predict
prioritise
prevent

TRESPASS

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

Deliverable D1.3.3

Dynamic features of socio-technical security models

Project:	TRESPASS
Project Number:	ICT-318003
Deliverable:	D1.3.3
Title:	Dynamic features of socio-technical security models
Version:	1.0
Confidentiality:	Public
Editor:	Lorena Montoya
Cont. Authors:	S. Bleikertz, J.W. Bullée, M. Ford, D. Ionita, H. Jonkers, L. Montoya, S. Saraiva, A. Tanner, A.S. Yesuf, J. Willemson, C.W. Probst
Date:	2015-10-30

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
AAU		Contributions at an earlier stage
BD	Henk Jonkers	1, 2, 3, 4, 5
CHYP	Margaret Ford	2, 3
CYB	Jan Willemson	B
DTU	Christian W. Probst	3, A, B
GMVP	Sérgio Saraiva	2, 3
GUF	Ahmed S. Yesuf	2, 3
GUF	Lars Wolos	2, 3
TUHH		Contributing to D1.3.2
UL		Contributions at an earlier stage
UT	Dan Ionita	3
UT	Jan-Willem Bullée	3, 4, C
UT	Lorena Montoya	1, 2, 4, 5, C
IBM	Axel Tanner	2, 3
IBM	Sören Bleikertz	2,3

Quality assurance		
Role	Name	Date
Editor	Lorena Montoya	2015-10-30
Reviewer	Zofia Lukszo	2015-10-15
Task leader	Lorena Montoya	2015-10-30
WP leader	Christian W. Probst	2015-10-30
Coordinator	Pieter Hartel	2015-10-30

Circulation	
Recipient	Date of submission
Project Partners	2015-10-30
European Commission	2015-10-30

Acknowledgment: *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

Key takeaways:

- The case study partners have identified dynamic aspects of each case study and the ability of the TRESPASS project to cope with such aspects has been explored. We found a large range of dynamic features differing in both nature, level and time scale. The dynamic features identified for the different case studies occupy different positions along each of these scales.
- A few dynamic features are not supported by the current version of the TRESPASS socio-technical security modelling language (TPL). Further work will determine whether extensions can enable the dynamic features that the TPL can't currently handle to be modelled in the future.
- A survey of security academics and practitioners was undertaken to identify the differences between past and predicted future emerging threats. We identified a number of themes that academics and practitioners consider will change within the next 5 years but that we found were not being mentioned in key reports. The TPL language is on track since none of the emerging threats identified seem to pose a problem.

The primary goal of the TRESPASS project is to develop tools that facilitate assessment and management of IT security-related risks in an organisation, spanning both technological and sociological issues.

The current deliverable D1.3.3 is concerned with the dynamic features that socio-technical security models must support. This will be done on the basis of the requirements from the case studies, taking into account project results, especially the validation of the model in the case studies. The topic of dynamic features focuses on circumstantial or contextual changes, particularly temporal ones.

In this deliverable, dynamic aspects have been identified based on the case studies, and the ability of the TRESPASS project to cope with such aspects has been explored. In addition, a survey of security academics and practitioners was carried out to identify the differences between past and predicted future emerging threats, in order to elucidate whether the model is likely to cope well with future threats.

1. Introduction

This document presents the analysis and conclusions related to dynamic features for work package WP1 ("Socio-technical security model specification") of the TRESPASS project. The goal of WP1 is to develop models that capture the essentials of an organisation and its structure on three core levels: the physical, digital, and social domains. The model contains entities, attributes, and relations that are relevant for analysing the organisation's security. Appendix A provides the context for this deliverable in the TRESPASS project. It describes the overall summary of the project and the TRESPASS workflow.

The socio-technical security models are at the heart of the technical part of TRESPASS, and constitute the interface between the organisation being modelled and the processes and tools developed in other work packages, such as the analysis tools of WP3, and the visualisation tools of WP4. For the integration into risk assessment frameworks (WP5), the models developed in WP1 are the entry point into the TRESPASS process. The socio-technical security models are therefore a key enabling factor for the TRESPASS process; they must be easy to develop and to visualise, to enable company users to interface with the TRESPASS tools, and they must be detailed enough to support the analysis tools to predict attacks, prioritise attacks, and suggest preventive measures.

