{TM} methodology is primarily used as a means of mapping actor relationships. Physical models and discussions revolving around them reveal the critical points at which the social dimension needs to be considered.

During the LEGO^{TM} evaluation and engagement sessions that were run extensively during years two and three of the TRE$_S$PASS project it was consistently fed back by participants that if only one social aspect emerging from the physical models should be preserved in the form of transferable data, it should be the set of actors with specific relationships, with any 'policies' that may be attached to them. The modelling process uncovers a diverse range of types and qualities of these relationships, and it is these that are to be recorded by another TRE$_S$PASS tool (see next Chap. 5).

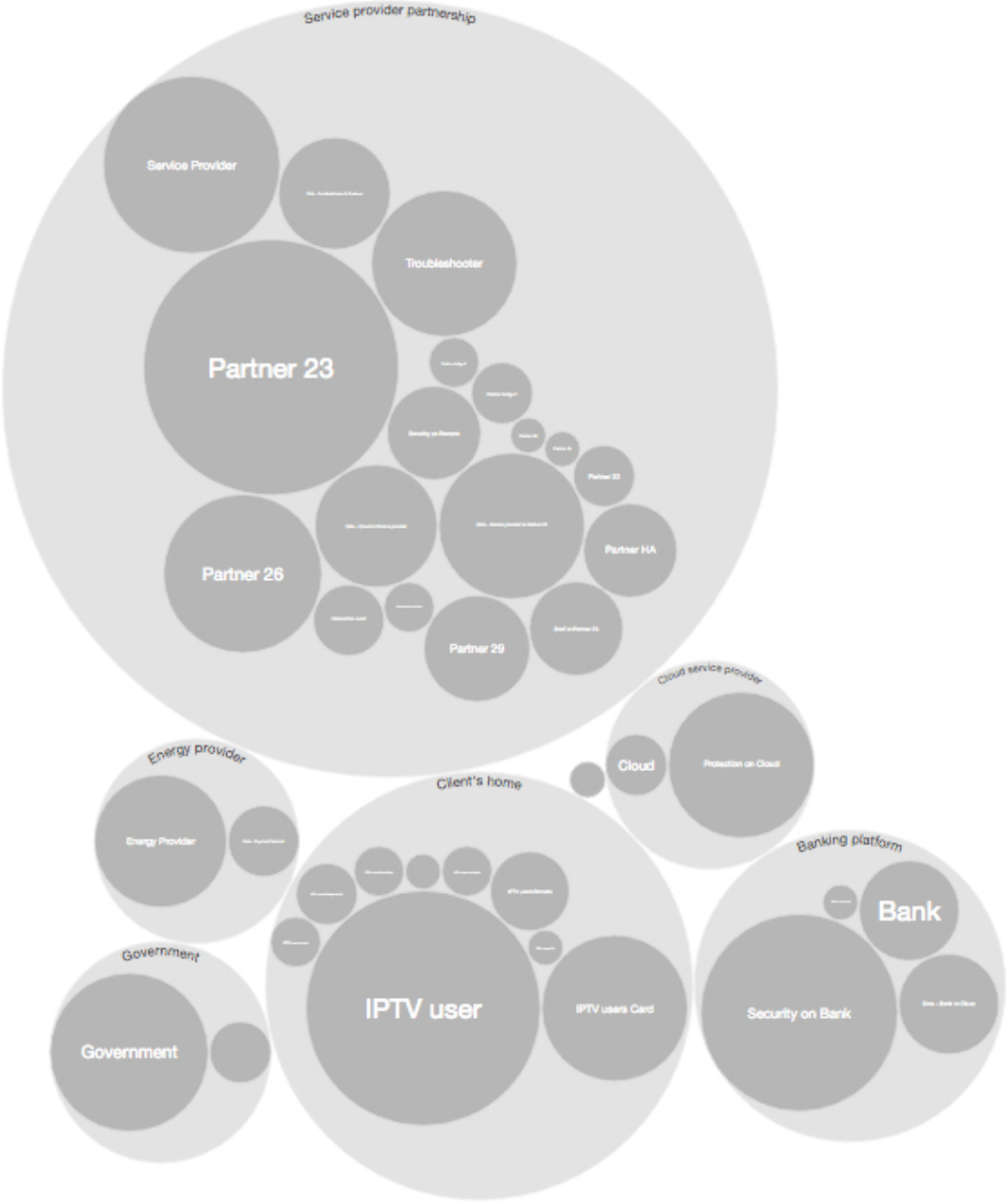


Figure 4.1: LEGO^{TM} data visualised with VISMIO.

5 Prototype: *InterActor*

From our extensive contact with security practitioners during the LEGO™ evaluation and engagement sessions, a need has been identified for a method where data can be captured during the co-creation process, or in a 'brainstorming' setting. This needs to be deployed during and after engagements and as a means to extend the modelling process, before insights that are produced are lost.

Furthermore, a parallel requirement has also been identified, for practitioners to be able to collate, manage and visualise the complex social interactions across any given scenario, and across any given business (see Sect. 4.2). This includes modelling their own roles within this business, as a way of managing and accounting for how an issue is being tracked within its workforce. There was a clear need to manage tasks by establishing a clear and comprehensible narrative that can be understood and developed by all team members and stakeholders involved in a risk scenario.

The 'unique selling point' of any such tool would be to package the analytical processes into a single place, making a potentially complicated task of understanding 'messy' social practices more manageable. The prototype described below has been conceived as a way of extending and facilitating the co-construction process, and is intended to be used on-site during and after workshops, in face-to-face sessions, and that if desired, work can be shared remotely via its web-based architecture. In addition, starting points are provided so that users may craft their own forms of input (using a spreadsheet view of their data) that will be relevant to their practice.

The overarching narrative of the prototype is to assist the practitioner in finding, mapping, and integrating the communities of practice and the social practices deployed by those communities that support controls. The tool is designed to provide a more refined view of how control strengths in specific areas are supported by (and are also based on) specific values and perspectives of actors, in groups or as individuals. Thus the prototype structurally analyses the outputs of participatory practitioner risk assessment workshops as developed in TRE$_S$PASS (see Sect. 4.2.1). The outputs of each participatory workshop can in this way be harnessed to create a richer and scaleable view of the complex interactions within a socio-technical model and system.

A minimal working example (MWE) is given as illustration of the functionality of the *InterActor* prototype. This is excerpted from our IPTV (Internet Protocol Television) case study, which has been modelled in detail and used as a testing ground for the development of the prototype. However, for the sake of clarity we present only one location in the scenario, the client's home, with children, carer and the technology needed to enact the IPTV home-banking service.

5.1 Scoping the prototype: consulting practitioners

Figure 5.1: Summer School, RHUL, 2016. A group models a 'smart home' scenario with LEGO™, while beside them an analyst transfers the actors, assets, and attacker goals from their physical model into the ANM on a laptop. This yielded a first visualisation of attack trees produced by processing the scenario, as modelled by the group.

After eighteen months of LEGO™ engagements and evaluations (Fig. 5.1) we sketched a potential prototype that would meet some of the requirements that we had elicited during these sessions. We then ran a discussion group with three participants met with in recent engagements in London, which included personnel working in banking, government/defence, and an independent practitioner where we presented sketches of a notional prototype derived from the requirements. The focus of this discussion was to develop some potential use cases for the prototype prototype:

- **Comparing operating models**.
- Maintaining **design goals** during new product development.
- **Tracking** how the relationships among teams and groups are developing.
- **Leveraging** the skills and interests of individuals and teams, with the aim of fulfilling the security role as an enabler.
- Teasing out the details of **communities of practice** and throwing light upon any shadow practices existing in the workplace.

Note that the above points concern relatively high-level abstractions of working processes.

An example **banking use-case** was given by one participant:

> *The ideal tool would allow the security practitioner to follow the overall progress of their work as it unfolds into different teams and contexts. In particular, it could be envisaged that the prototype records data during a 1-2 day internal workshop on designing a new product and planning for its launch. Models created by different teams, based on their own work, could be merged via the prototype in order to develop a common shared representation of goals and of progress made towards them.*
>
> *It was stated that resulting mappings of actor networks could be integrated with Visio swim-lanes diagrams and be used to track the rest of the development cycle and its future in the business. This ability to map out the social context of an initiative would be a valuable way to simultaneously (and in parallel) map out cyber-security risks against the infrastructure of the business. Use of the tool in this way would allow our practitioner to see whom (and what) to leverage, and thus for them to be clear about where social practices impact the infrastructure. In the example given, the predominant values and skills of teams and individuals can be followed and planned for in relation to the development of the new product.*

5.1.1 Technical Architecture - *InterActor*

From this discussion session and from the requirements we had gathered during the eighteen month programme of LEGO™ modelling engagement and evaluation, we developed a brief for the *InterActor* prototype. This tool is designed as a simple web-based desktop application. It has three central technical aims, that it should be **responsive, scaleable, and shareable**.

Its components are *node.js* and *d3.js*. It is a flexible *Document-based* schema, stored in JSON format. Much of the logic in querying/manipulating the data is therefore carried out beforehand, written in the node based middleware for the tool, or “App” as this has become generally known. In terms of how the graphing of elements is presented to users, there is a web server instance with a d3 and HTML focused front-end. D3 uses JSON to hold the data which it applies into its visualisation code, in a simple network/directed graph that shows a collection of nodes and a collection of relationships. The data generated by the prototype is held in a document-based database as JSON files.

Export. As well as exporting in textual and spreadsheet form, the prototype will export graphs as .jpgs, pdfs, and .svg files. In addition to this there will be scope for the exporting of a simplified UML description. UML uses the categories of ‘Actors’, ‘Roles’, ‘Props’ and ‘Actions’, and it should be possible to add a future feature, to allow a UML-based output from the system.

Integration. Within the ANM, the expert user is able to customise their software in order to summon up the relevant social data at any point on their ANM model (see Fig. 5.2).

In addition, and more immediately, the ANM user is able to import actors as .xml files exported from *InterActor* (Fig. 5.17). When working with the prototype alongside the ANM in this way, users will be able to see which LEGO^{TM} parts relate to the actors imported into the ANM. In this way, an evidence trail is left, and importantly, the linkage is preserved between treatments that are developed for the scenario and the perspectives of stakeholders that took part in early explorations of the scenario.

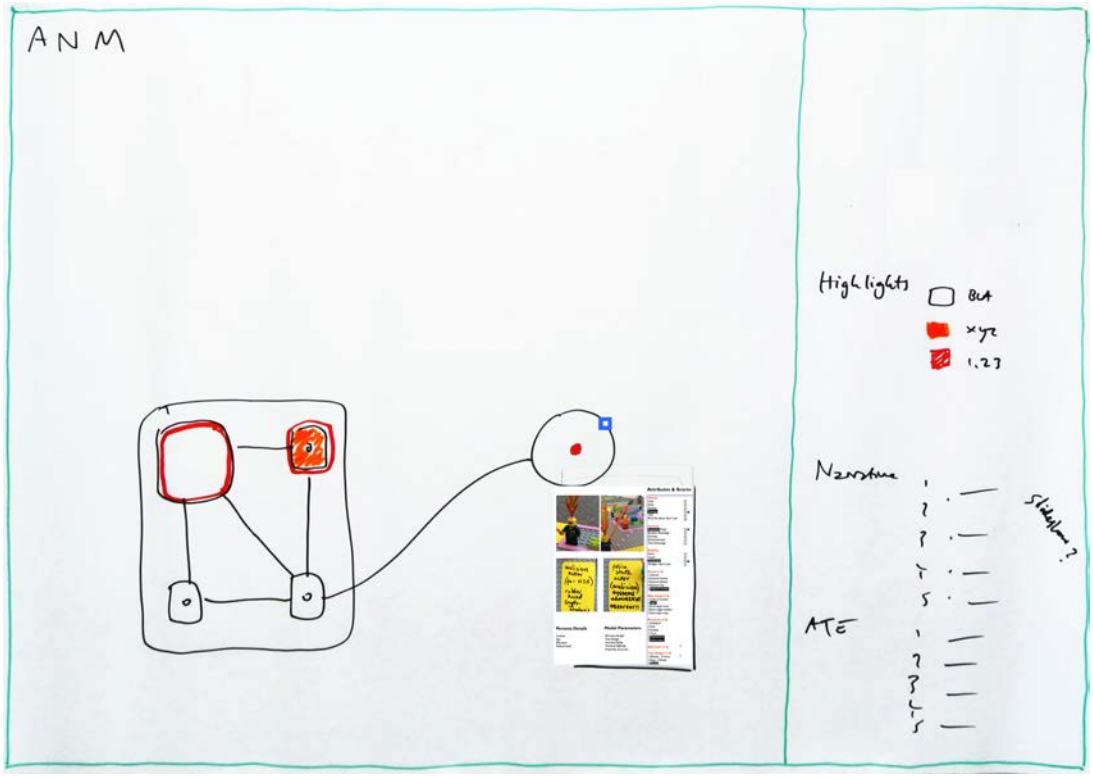


Figure 5.2: *InterActor*: linkage to and from the ANM. A schema for the expert development of the ANM, showing a model with several parts. One part has an indicative small blue square to be clicked upon to reveal the data from *InterActor*. This connects to the prototype where data may be viewed and edited in depth.