Models of organisational infrastructures have been used before, e.g., to identify insider threats in organisations and to compute attacks on organisations. The challenge in this work package is to integrate the modelling of policies and social dimensions, and again to do so in a way that supports implementation, analysis, and visualisation.

An important aspect of the models is modularity, not only to support modular model development and maintenance (WP5), but also to support compositional analysis of the models being developed (WP3). The TRESPASS socio-technical security models will also be modular in the sense that different features can be added on demand; features such as detective components, for example, are optional and only added when needed for modelling the organisation.

1.1. Goals

The world is dynamic and evolves over time. A simplified view of the world, i.e. a model, should be dynamic as well. The analysis of dynamic features is relevant because it could point to varying levels of attack success probability and the need to ensure that the model is able to handle more detail e.g. to account for the temporal dimension.

The objective of Deliverable D.1.3.3, Dynamic features of socio-technical security models, is to develop support for dynamic features in socio-technical security models based on the requirements from the case studies taking into account the results especially from WP7 based on the validation of the model in the case studies.

The objective of this deliverable is two-fold:

- To make an inventory of the dynamic features of the four case studies and evaluate whether the TRESPASS model can cope with them, and
- To compare threats from 15 years ago to those expected for the future 5 years and to identify which of those emerging threats could have implications for the TRESPASS model.

1.2. Choices made

The case study owners supply the content about the dynamic features. The analysis of the change in threats will allow determining whether the TREsPASS model needs to be adapted or extended to cope with changes in the threat spectrum. The source of information for the emerging threats is a survey of security academics and practitioners as well as two recent reports.

1.3. Foreground and background

The text in this deliverable constitutes foreground.

1.4. Document structure

This document is structured as follows. Chapter 2 provides the application context in the form of four case studies summaries, and Chapter 3 gives a description of dynamic features for each of the four case studies. Chapter 4 discusses the emerging threats, while Chapter 5 presents the conclusions. Finally, Appendix A presents a project summary i.e. a more high level contextual view of the project, Appendix B describes the TPL language and Appendix C presents the extended explanation of the emerging threat findings.

2. Case Study Summaries

The TRESPASS process and tools are being validated by means of three case studies, each of which support the iterative development of both the TRESPASS process and tools as well as the iterative development of the organisation-specific socio-technical security model. The case studies concern a cloud infrastructure, a telecommunications infrastructure, an organisation processing privacy sensitive data and an ATM infrastructure. We provide a brief summary of each case study as to provide sufficient context for the reader to understand the following chapter.

2.1. IPTV

In this section we describe the "IPTV case study", that has been used as a running example throughout the project[1]. The technical details as well as the people and companies involved are confidential and we therefore present an anonymised and slightly redacted version of the original case study. However, all the important features have been retained and the processes are fundamentally the same as in the original case study.

The case study concerns a system supporting primarily elderly and disabled people in performing online payments and managing their own money from their home. With the target demographic in mind, the system should be integrated into an existing device that is familiar and easy to use for the intended user groups, namely the television set. In practice this is accomplished by hooking up a small, dedicated computer to the TV and an enhanced remote control with a built-in card reader for authentication as illustrated in Figure 2.1. In this case study there are many different security aspects that may be considered: from the strictly technical, such as how information is protected while stored or transmitted, to the socio-technical, covering security issues arising from the use of and interaction with the technology. Within the project, we have explored the socio-technical features of the case study, as a means of validating the methods and tools which are being developed. In particular this case study has provided a context in which to explore the many possible approaches to handling social data.

2.1.1. Normal Usage and Context Assumptions

Figure 2.1 shows an overview of the IPTV case study: there are two primary actors: the attacker (represented by a devil in the figure) and the victim (the IPTV owner/user).

[1] Here IPTV refers to televsion service(s) over the IP protocol.

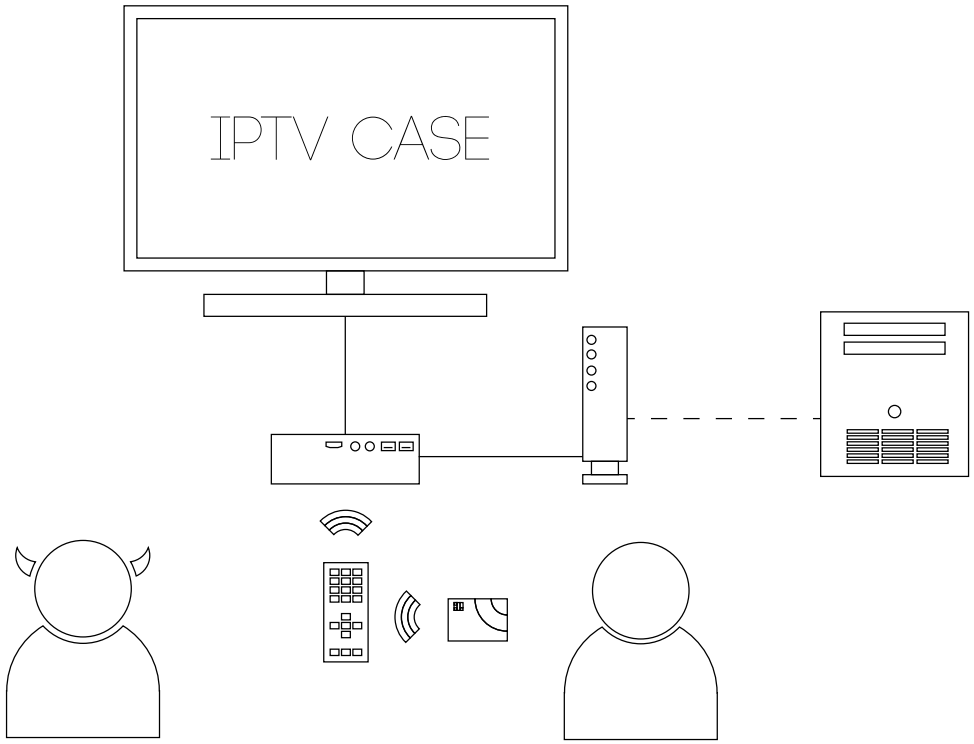

Figure 2.1.: IPTV case study

Under normal operation, the user would first open a session on the IPTV, using a standard password based authentication scheme. From this session, the user can then use different services, e.g., pay a bill or transfer money, by using a payment card with concomitant PIN code. The payment card is read by a card reader built into the IPTV remote control on which the PIN code is also entered.

The design is intended to be simple and offer the means for people of all ages and abilities to be able to access the services they require. It is intended to complement other means of delivery, not to replace them. In particular, it offers the opportunity for people who are not familiar or comfortable with mobile technology to receive the benefits of the ever-increasing range of mobile services in their homes via their television screen (Egelman, Brush, & Inkpen, 2008). Although this system could offer great convenience, it also has the potential to expose the account holder to significant social risks, particularly those stemming from the involvement of both professional carers and family members. These carers could be considered as knowledge insiders, with the potential to act as malicious insiders.

We have made a number of assumptions about the context for the case study:

1. The card-holder has a functional IPTV in his/her house prior to the attack.
2. The IPTV security configuration ensures security for the communication of data between the different physical devices.

3. One Internet Service Provider (ISP) is used for all Internet access.
4. The source code of the software of the IPTV system is not freely available.
5. Firmware updates are not cryptographically encoded.
6. The IPTV set-top box uses a standard API.
7. The user can log on and off the IPTV system at will.

While these assumptions help delineate the scope of the case study, they are not critical and can be relaxed or modified to better capture a specific system.

2.2. Telco

Telecommunications products and services are functional in a complex environment involving a multitude of different interconnected networks, service providers and network operators with opposed financial interests acting in highly competitive markets offering complex products and services.