5.1.2 Structure of the *InterActor* prototype

InterActor is designed to be a compact, online portal for entry of data from participatory sessions, to be used after and during these sessions, making interactive visualisations available to users so that their data is immediately visible to them.

The prototype is a readily available encapsulation of the manual analytical techniques that have been previously used in TRE$_S$PASS to process this type of data. These techniques were demonstrated and described in previous Deliverables. The digital tool operates in

such a way that the techniques can be applied in depth or with a light touch, depending on the level and amount of data that is encoded with the prototype.

1. **Register and login**. Users first encounter the prototype online with an opportunity to Register (Fig. 5.3) and Login (Fig. 5.4). There is also a short text to introduce and contextualise the prototype within the area of cyber-security.
2. **Project creation area**, where the problem space can be succinctly stated at the outset. This is where the ideation of core organisational values can find expression. It is the arena for defining the core goals, motivations and values of the organisation in question. This can be revisited and redefined at any stage (Fig. 5.5).
3. **Workshop creation area**, here a list of all other workshops can be found, and new ones can be added (Fig. 5.6). Each workshop within this can displayed separately with a list of all the actors and their relationships. Connections between elements in each workshop area can be made by users.
4. **Adding new data** Users can initially view sample data and see the resulting mapping as a working demo. After (or instead of) this they can open the blank *pro forma* template to begin work. There is a standardised range of fields (including numerical data extracted as desired from the physical modelling). These include Name, Class, Scale, Groups, Narrative Fragment, and others. Each item is given a unique ID by the system. The data-entering process includes the possibility of adding new parameters prompted by the specifics of the data-type, in the blank data spreadsheet page (Fig. 5.14).
5. **Scaling and Heatmap**. The actor graph shows thickened connecting lines, derived from values in the data, in this case the number of positive or negative keyword occurrences resulting from discourse analysis of the transcript of our participatory workshops. The data element of Scale determines the size of icons, and, in the case of LEGO™ models, is based upon the physical mass and height of the elements built into the model (Fig. 5.10).
6. **Actors and Actor pages**. Actors are recorded in node/edge (source/target) format. This allows the system to display a force directed graph of connected items (Fig. 5.7). Additionally, by clicking on an actor's node in the map (Fig. 5.12) users can see in a separate window the visual summary of an actor. This may contain detailed attributes of an attacker or defender of a system for example (Fig. 5.13).
7. **Iconography**. Users can select and upload their own photographs of parts of the LEGO™ models, diagrams, and other material to create unique icons for their actors. These are visually scaled on the maps according to how they were modelled in the physical model. This acts as a memory aid and for the continuing discussions of users (Fig. 5.13).
8. **Groups and Classes**. These can be created and populated by the users, from either the spreadsheet view or from the 'Add Actor' and 'Add Relationship' pages of the app (Fig. 5.14).

9. **Edit data**. Users can edit and refine data in the spreadsheet view (Fig. 5.14) as well as in the individual actor and relationships pages.
10. **Query**. Users can query the data and results will appear in a table view (Fig. 5.15).
11. **Protocols for coding of raw data** The 'Help' page gives advice and explanations to new users of the prototype as to how to transcribe data from LEGO™ and other forms of group work. This allows users to begin the process of entering data and of customising this tool to meet their own needs. (Fig. 5.16).
12. **API** Handover constrains and translates the input LEGO™ data to work with the *.xml* format. A set of nodes representing actors and other items from the socio-technical modelling engagement work can be exported to the ANM (Fig. 5.17).
13. **Feedback area** An email will be sent on clicking Feedback, populated with a small number of questions for users to respond to if they wish, as well as adding any other comments:
    - What do you think are the strengths and weaknesses of this prototype?
    - Would you consider using it in your risk assessments, and if so, in what situations, and how?
    - Do you think it could be used in conjunction with any other tools and methods that are available to you in your risk assessment protocols?
    - Finally, Do you have any suggestions about how the prototype could be improved?

5.2 Current state-of-the-art

During our review of the relevant state of the art, no comparable tools to the LEGO™ modelling analogue tool kit and the *InterActor* prototype produced by TRESPASS for visualising socio-technical patterns were found to exist in the security domain. It is, however, possible to identify other tools that are available to the general user, that can be loosely compared in terms of the visualisations that they produce, these include:

- Mind-mapping tools. Browser-based collaborative too 'Mind42', or 'Mindview' which has a limited calculatory function of costs associated with nodes and branches of the map.
- Socio-political patterns; regarding the graphical mapping of actor and organisational relationships (convex hull groupings, and 'marching ants' dashed and dotted arrows). Please see:

  http://www.whodotheyserve.com/#map/gylNwpQO-l/node/g1bOZDnYyx

- Actors and relations; for other examples of force-directed ontology diagrams that utilise sliders for values to be graphed. Please see:

  http://vowl.visualdataweb.org/webvowl/#goodrelations

With these tools in mind the present prototype could be described as an iterative modelling graph that presents collaborative and organising features specifically adapted for the purposes of information security risk assessment analysis. Moreover, the specific features have been designed in consultation with practitioners in such a way to support their information security risk assessment decision-making processes, employing visualisations to do so.

Figure 5.3: *InterActor*: The prototype as it first appears to users.

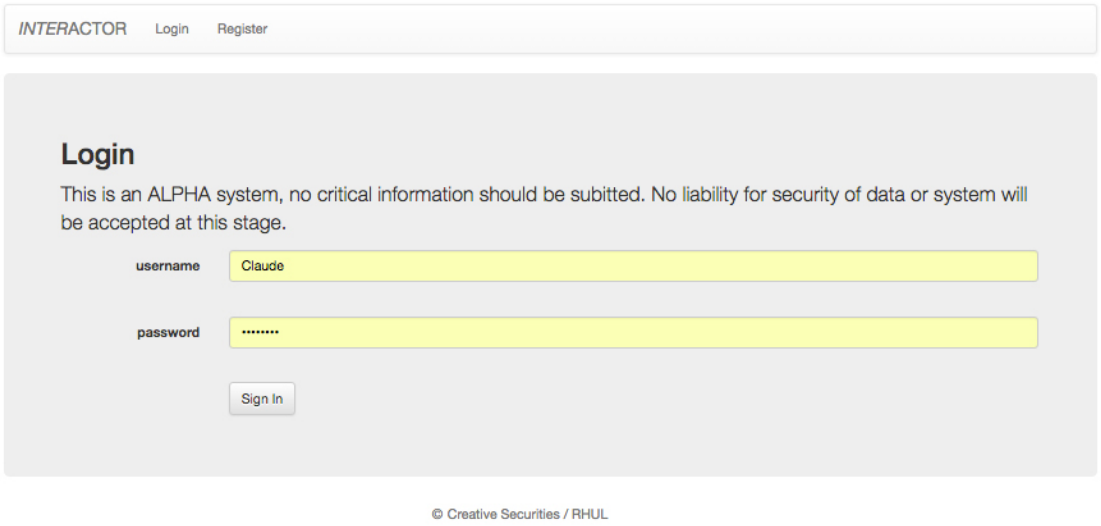


Figure 5.4: *InterActor*: logging in.

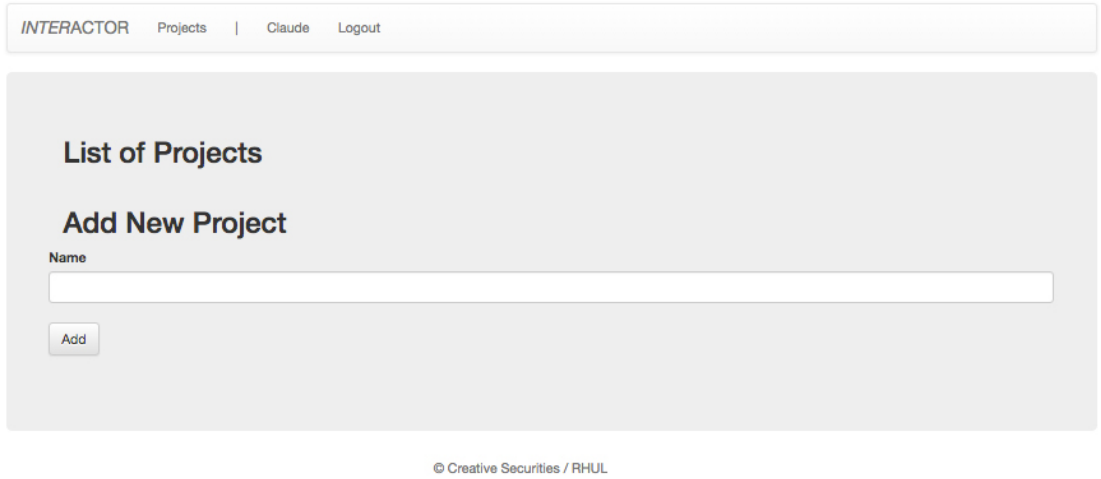


Figure 5.5: *InterActor*: creating a new Project space. After this has been done, users can then create new files for each new workshop as part of this project (see next image).

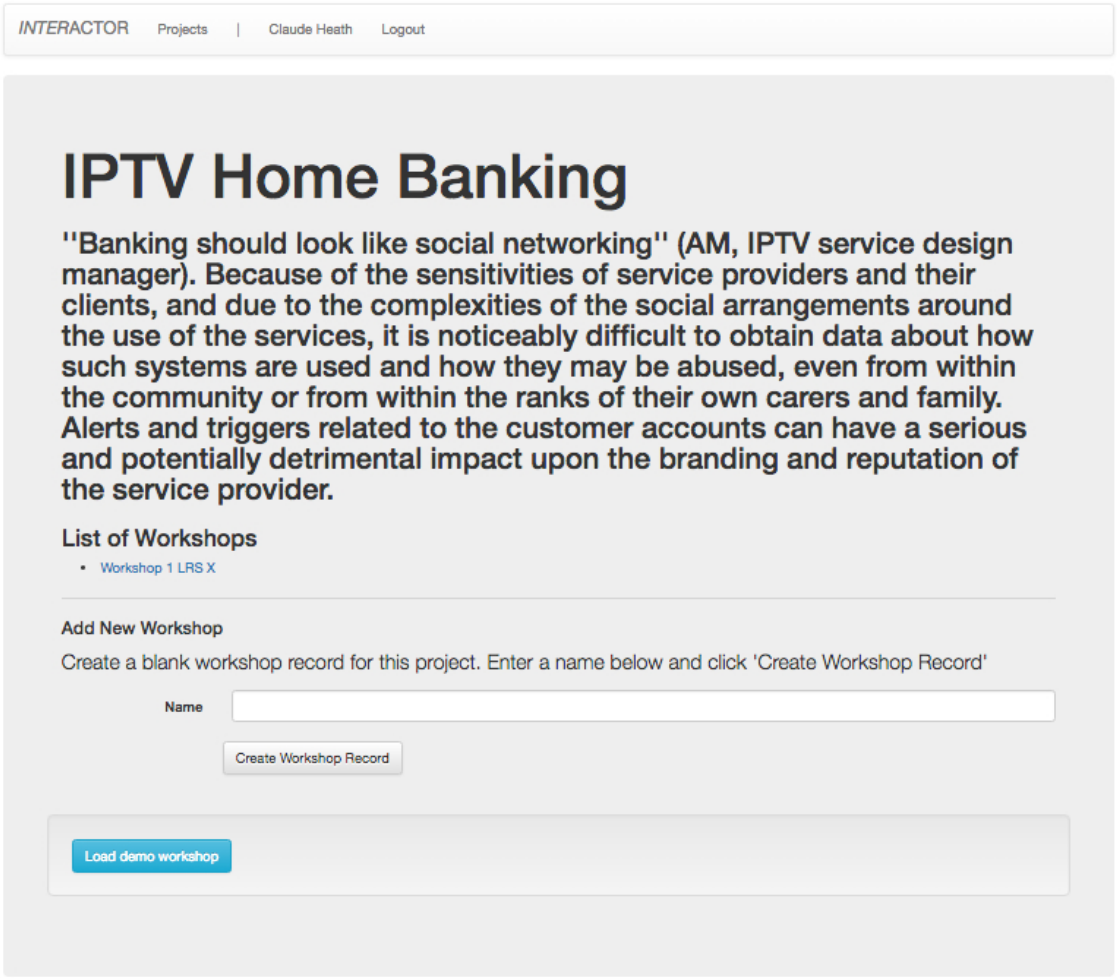


Figure 5.6: The actor-mapping prototype: adding new workshop. The problem definition added by users when first creating the project appears under the title of the workshop. Below, a button 'Load Demo Workshop' is for pre-prepared sample data, allowing users to test the functionality of the prototype, and providing a basis for customising their own approach to its use.

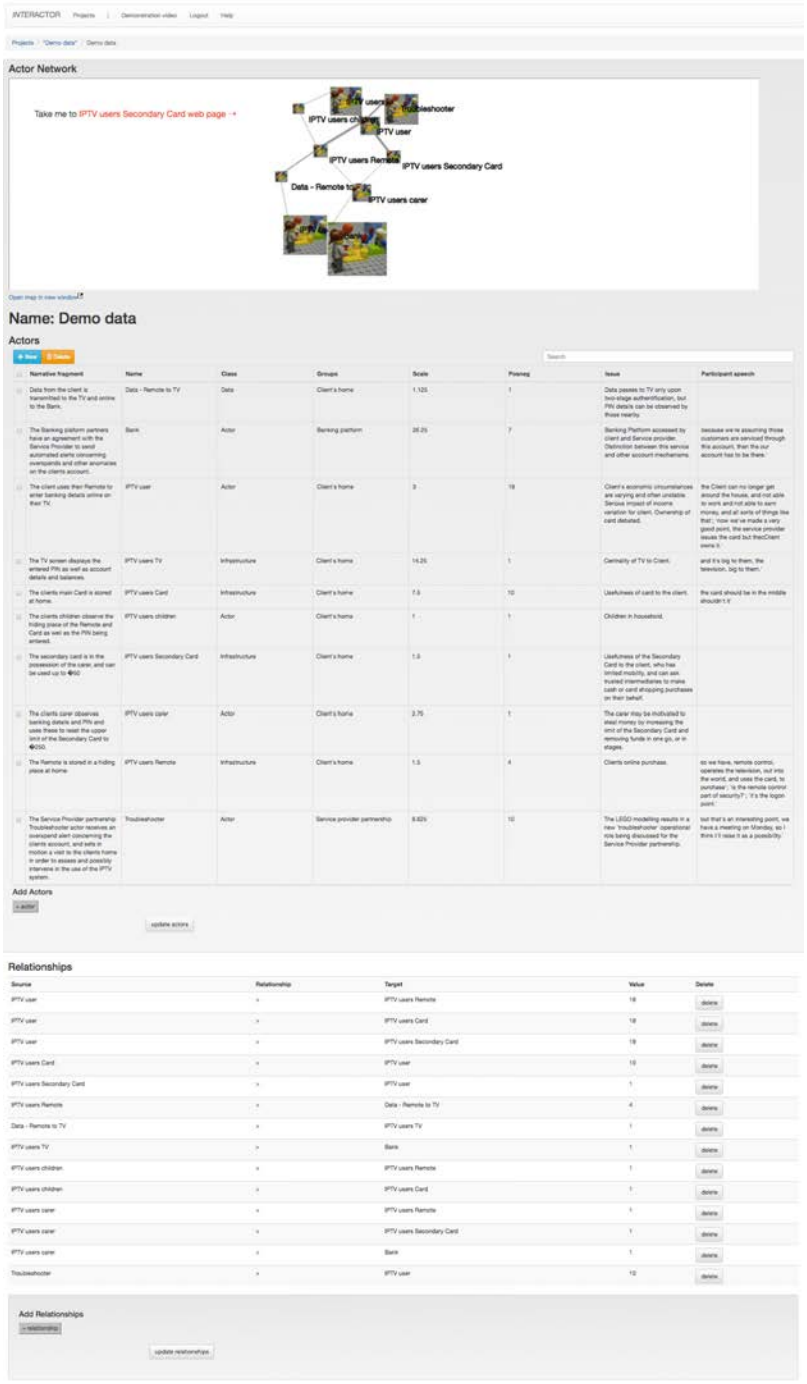


Figure 5.7: *InterActor*: overview of the central page for viewing the map (top), adding and editing actors (middle) and their relationships (bottom). Data is visualised in an interactive network graph which can also be seen in its own window. Note 'Export' button at bottom.

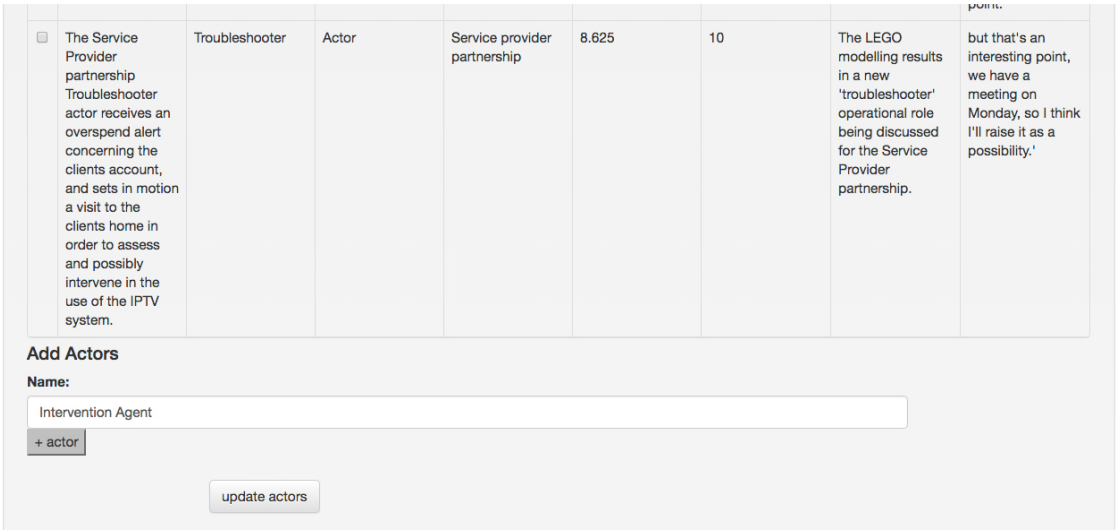


Figure 5.8: *InterActor*: adding an intervention actor, in this case a positively motivated agent who may be despatched to visit the client to forestall a potential misuse of the secondary card, initiating precautions.

Relationships

Source	Relationship	Target	Value
IPTV user	>	IPTV users Remote	18
IPTV user	>	IPTV users Card	18
IPTV user	>	IPTV users Secondary Card	18
IPTV users Card	>	IPTV user	10
IPTV users Secondary Card	>	IPTV user	1
IPTV users Remote	>	Data - Remote to TV	4
Data - Remote to TV	>	IPTV users TV	1
IPTV users TV	>	Bank	1
IPTV users children	>	IPTV users Remote	1
IPTV users children	>	IPTV users Card	1
IPTV users carer	>	IPTV users Remote	1

Figure 5.9: *InterActor*: adding relationships between actors. Here a detail shows actors and the values associated with these relationships, which determines the weight of lines connecting actors on the map.

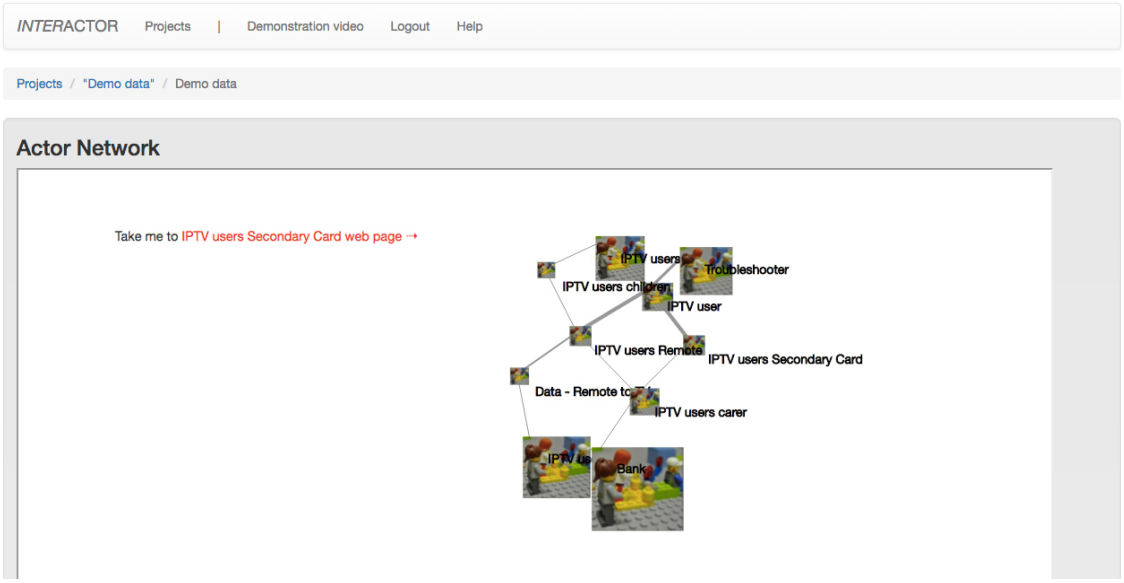


Figure 5.10: *InterActor*: users can see the mapping has weighted lines connecting items which reflect the data they have entered for each actor or item. The graph is interactive and force-directed and can be reconfigured by users.

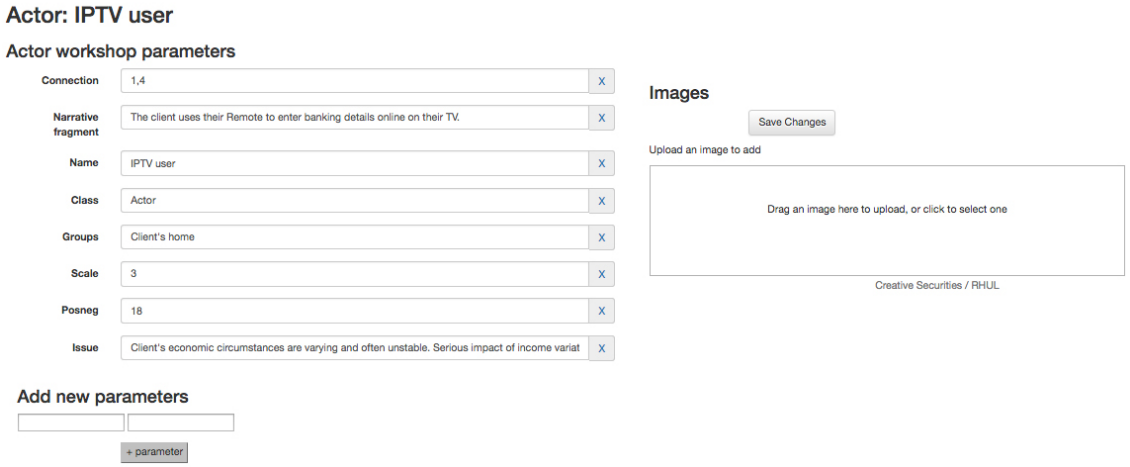


Figure 5.11: *InterActor*: The IPTV client's page, showing detailed information gathered from stakeholders, about the attributes of the client, their possible behaviours and vulnerabilities, as well as their existing support structures and networks.

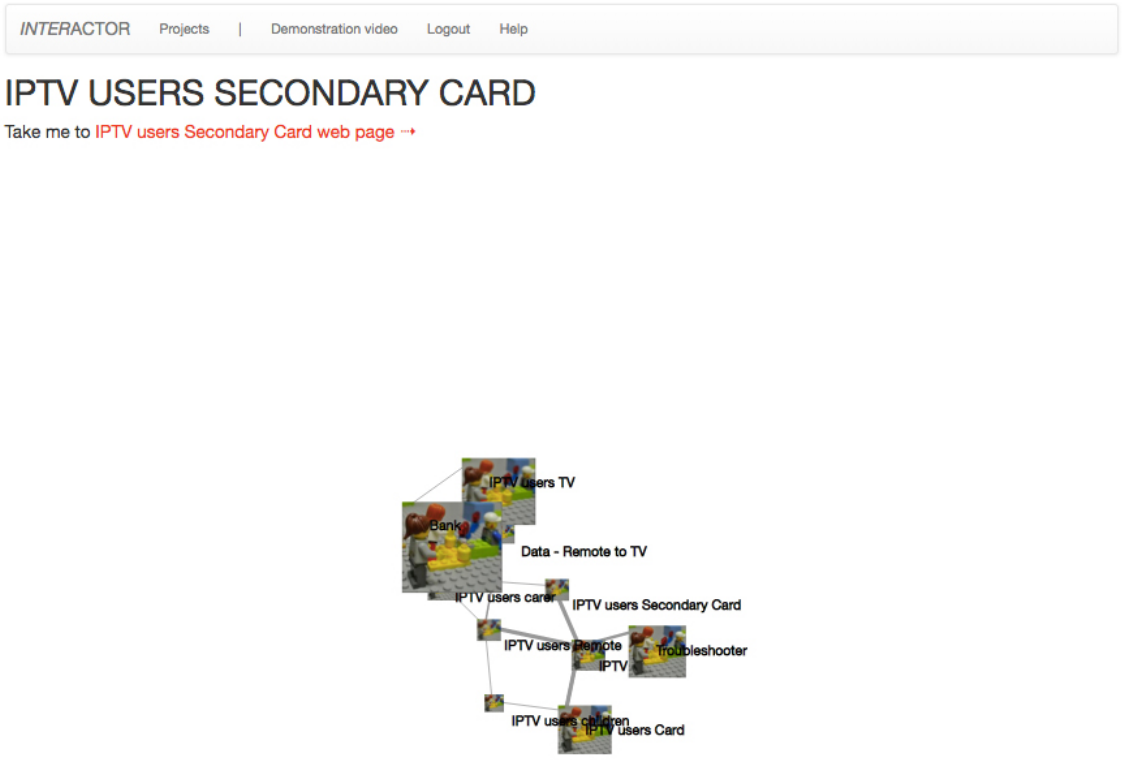


Figure 5.12: *InterActor*: from the general actor map, users can click on an actor's node to investigate the narrative further, for additional information about a potentially vulnerable secondary payment card that is stored on the client's premises.