Due to the market structure described above, new customers are not easily available, but normally need to be lured away from competitors. As the providers try to escape the pricing pressure resulting from replaceability of the communication goods, e.g. new tariffs more and more become a mixture of free (flat rate) components being heavily advertised and, less noticeable, much more expensive components for compensation and revenue generation. New products need to be launched under significant time pressure resulting from strong competition in the market, leaving little time and space to account for potential misuse of the product. Apart from that, often the misuse resulting from product design flaws is a learning process which takes place once the respective product or service has been launched into the market.

The above tendency, in contrast, encourages cherry-picking among customers of Telco companies. This is especially true for so-called knowledge insiders that know the market very well, trying to make as much use of (or monetary gain from) the products offered as possible.

An example of the sort of fraud addressed by the project involves using insider knowledge to exploit flat rate tariffs for call termination, which despite the terms and conditions of the respective network operators, provides a profit for the fraudster (refer to Figure 2.2). An example includes the fraud involving the false pretense of being willing and able to pay for calls.

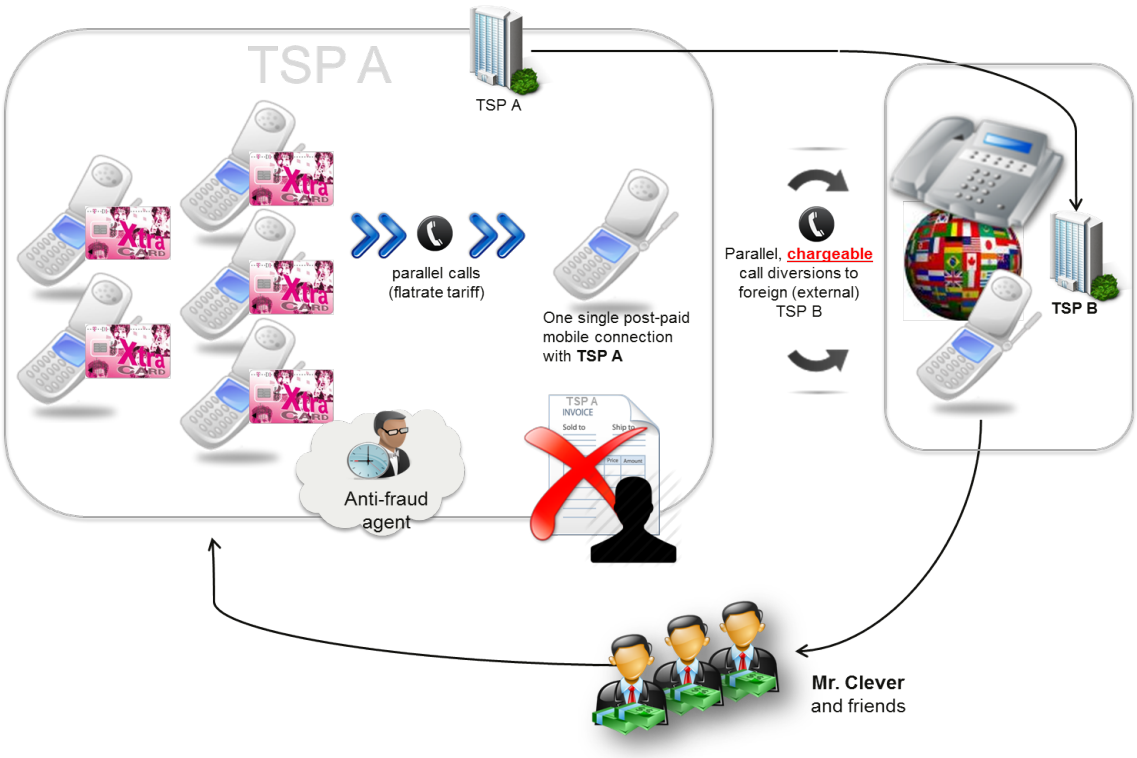

Figure 2.2.: Fraud scenario - fraud involving the false pretence of being willing and able to pay.