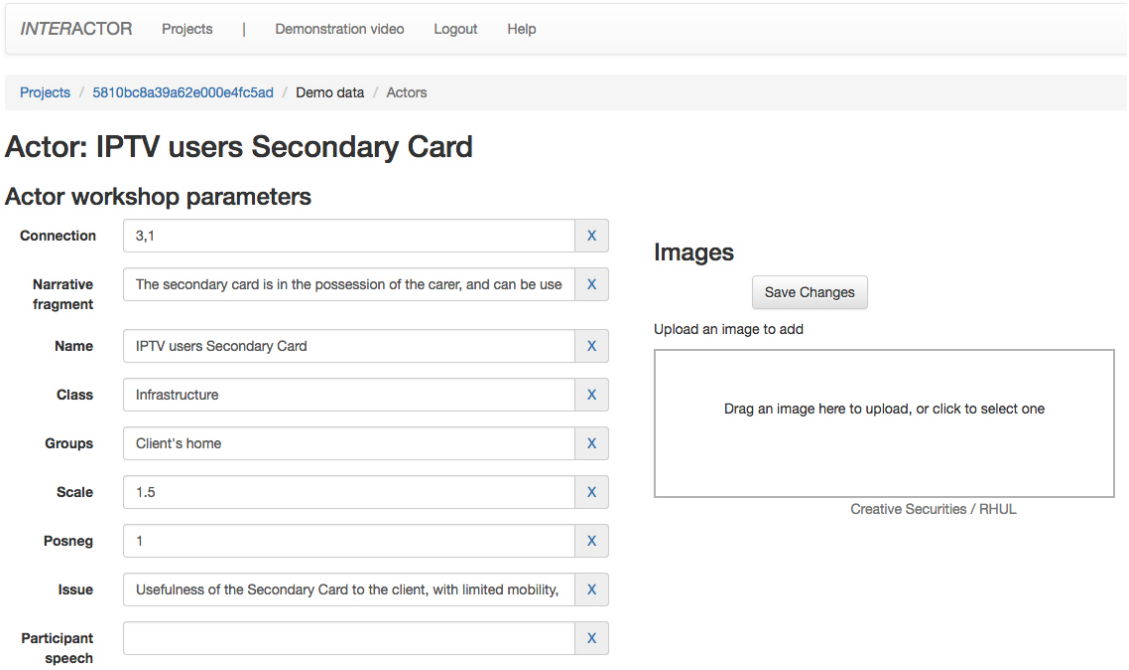
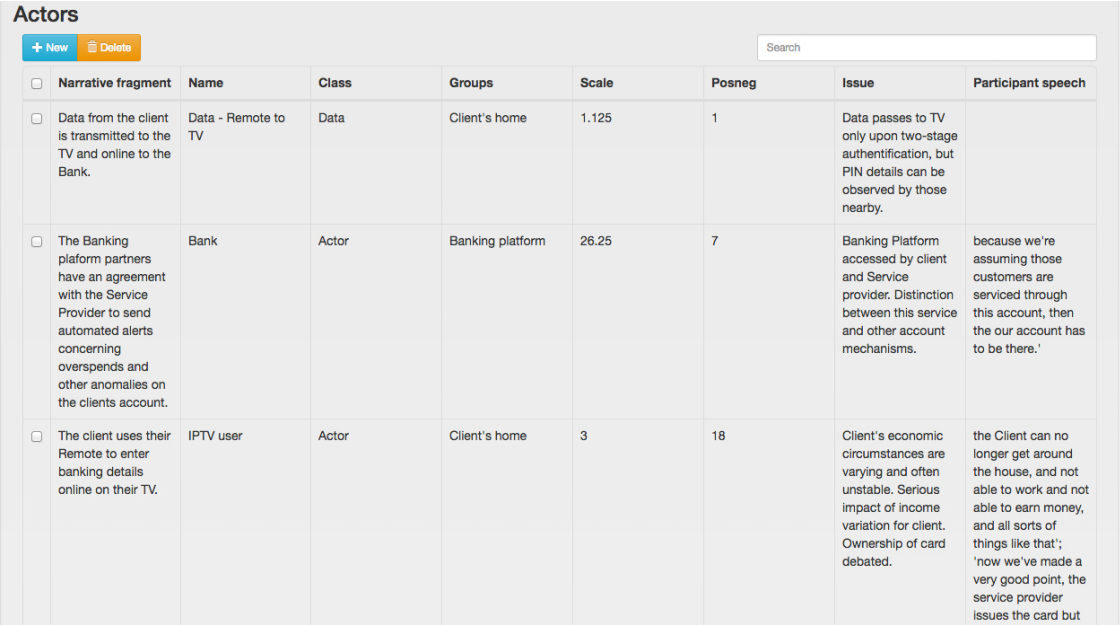
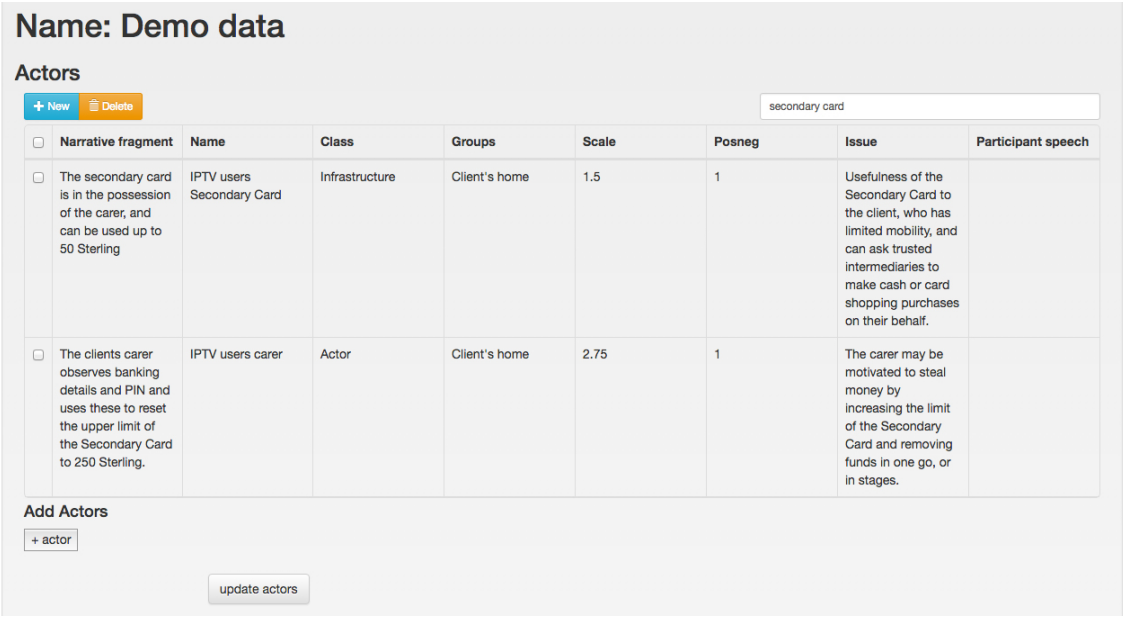


Figure 5.13: *InterActor*: from the general actor map, users can click on an actor's node and call up additional information about that actor, here revealing that the secondary card is in the possession of a carer. At this point it is also possible to upload an image of the actor to be used as an icon for it, and there can be as many of these uploaded images as desired, forming a bank of images and data.



Narrative fragment	Name	Class	Groups	Scale	Posneg	Issue	Participant speech
Data from the client is transmitted to the TV and online to the Bank.	Data - Remote to TV	Data	Client's home	1.125	1	Data passes to TV only upon two-stage authentification, but PIN details can be observed by those nearby.	
The Banking plaform partners have an agreement with the Service Provider to send automated alerts concerning overspends and other anomalies on the clients account.	Bank	Actor	Banking platform	26.25	7	Banking Platform accessed by client and Service provider. Distinction between this service and other account mechanisms.	because we're assuming those customers are serviced through this account, then the our account has to be there.'
The client uses their Remote to enter banking details online on their TV.	IPTV user	Actor	Client's home	3	18	Client's economic circumstances are varying and often unstable. Serious impact of income variation for client. Ownership of card debated.	the Client can no longer get around the house, and not able to work and not able to earn money, and all sorts of things like that'; 'now we've made a very good point, the service provider issues the card but

Figure 5.14: *InterActor*: the spreadsheet view of the data , including add actor and update options and search at top of sheet (out of view). Users can edit cells and select and add new rows to create their own sheets.



Narrative fragment	Name	Class	Groups	Scale	Posneg	Issue	Participant speech
The secondary card is in the possession of the carer, and can be used up to 50 Sterling	IPTV users Secondary Card	Infrastructure	Client's home	1.5	1	Usefulness of the Secondary Card to the client, who has limited mobility, and can ask trusted intermediaries to make cash or card shopping purchases on their behalf.	
The clients carer observes banking details and PIN and uses these to reset the upper limit of the Secondary Card to 250 Sterling.	IPTV users carer	Actor	Client's home	2.75	1	The carer may be motivated to steal money by increasing the limit of the Secondary Card and removing funds in one go, or in stages.	

Figure 5.15: *InterActor*: users can search the data spreadsheet and the page will display the results. The results for a search on the 'Secondary Card' are shown here.

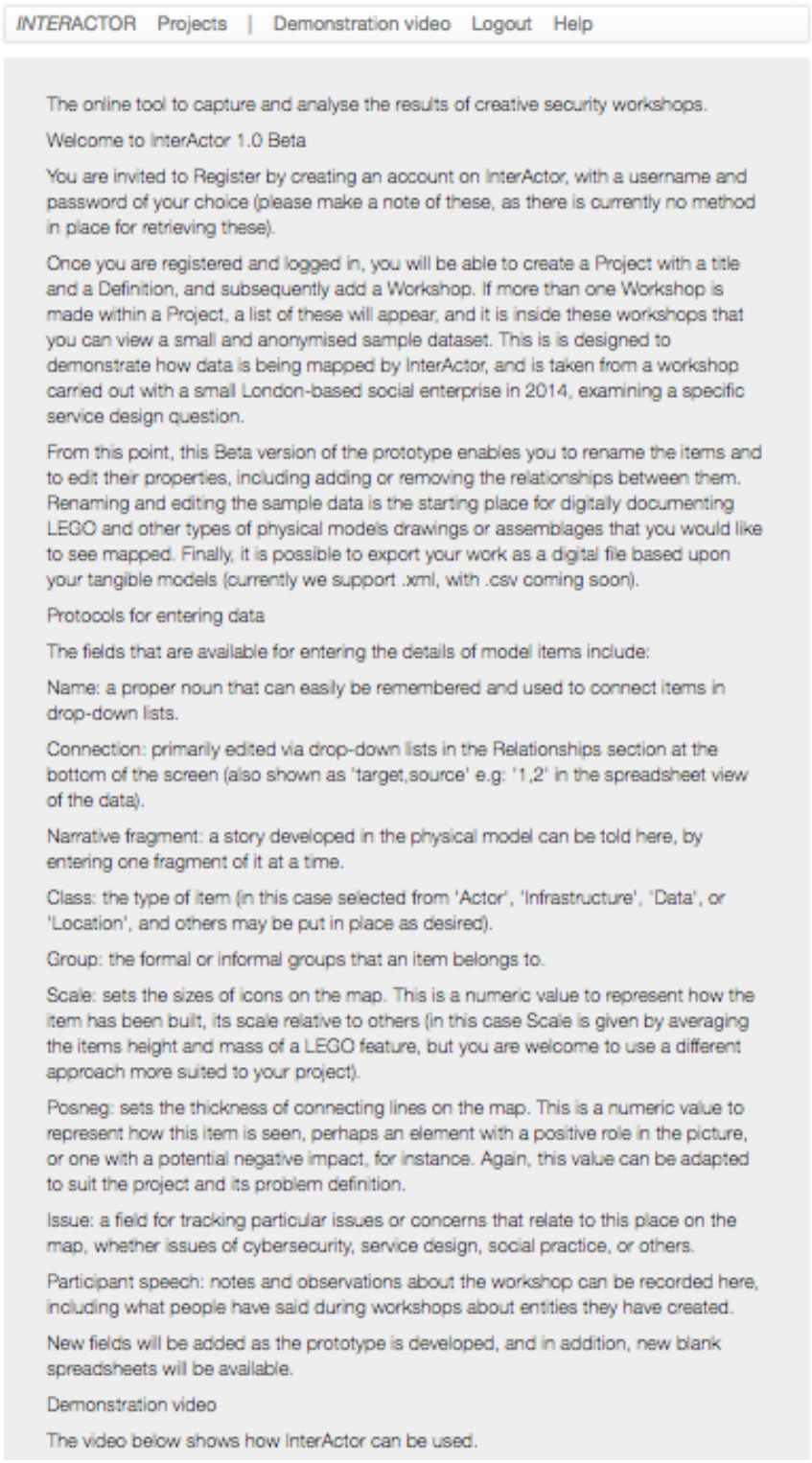


Figure 5.16: *InterActor*: the Help page on *InterActor* includes tips and protocols for entering data, and a demonstration video of the prototype in action.

```
▼<system xmlns="https://www.trespass-project.eu/schemas/TREsPASS_model"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="https://www.trespass-
 project.eu/schemas/TREsPASS_model https://www.trespass-
 project.eu/schemas/TREsPASS_model.xsd" author="INTERActor"
 version="0.0.0" date="2016-06-14 10:17:42" id="id-BkZ-hlL8Gx-model">
   <title>Clients home IPTV</title>
  ▼<actors>
    ▼<actor id="actor__IPTV user" type="tkb:actor" name="IPTV user"
     interactor_id="58075305dc137b000ec30e6d">
       <atLocations/>
     </actor>
    ▼<actor id="actor__IPTV users Card" type="tkb:actor" name="IPTV
     users Card" interactor_id="58075305dc137b000ec30e6e">
       <atLocations/>
     </actor>
    ▼<actor id="actor__IPTV users Secondary Card" type="tkb:actor"
     name="IPTV users Secondary Card"
     interactor_id="58075305dc137b000ec30e6f">
       <atLocations/>
     </actor>
    ▼<actor id="actor__IPTV users Remote" type="tkb:actor" name="IPTV
     users Remote" interactor_id="58075305dc137b000ec30e70">
       <atLocations/>
     </actor>
    ▼<actor id="actor__Data - Remote to TV" type="tkb:actor" name="Data
     - Remote to TV" interactor_id="58075305dc137b000ec30e71">
       <atLocations/>
     </actor>
    ▼<actor id="actor__IPTV users TV" type="tkb:actor" name="IPTV users
     TV" interactor_id="58075305dc137b000ec30e72">
       <atLocations/>
     </actor>
    ▼<actor id="actor__IPTV users children" type="tkb:actor" name="IPTV
     users children" interactor_id="58075305dc137b000ec30e73">
       <atLocations/>
     </actor>
```

Figure 5.17: *InterActor*: the exported .xml file from *InterActor*.

6 Evaluation

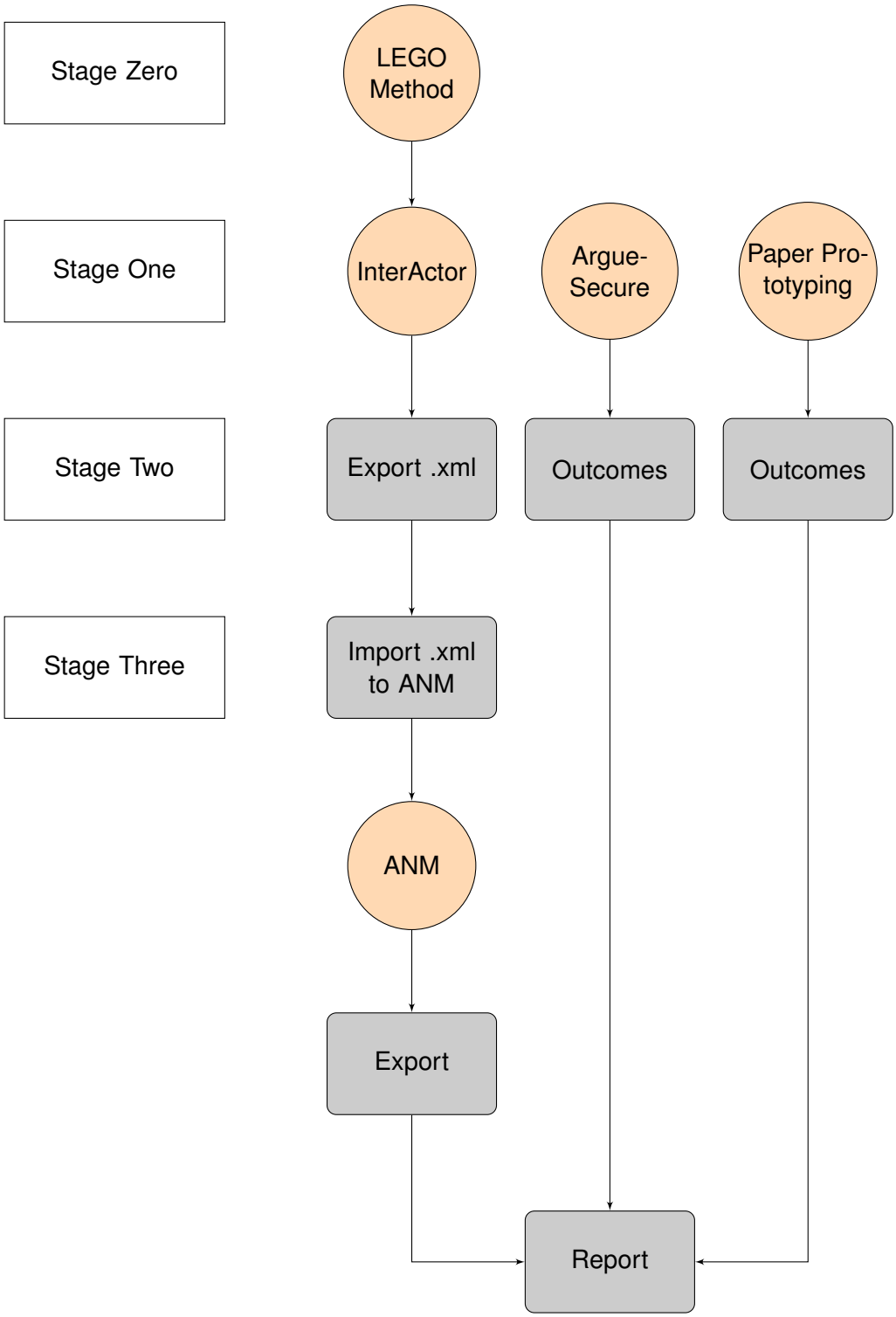
Over the course of the project we have gathered feedback from our engagement programme with security practitioners, designers and other stakeholders who seek a clearer understanding of information security risk in their domain. The many different types of engagement that we have run have ranged from 'stage zero' scoping of cybersecurity issues, to those working with specific issues to do with banking and financial markets, service design, and employee monitoring in the workplace. The move from 'stage zero' to higher levels of problem scoping and treatment is seen in the following diagram, showing a palette of tools produced by TRE$_S$PASS for extracting, managing, and visualising social data.

The forms of social data that we derive are of the following kinds:

- Scoping of issues.
- First models of scenarios.
- Organisational/individual relationships and skills.
- Multiple stakeholder perspectives.
- Tacit knowledge of participants.
- Management of issues relating to the above.

6.1 Stages 0-3 of the TRE$_S$PASS risk assessment process.

This diagram shows a number of paths that users can take, using TRE$_S$PASS tools and methods, towards completing a risk assessment. The progression is from initial scoping and problem statement, towards a more refined view of the problem space. As the typical user moves through these tools, increasing levels of detail are dealt with and visualisations become more informative.



Our evaluation approach was structured in two stages. In the first stage we identified which social data should be collected and how this should be done in a series of feedback sessions with relevant stakeholders. Typical feedback is documented in the section

below. From this feedback, the InterActor prototype was developed. In the second stage, the prototype was evaluated against typical user journeys constructed from the feedback sessions.

6.2 Feedback on social data methods from practitioners and designers

Below is a sample of typical practitioner feedback on the physical modelling process with LEGO™. This feedback also provides an insight into how and why the *InterActor* prototype was conceived. The core purpose of the *InterActor* prototype is to meet the need described in the feedback for translating the insights produced by physical and other forms of modelling and brainstorming into a format that can be read and processed by other tools ordinarily being used by practitioners.

As the feedback shows, the *InterActor* prototype must include features that:

- Encourage interaction and the sharing of perspectives between disparate stakeholder groups;
- Communicate virtual and abstract concepts;
- Present the social landscape for technical responses to security risks;
- Show the strengths of social relationships and communities of practice;and
- Preserve the speed with which collaborative physical models of risk scenarios can be built.

Q. What are the strengths of the method?

> 'Communication of virtual concepts. Highlighting gaps in understanding, and differences in perception.' - Practitioner.

Q. Would you use this method in your risk assessments, if so, how?

> 'Yes. Explanation of virtual concepts to those with no understanding of terminology. Creating a communication interface between interdependent teams with no established working relationship.' - Practitioner.

IASDR 2015 workshop (International Association of Societies of Design Research), Brisbane, Australia.

> 'I had a hundred new thoughts, to do with considering different personas and perspectives, and adapting designs according to the problem.' – Practitioner.
>
> 'This method is better than block diagrams for enabling users to better frame their own solutions, and getting new ideas on how to show comparative solutions and how they work. Everybody needs to understand a security model at an intuitive level.' - Practitioner.

> 'If you show me this model, I'm more likely to understand the technical implications.' – Designer.

Sunderland City Council. Direct Payments workshop, 2016:

Q. What kind of support do people need, and how can we offer this support?

> 'We talked about things that our community champions are going to need in this new world-order, to be able to support vulnerable people.'– Participant.
>
> 'The client household moved into the centre of the model after first of all having it at the edge.' – Public sector digital innovation manager.

CyberUK 2016, Masterclass 4, Liverpool, UK. Modelling the terrain: cybersecurity risk and LEGO™.

> 'Visualises data flows, risks including users, devices, suppliers, environment, and so on.' - Practitioner.
>
> 'Great way to show an alternative perspective.' - Practitioner.
>
> 'The method could be used in conjunction with threat modelling.'
>
> 'Good for user training in information risk management, for example IAO's and IAA's.' - Practitioner.

Royal Holloway, Information Security Group, Cyber Risk Summer School 2016.

> Brainstorming sessions with LEGO is a faster method than collecting individual feedback using risk assessment questionnaires. It substantially decreases the likelihood of misunderstandings between different individuals or groups: where variances in use of terminology can complicate discussions unnecessarily, a solid model can provide a greater degree of certainty for all parties. – Summary of practitioner feedback.

Royal Holloway, Information Security Group, Cyber Risk Summer School 2016.

> Collaborative modelling and discussion as well as a level of automated analysis of the resulting model can complement each other. Iterative refinement of the risk analysis in this way, allows us to progress from a 'static' risk analysis to a 'dynamic' view of the system and its risk posture. – Summary of practitioner feedback.

6.3 User Journeys

A user journey is a clear model of how users interact with a service or technology and a definition of what motivates them. In the context of TRE$_S$PASS this must include an understanding of how the ANM and other tools can help them to achieve their business goals. The deployment of user journeys as part of the evaluation process allows the developers of tools and processes to assess the success of those tools in their proper context, since this would always be measured with reference to the goals of a user. In the context of TRE$_S$PASS, for a user journey to be successfully defined, a security practitioner would need to be both able and willing to undertake a 'user journey' through the tools, applying their own skills and aptitudes to attain their goals through using the tools.