2.3. Cloud

Cloud computing has gained remarkable popularity in recent years due to the economic and technical advantages of this new way of delivering computing resources. Customers benefit from rapid provisioning and seemingly infinite scalability, while only being charged on a pay-per-use basis. Computing resources can be provided on different abstraction layers (Mell & Grance, 2009b), where the lowest one provides basic resources (servers, network, and storage), and higher ones provide applications to the end-users (e.g., Google's GMail, Salesforce.com). In this case-study we are focusing on the lowest abstraction layer, that is *Infrastructure-as-a-Service* or *Infrastructure Clouds*, since it is the most generic layer and higher ones often build upon this layer.

Although the benefits of cloud computing are evident and users demand cloud services, security is a major inhibitor (Mell & Grance, 2009a). An analysis of risks and threats in cloud computing has been conducted in (Cloud Security Alliance, 2010) and (ENISA, 2009). In particular, both reports agree that insider attacks and malicious insiders are a major risk and are among the top 10 threats. The risk is amplified due to the disappearance of physical boundaries that makes it very challenging to define a security perimeter that divides insiders from outsiders (Hay, Nance, & Bishop, 2011; Pieters, 2011).

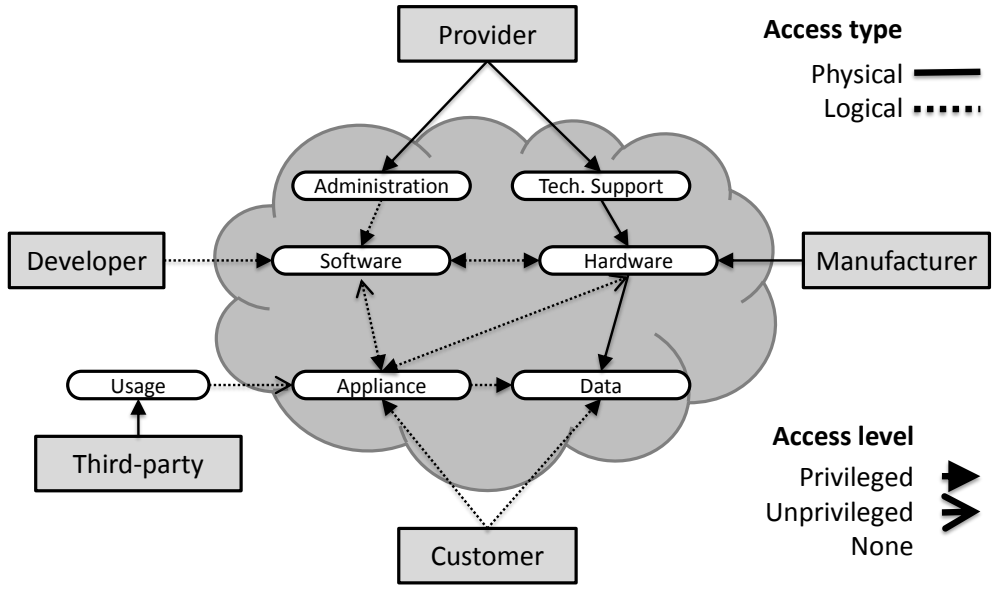

Figure 2.3.: Overview of entities and components in an infrastructure cloud model.

Figure 2.3 provides an overview of the entities and components involved in a model of an infrastructure cloud. As compared to a typical IT department within an organisation, the provider of the cloud services in such a shared infrastructure cloud is a new additional and powerful party. The multi-tenancy (different customers, including competing organisations, using the same cloud services) lead also to an unprecedented sharing of computing and infrastructure resources. The cloud provider therefore becomes an important additional factor (and risk), as it has full physical and logical access to all resources across the different consumers. In addition, the infrastructure itself is dynamic and flexible in response to the requirements of the customers.

If risk assessment in complex technical infrastructures is already difficult, it is even more complicated when human factors and physical infrastructure are added to the setup, which are correspondingly often ignored (Probst & Hunker, 2009).

The special interest to investigate this scenario within the TRESPASS project is therefore to develop models and processes that support risk assessment in complex organisations *including* human factors and physical infrastructure. The goal of this support is to simplify the identification of possible attacks and to provide qualified assessment and ranking of attacks based on factors such as the expected impact.