In this way, the motivations and goals of practitioners should be fed into the design process that leads to the production of the tools. This has become standard and best practice in design. Specifically, what 'pain points' are addressed at each stage of the journey, and how? Other points along these journeys can be defined by the following questions, which can be used selectively depending on the use-case in question, for example:

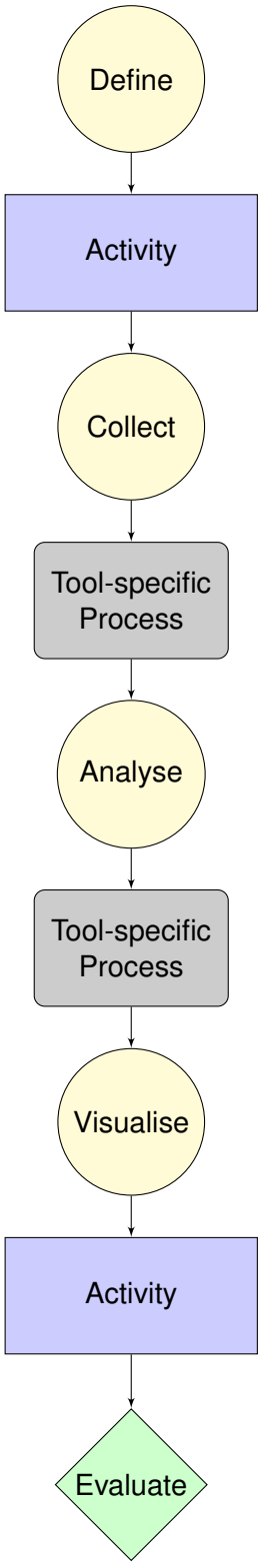
Context: Where are the users? What is around them? What distracts them?

Progression: How does each step enable them to get to the next?

Devices: What device are they using? Are they a novice or expert? What features does the device have?

Functionality: What type of functionality are they expecting? Is it achievable?

The diagram below presents a template of a user journey illustrates the journey elements and the flow between them. In the following subsections we outline the user journeys that take users from LEGO^{TM} modelling in a Stage Zero activity to developing a new risk map in the ANM. The examples we use below are based on the IPTV scenario.


Define
Activity
Collect
Tool-specific Process
Analyse
Tool-specific Process
Visualise
Activity
Evaluate

Key to User Journey Flowcharts

6.4 User Journey: Use the LEGO™ methodology to scope a problem

Use Case and Task Use-case: Consultant wishes to scope the IPTV scenario before a more detailed risk analysis, and to extract initial insight about how to model the scenario, including any relevant tacit or previously un-shared knowledge that stakeholders may possess about the scenario.

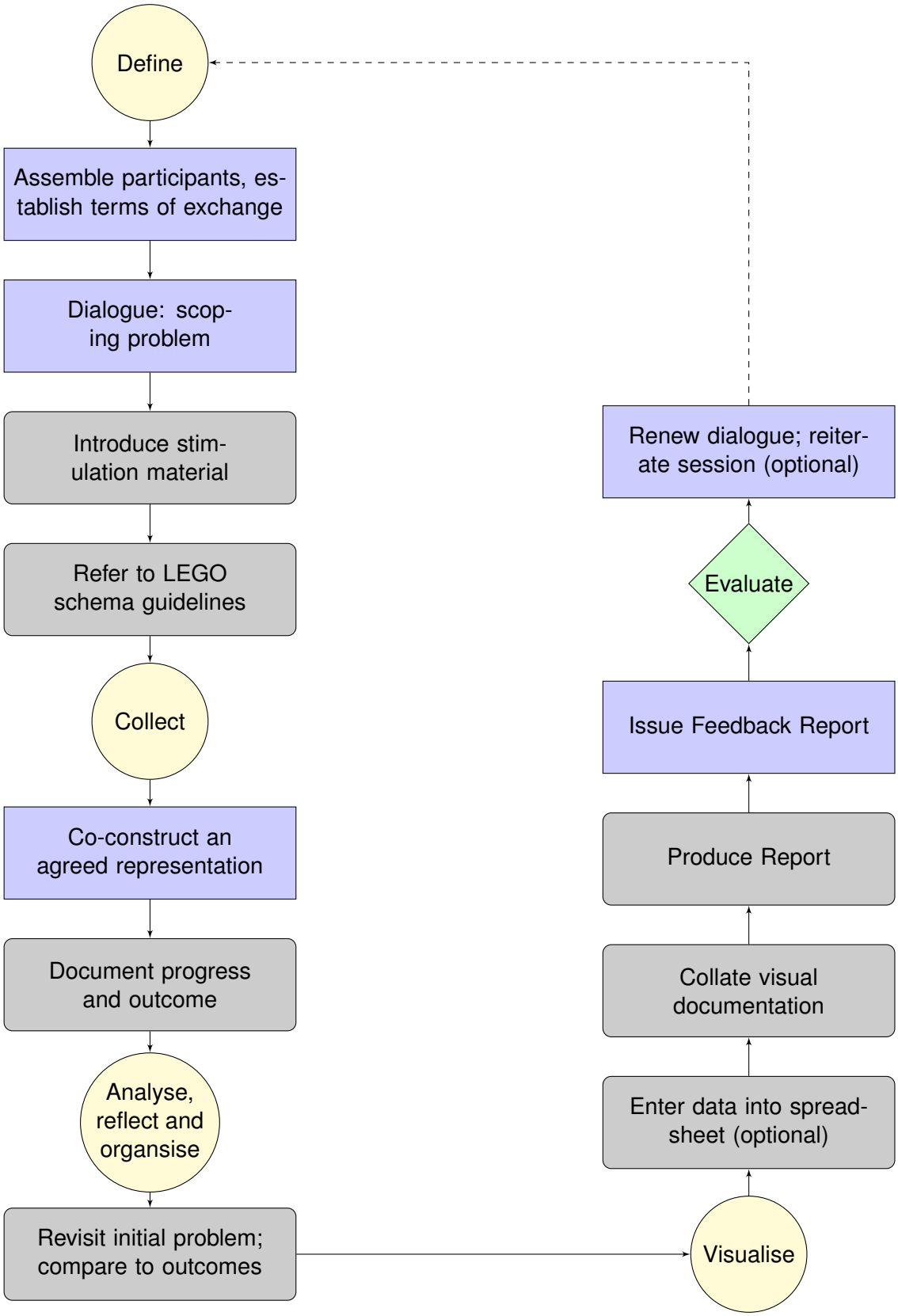
Task: Assemble participants and introduce the way in which the exchange will be managed. Provide stimulus materials and begin by asking participants to frame their starting question. Commence to jointly build the scenario using the LEGO™ kit and the guidelines provided with the kit. Document the results during and after the session. Re-examine the starting questions at the end of the session, and include this and the visual documentation in a rapid feedback report which can later be followed up if another iteration of modelling is required or requested.

User testing	Participants	Feedback and outcomes
SME, London	7	2 LEGO sessions, feedback provided to SME
Miscellaneous venues	174	LEGO sessions (See Appendix B, D4.2.2 for details and full list of engagements)

Testimonial

> "I just wanted to thank you for the excellent session you ran for us this morning; very complex and in depth but incredibly useful! Mapping out where we are, where we want to go, how we'll get there - clarifies all sorts of things....
>
> It is very unusual for me to be able to sit and do something like that, because everything is up here [points to head], so it's very healthy for us, I definitely think we should get our own LEGO kit, and everything is captured in 3D."

NK, CEO, participant, London 2014. (See Fig. 6.1).


Define
Assemble participants, establish terms of exchange
Dialogue: scoping problem
Introduce stimulation material
Refer to LEGO schema guidelines
Collect
Co-construct an agreed representation
Document progress and outcome
Analyse, reflect and organsise
Revisit initial problem; compare to outcomes
Visualise
Enter data into spreadsheet (optional)
Collate visual documentation
Produce Report
Issue Feedback Report
Evaluate
Renew dialogue; reiterate session (optional)

Sample evaluation output 7 SME participants modelled their IPTV home-banking service, as part of the TRESPASS case study (Fig. 6.1).

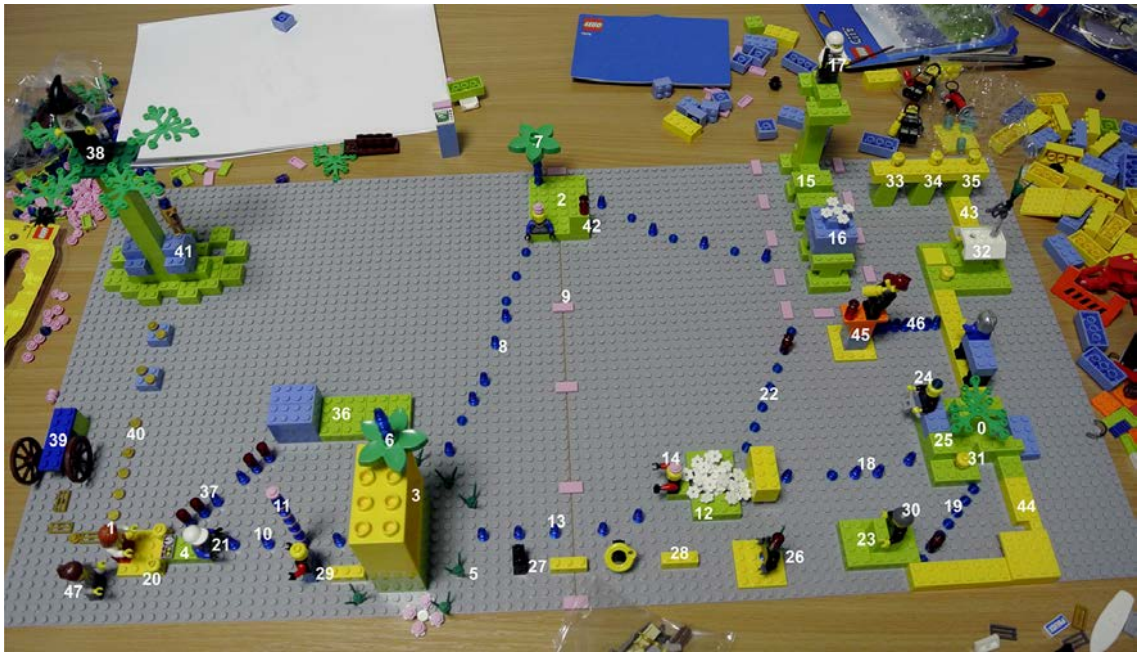


Figure 6.1: The first iteration of the LEGO model of the IPTV home-banking service design concept, London, 2014.

6.5 User Journey: *InterActor*

Task Use-case: Consultant performs a risk analysis of the IPTV scenario following on from the initial LEGO^{TM} session with stakeholders. They are examining the data from this session using the *InterActor* prototype, specifically at where social interactions and practices identified during the session may impact on a subsequent risk analysis of IPTV, carried out with the aid of the ANM.

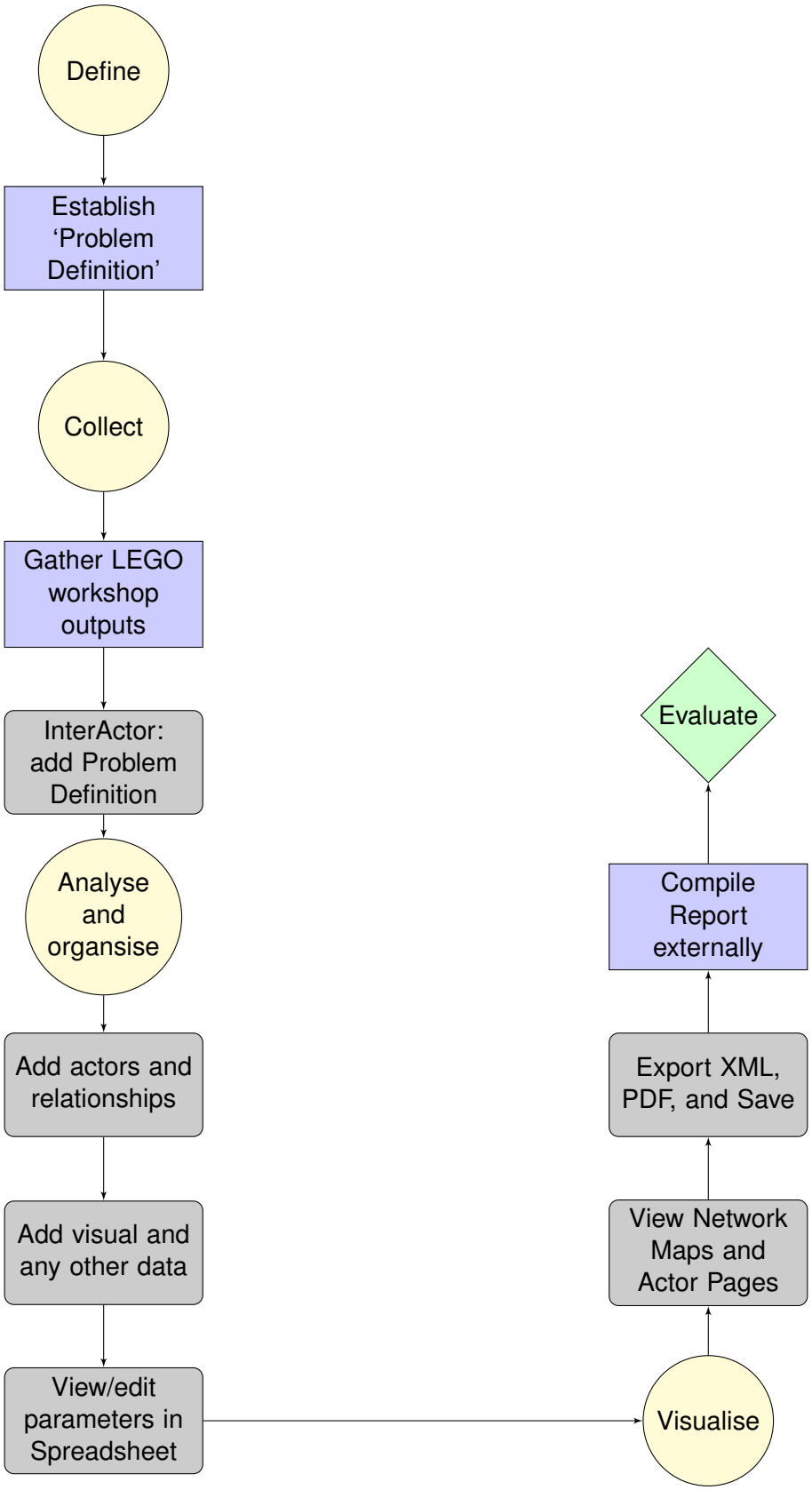
Task: use the prototype to transcribe data from the LEGO^{TM} models (for another form of input). First, frame your work with a statement of the problem space (which can be revised at a later point if necessary). Go on to create actors and add their relationships to each other. Add any narrative fragments that link two or more actors. These should be significant to the social aspects of the IPTV scenario. Compile the actor network, add photographic and other information to actors and export as a PDF to share with colleagues.

User testing	**Date**	**Participants**	**Feedback and outcomes**
RHUL, study group	July-Sept 2016	4, in 2 sessions	App testing, written and verbal feedback.
RHUL, advisory panel	July-Sept 2016	3, in 2 sessions	Scoping of tool, development suggestions, and qualitative feedback (See Appendix B, D.4.2.2 for further details).

Testimonial

> "I was very impressed with the progress that has been made. I think there is much more of a tangible asset here now which can be related to industry applications. One area of interest to me was the use of the tool as an exploratory/diagnostic device that helps us to understand the organisation and the moving parts that comprise it. Going into the process 'eyes open' as opposed to looking for an answer to a question, this more creative relaxed approach would work well in terms of leveraging all of the information produced by the work carried out in the prototype. Secondly, the potential to provide different perspectives on the same relationships/interconnections would be very useful in terms of nurturing better relationships and potentially highlighting critically weak relationships which could constitute risk if they break down or are targeted by malicious actors. Very much looking forward to seeing how the project progresses as the potential seems vast."

Sean Kearney, Information Security Consultant, Deutsche Bank, London. October 2016.


Define
Establish 'Problem Definition'
Collect
Gather LEGO workshop outputs
InterActor: add Problem Definition
Analyse and organsise
Add actors and relationships
Add visual and any other data
View/edit parameters in Spreadsheet
Visualise
View Network Maps and Actor Pages
Export XML, PDF, and Save
Compile Report externally
Evaluate

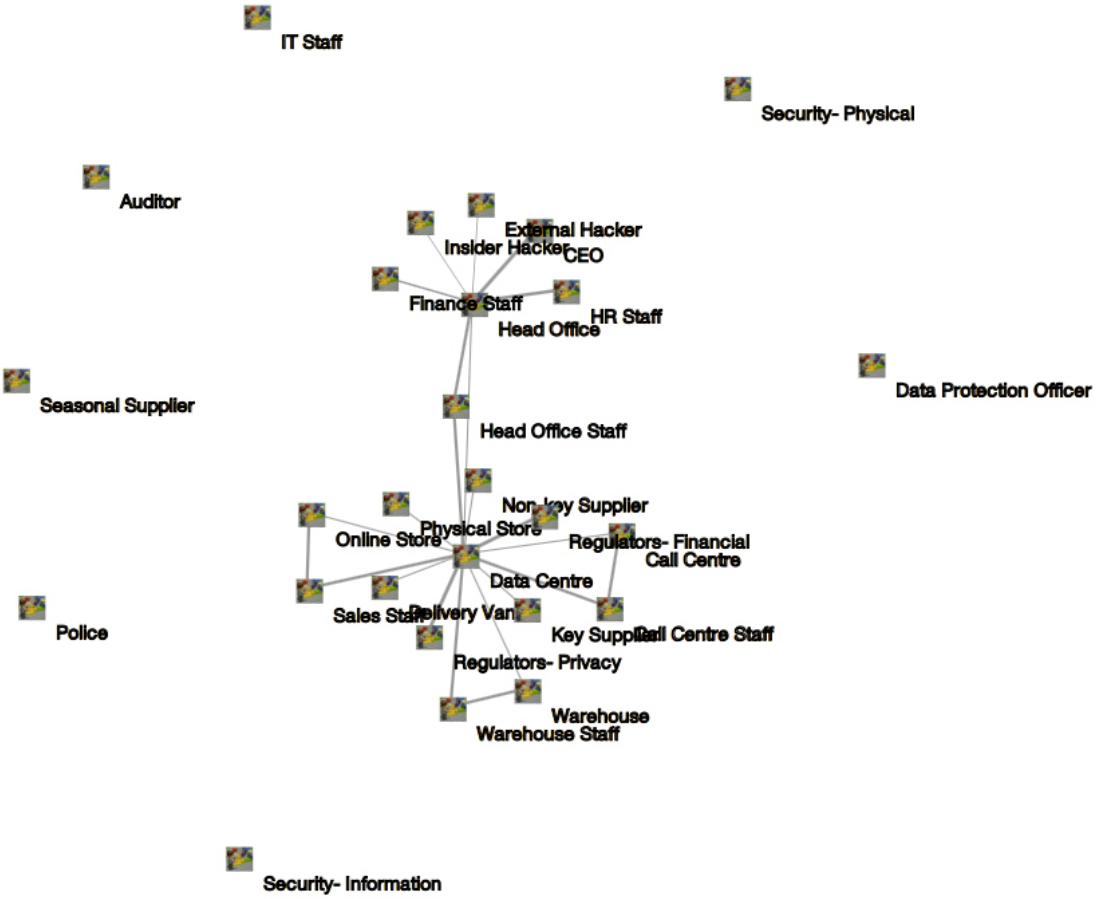


Figure 6.2: The participants used the current data template in *InterActor* to transcribe the physical model of the 'Acme' retail environment.

Sample evaluation output

6.6 User Journey: *InterActor* to ANM

Task Use-case: Consultant performs a risk analysis of the IPTV scenario following on from the initial LEGO™ session with stakeholders. They are examining the data from this session using the *InterActor* prototype, specifically where social interactions and practices identified during the session may impact on a subsequent risk analysis of IPTV, carried out with the aid of the ANM.

Task: use the prototype to transcribe data from the LEGO™ models (for another form of input). First, frame your work with a statement of the problem space (which can be revised at a later point if necessary). Go on to create actors and add their relationships to each other. Add any narrative fragments that link two or more actors. These should be significant to the social aspects of the IPTV scenario. Compile the actor network, add photographic and other information to actors and export as a PDF to share with colleagues. Also export an XML file of the actors and import these in the ANM. Once there, build a more complete model around these actors and view attack trees that results. Lastly, edit parameters in the model before making a second tree to compare to the initial one. The result of your analyses in the ANM can then be compared to the starting Problem definition created in *InterActor*.

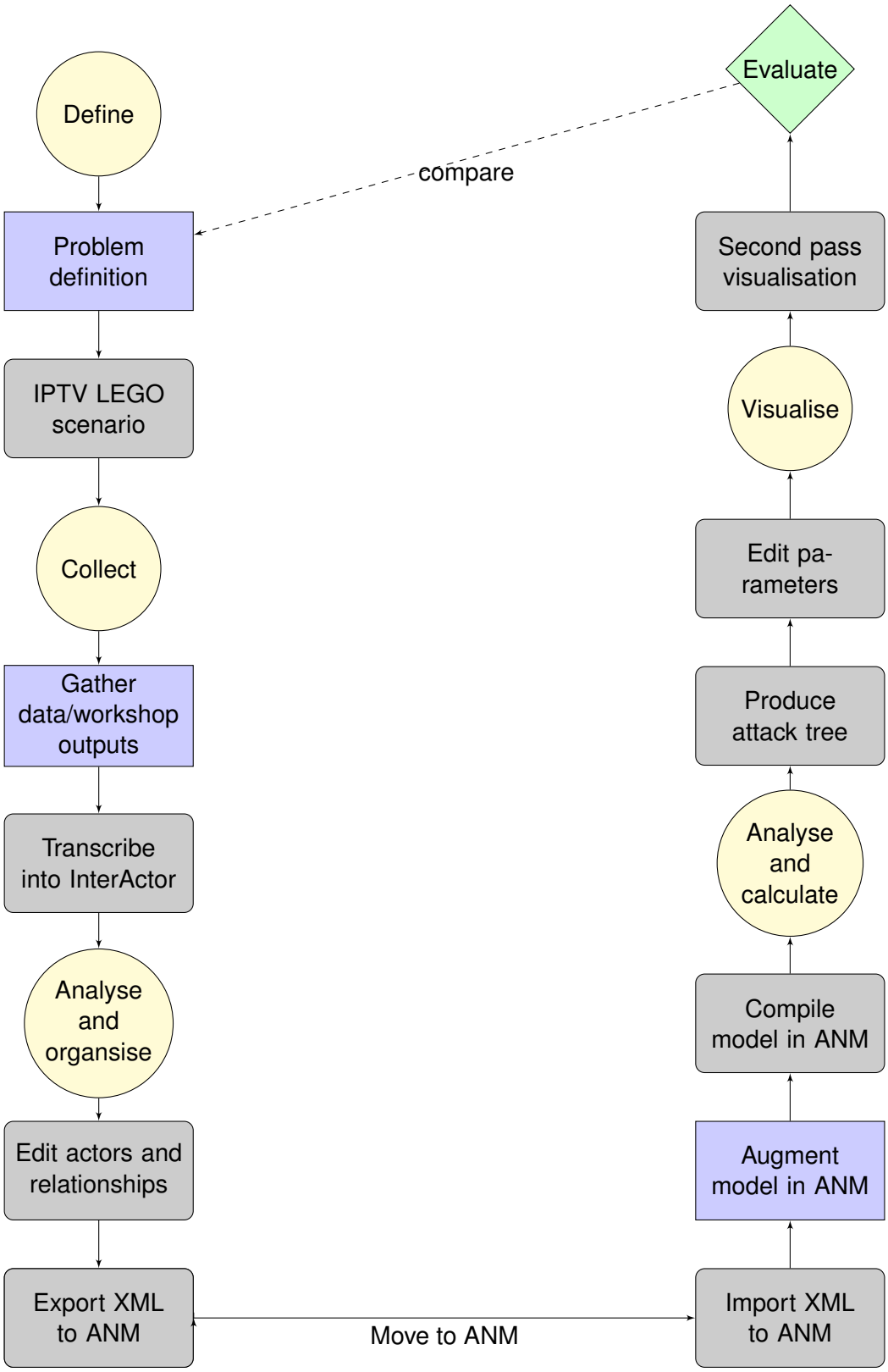
User testing	**Date**	**Participants**	**Feedback and outcomes**
RHUL, study group	July-Sept 2016	4, in 2 sessions	prototype testing, written and verbal feedback.
RHUL, advisory panel	July-Sept 2016	3, in 2 sessions	Scoping of tool, development suggestions, and qualitative feedback (See Appendix B, D.4.2.2, for further details).

Testimonial

> "There is serious potential for this TRE$_S$PASS work to bridge the gap between specialist Information Assurance (IA) practitioners and those responsible for the business concerns they are supposed to be protecting. By engaging with those most closely associated with the operation of the business it increases the chances that risks will be better assessed and prioritised.
>
> Furthermore, the visualisations and LEGO™ models can be used to assist in the deeper understanding of the key stakeholder groups. Those with responsibility for the business can gain insight into less obvious attack vectors and the Information Assurance professionals can gain a greater understanding of the business process.

> The prototype can be used to translate from the LEGO™ models into a prioritised risk list. Provided the link between the LEGO™ models developed and the risks identified remains, it is possible to maintain a common understanding across both the Business and Information Assurance teams as activities move into the risk treatment phase.
>
> In referring to the physical model the non-specialist Information Assurance (IA) stakeholders can use this method as their touch-point to understand the risks. My view is that it is important to ensure that the link between the model and the risks are not broken as the computerised model evolves, as this would lead to a misalignment in understanding of the risk between the IA and non-IA stakeholders."