For cloud infrastructures, the TRESPASS model distinguishes components at a level of abstraction that corresponds well to security-relevant control points in these domains, enabling the discovery and analysis of potential attacks that exploit their connectivity. Using the model, one can formalise typical components in cloud infrastructures and their interrelationships. These include network components like switches, routers, firewalls; virtual and physical servers; actors, including administrators, users, and attackers; location details that represent rooms, doors, and other physical consideration. Because these com-

ponent models show how actions on one element influence other elements, they can be combined with the connectivity relations to form an implicit search-space of all possible activity paths in the system.

2.4. ATM

ATM machines are composed of a money safe and a computer that controls the ATM's devices (screen, keyboard, printer, network interfaces, money safe mechanisms, etc.) through software programs. Most ATM computers are composed of outdated hardware running legacy operating systems (i.e. Windows NT), which are not supported by the vendors or by the anti-virus providers. The installation of the ATM machines varies as there are well protected ATMs installed inside bank branches, while others are deployed in the street and some are not even embedded in a wall.

ATM attacks are common and include classic physical attacks and emerging digital attacks. Examples include:

- Physical attacks where the attacker physically steels the ATM to open the safe and take the money.
- Digital attacks where the attacker installs a malware agent into the operating system to take control of the devices including the ability to withdraw money from the safe through the device' s interfaces.

In order to perform a proper risk assessment of the ATM network as a whole, four types of data must be considered and combined into a single unified model, suitable to be processed on a consolidated data schema:

- Technical data (about the machines)
- Environmental data (about the territory)
- Historical data (about past occurrences)

Attacks do not happen randomly in time and are neither equally distributed over the territory. Machines installed on certain places are more likely to be attacked than others, thus spatio-temporal hotspots exist. This case study therefore adds both the temporal and a geographic dimension to the project.

The ATM case study builds an analysis process at the macro-level based on data from the ATM network and surrounding area, and outputs the vulnerability level of each ATM. More specifically, this case study illustrates how to perform an analysis at a macro level for identifying priority areas in need of detailed analysis using the TRESPASS model and tools.

3. Dynamic Features

In general terms, research into System Dynamics involves studying how a physical system develops or changes over time and studying the causes behind such changes (Wikipedia, 2015). In general, dynamic refers to being energetic, capable of action and/or change, or forceful, while static refers to being stationary or fixed. Both terms can be applied to different types of things, such as programming languages (or components of programming languages), Web pages, application programs, etc. (Rouse, 2015). For example, a static Web page displays exactly the same information to everyone visiting it. Dynamic Web pages, on the other hand, are capable of producing different content for different visitors from the same source code file. The website can display different content based on the operating system or browser the visitor is using, the type of device being used to navigate, or even the source that referred the visitor (McDunnigan, 2015).

In addition, in the security literature there is a thorough discussion of static versus dynamic model analysis. Static analysis refers to the testing and evaluation of an application by examining e.g. the code without executing the application. Dynamic analysis refers to the testing and evaluation of e.g. an application during runtime (Intel Corporation, 2013). It must be noted that this deliverable, however, is not concerned with the forms of analysis but rather with the identification of those features in an socio-technical information security model which are dynamic.

Dynamic features of models are related to circumstantial or contextual changes, particularly those concerning temporal changes. Temporal changes could cause attack success probability not to be fixed but to vary instead. It is therefore necessary to identify not only what might change but also whether the existing TRE$_S$PASS model is able to cope with such changes. For example, threats might be evolving over time because the attacker motivation might not remain fixed. The amount of staff being physically present throughout the day, week or month might also vary. From the defense viewpoint, it is possible that what constitutes an asset also changes over time.

3.1. Case Studies

The case study owners were asked to elaborate on what is ‘dynamic’ in the case studies. The following three questions were investigated:

- What could be considered to be ‘dynamic’ in the case study?
- Does the TRE$_S$PASS model(s) already cope with those dynamic features or is that yet to be done?

- Have the risk(s) associated with this case study evolved over time ?