Ian D. McKinnon, UK Public Sector IA Specialist, BSc MSc MBCS CITP M.Inst.ISP SCP CISSP. October 2016.


Define
Problem definition
IPTV LEGO scenario
Collect
Gather data/workshop outputs
Transcribe into InterActor
Analyse and organise
Edit actors and relationships
Export XML to ANM
compare
Move to ANM
Evaluate
Second pass visualisation
Visualise
Edit parameters
Produce attack tree
Analyse and calculate
Compile model in ANM
Augment model in ANM
Import XML to ANM

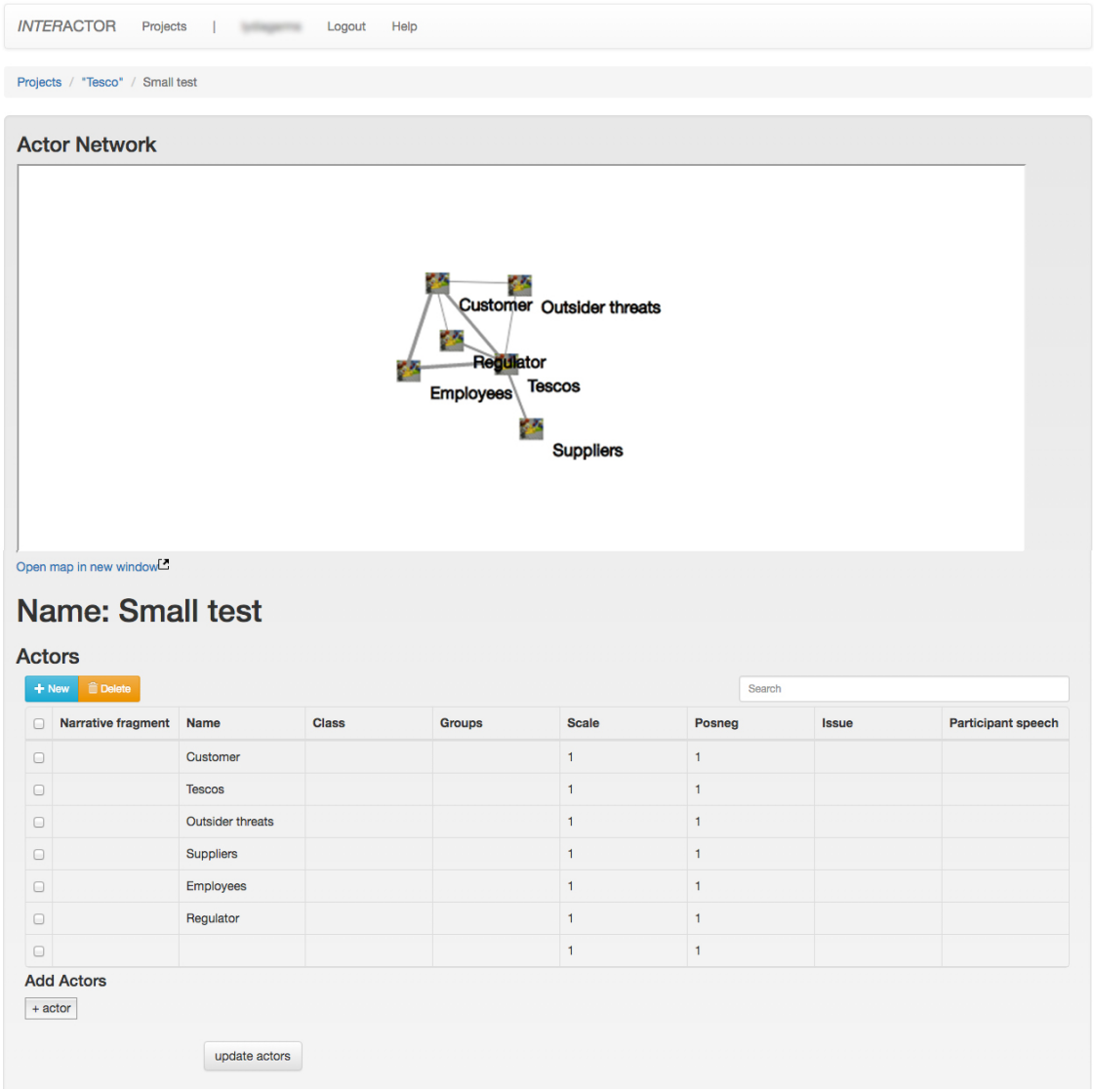


Figure 6.3: .

Sample evaluation output

6.7 Discussion: Seeing the wider picture - the Acme case study

Acme retail scenario Wherever possible in the following discussion of our evaluations, specific instances are given of how our approach will impact an analysis of attack probabilities. We do so not in the sense of the risk calculation that is possible in ANM, although this is also referred to, but also in terms of how this analysis will benefit an a decision process that is part of the larger picture for practitioners. This will be illustrated with quotes

```
<system xmlns="https://www.trespass-project.eu/schemas/TREsPASS_model" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="https://www.trespass-project.eu/schemas/TREsPASS_model https://www.trespass-project.eu/schemas/TREsPASS_model.xsd" author="INTERActor"
version="0.0.0" date="2016-06-14 10:17:42" id="id-BkZ-hlL8Gx-model">
  <title>Small test</title>
  <actors>
    <actor id="actor__Customer" type="tkb:actor" name="Customer" interactor_id="580df62f161983000e75a6c8">
      <atLocations/>
    </actor>
    <actor id="actor__Tescos" type="tkb:actor" name="Tescos" interactor_id="580df660161983000e75a6c9">
      <atLocations/>
    </actor>
    <actor id="actor__Outsider threats" type="tkb:actor" name="Outsider threats" interactor_id="580df674161983000e75a6ca">
      <atLocations/>
    </actor>
    <actor id="actor__Suppliers" type="tkb:actor" name="Suppliers" interactor_id="580df6b1161983000e75a6cc">
      <atLocations/>
    </actor>
    <actor id="actor__Employees" type="tkb:actor" name="Employees" interactor_id="580df6bd161983000e75a6cd">
      <atLocations/>
    </actor>
    <actor id="actor__Regulator" type="tkb:actor" name="Regulator" interactor_id="580df6f8161983000e75a6ce">
      <atLocations/>
    </actor>
    <actor id="actor__null" type="tkb:actor" name="null" interactor_id="580df936161983000e75a6d1">
      <atLocations/>
    </actor>
  </actors>
  <edges/>
  <locations/>
  <assets/>
</system>
```


Figure 6.4: The exported .xml file which contains the actors transcribed into the prototype.

from practitioners and screen-shots of the evaluation tests that dealt with an online and physical shopping outlet (renamed ‘Acme’, although based on an actual case in the UK, based on the current experience and employment of one of our participants).

As Fig.6.2) shows, participants modelled with LEGO™ the ‘Acme’ retail environment, both as an online service and as a ‘bricks and mortar’ service (Fig. 6.2). They then were able to produce a mapping of the physical model, showing the key relationships between actors and assets. It was noticeable that the resulting digital map did not include Acme’s customers, despite their having featured prominently in the source model. This may have been an oversight but also may have been a result of these security practitioners reverting to following an asset-based procedure as opposed to a more people-centric one.

The resulting map contains a dense and relatively balanced network. The thickness of lines indicates something of the approach being developed here, which is that heavier lines need less protection than thinner ones, and that the more tenuous lines indicate relationships that attackers may want to attack. The ‘Head Office Staff’ seem relatively exposed at the centre of the whole network. It would be interesting to know how another iteration of the *InterActor* modelling might re-configure this network if the customers were given a place in it.

In contrast to the previous user-journey outputs (Fig. 6.2), these outcomes placed the customer at the front and centre of the ‘Acme’ retail environment (Fig. 6.3). In a much reduced or abstracted graphing of the same data, the customer’s position is bolstered by the proximity of the regulator, and by contact with shop-floor employees rather than by any connection with ‘Acme’ as an organisation.

This resulted in an exported .xml file which contains these actors, and can be imported into the ANM, where it is then augmented by the addition of other types of entity, both social and technical. As was the case in the RHUL Summer School (see (The TRESPASS Project, D4.2.2, 2016)), this import functionality demonstrates how users are able, over a comparatively short period of time, to migrate from the physical modelling part of the

TRESPASS platform, to the area where in the ANM these models result in attack tree visualisations based upon the same scenario.

7 Conclusions

This deliverable presents a strand of the work undertaken on the TRE$_S$PASS project to visualise the social dimensions of cyber security risk and place those social dimensions within a socio-technical system. The second strand of this work is presented in (The TRE$_S$PASS Project, D4.2.2, 2016). During this four year project we have engaged extensively with security practitioners in order to identify which social aspects of a cyber security risk scenario are of most important to the risk assessment process. Then using physical modelling and paper prototyping we identified the requirements of a prototype that could support security practitioners in the visualising of social aspects of cyber security risk. Finally, we developed a series of user journeys that takes users (the security practitioner) from conducting a Stage Zero brainstorming session to scope the risk landscape of a particular scenario, to developing a visualisation of the interactions and relationships at work within the scope and finally to bringing this social understanding to the attack maps within the ANM. This deliverable describes this development journey and presents the prototype that was produced in conclusion.

The ANM puts the creation of models at centre-stage, in a way that is comparable to the physical modelling. The user journey that we have developed, reflects how the digital modelling in the ANM can be brought together with the physical modelling of LEGO^{TM} via a broker prototype, *InterActor*. Throughout this deliverable we demonstrate that this journey was designed with the target user community. The user community brought a detailed understanding of day to day risk assessment activities and we contributed design-know how and a theoretical understanding of the importance of networks of relationships and interactions to the defence of an organisation's information assets.

In our design of *InterActor* we were careful to not only reflect the input of the target user community but also of the other development initiatives within TRE$_S$PASS. Risk or impact-based highlights are visible within the ANM, and also in *InterActor*. In the former, nodes are highlighted to show top leaves of an attack tree. In the latter, this is as a result of a user's search for such terms as keywords. In each case a user can then perform other operations on these results if they wish. In addition, each data-type has a distinct graphical character in these tools, bringing them to the user's attention in appropriate ways.

The TRE$_S$PASS risk assessment process uncovers many facets of socio-technical systems that would have been difficult to detect otherwise, and does so in a compressed time window. This on its own is a step beyond the current state of the art of risk assessment, but we take a further step in providing mechanisms for users to link social data to visualisations that aid iterative evaluation and the sharing of insights.

WP4 has replaced the notion of a generalised persona profile with one that is based directly on the observations of stakeholders. Using *InterActor* users can summon up the

synopsis page of any actor on their model, seeing there a rich representation of what this actor means within the model of the system. Another step is then possible by combining recognisable icons for many actors, progressing towards a picture of social practices in this space. In this way a security practitioner will be able to continually update their understanding of the social dimension, and this can be merged with more comprehensive technical models in the ANM producing and analysing attack paths as a result.

References

Flach, J. (2012, September). Complexity: learning to muddle through. *Cognition, Technology & Work*, *14*(3), 187-197. doi: 10.1007/s10111-011-0201-8

Heath, C. P., Coles-Kemp, L., Hall, P. A., et al. (2014). Logical lego? co-constructed perspectives on service design. *DS 81: Proceedings of NordDesign 2014, Espoo, Finland 27-29th August 2014*.

Moody, D. (2009, November). The "physics" of notations: Toward a scientific basis for constructing visual notations in software engineering. *IEEE Trans. Softw. Eng.*, *35*(6), 756–779. Retrieved from http://dx.doi.org/10.1109/TSE.2009.67 doi: 10.1109/TSE.2009.67

Norman, D. A., & Stappers, P. J. (2015). Designx: Complex sociotechnical systems. *She Ji: The Journal of Design, Economics, and Innovation*, *1*(2), 83 - 106. Retrieved from http://www.sciencedirect.com/science/article/pii/S240587261530037X doi: http://dx.doi.org/10.1016/j.sheji.2016.01.002

The TRE$_S$PASS Project, D2.3.2. (2015). *TRE$_S$PASS social data and policy extraction techniques.* (Deliverable D2.3.2)

The TRE$_S$PASS Project, D4.2.2. (2016). *Methods for visualization of information security risks.* (Deliverable D4.2.2)

The TRE$_S$PASS Project, D4.3.1. (2014). *Initial visualisations of socio-technical dimensions of information-security risks.* (Deliverable D4.3.1)

Thompson, J. D. (1967). *Organizations in action: Social science bases of administrative theory*. Transaction publishers.

Tidwell, J. (2005). *Designing interfaces: Patterns for effective interaction design*. O'Reilly Media.