The method used for obtaining the dynamic features was the following: i) the case study owners were interviewed and asked what they considered to be dynamic in their case study, i.e. what aspects of the case studies could change in such a way that the outcome of an attack (e.g. probability of success) would change, ii) the responses obtained from the interviews were structured, merged and grouped, iii) the features that were deemed to be dynamic were modelled. Initially this was done by two of the authors of this deliverable, but in a later stage the developers of the model were asked to do it as well. That said, we did not conduct a reliability analysis, however, as we believe that different persons will reach the same conclusion. For each identified feature in the Cloud and IPTV case studies, it was indicated whether the feature could be modelled using the TPL language. In the case of the Telco case study, it was tested on both the TPL language (refer to Appendix B for a TPL language description) and on the e3value fraud model (e3fraud methodology is described in-depth in (Ionita, Wieringa, Wolos, Gordijn, & Pieters, 2015)). An overview of the result of this process is presented in Table 3.5. The last column of this table points, among other things, to the specific TPL feature that it relates to.

3.1.1. IPTV

The social structures are the most dynamic features of the IPTV case study. While the technical architecture is relatively standard and fixed, the social aspects of the case study provide the greatest challenges in analysing the environment and understanding the range of potential attacks. The organisation under investigation in this case study relies on complex networks of supportive relationships in order to be able to deliver high quality socially-motivated services. This involves a high degree of trust and confidentiality in the handling of sensitive client data. It also requires a heightened awareness of the potential social, commercial and legal implications of key service design decisions. Important features include:

- Organisational structures;
- Roles;
- Cultures; and
- Individual characteristics.

Perhaps one of the most challenging aspects of this case study has been the focus it places on handling of data at the level of both a single individual and the wider organisation. This has required a particular approach to modelling, with an emphasis on the individuals involved, especially potential users of the service. As data gathering and research have progressed within the project, different elements have helped to produce a more complete view of the issues presented by this case study. While it has provided a basic testing-ground for some of the socio-technical approaches, the financial aspects of the case study have also formed a basis for some of the emerging threats work around security issues in the financial services sector.

The fundamental nature of the threats associated with the case study remains essentially the same over time, however in terms of both financial threats and emerging social engineering attacks, this is a very dynamic area. Particular care is required when people with limited experience of technology are being encouraged to engage with digital services. While there may be considerable benefits in terms of cost and convenience, it also opens up new avenues for potential abuse. One example is the now common attack of cold calling people in their own homes and offering remote technical support for their computers. The cold caller may then take control of the computer and even harvest financial data. This attack relies on technology being in the hands of people who are not entirely confident in their ability to maintain it, and has in some cases resulted in considerable inconvenience and financial loss for the individuals concerned.

Overall, the TRE$_S$PASS model is well suited to representing the kinds of digital and physical structures, as well as trust relationships, presented by this case study.

The dynamic aspects of the IPTV case study are summarized in Table 3.1 and an indication of whether the TPL language is able to support each aspect. A description of the TPL language is included in Appendix B.

3.1.2. Telco

Telecommunication companies by nature are flexible, time dependent, and customer-oriented sectors of the economy. These features have either direct or indirect influence on the revenue of the telecom companies. The fact that there is a customer interest in a new service can potentially affect the business model of the telecommunication companies, which leads to change in their existing ways of providing telecommunication services to their customers. Either they could add a completely new service or modify the existing one.

In general, we can see the dynamic features of the telecommunication sector from two broad perspectives: i) the company level and ii) the customer or service level.

From the perspective of the telecom companies, there are several elements which need timely modification. The following elements are dynamic features in the telecommunication sectors:

- The business model;
- Revenue assurance techniques;
- Fraud management processes;
- Human resource management at the company level;
- Infrastructure security management;
- Customer privacy protection policy;
- The types of contracts for the telecommunication services.

The reasons behind such changes fall under two categories: internally motivated or externally pressurised. Internally motivated in the sense of the way the activities of the employees are controlled, their security level, the increase/decrease in revenue. On the other hand, the factors that are externally motivated include e.g. the market competition, the standard organizations, auctions.

From the customer or service perspective, the types of telecommunication services and the customer behaviour towards those services is what leads to some elements being dynamic. For example, consider a customer having an agreement with the telecom company for having the IP-Phone service integrated with additional services. While being away from his premises, this customer has the possibility to access the IP-Phone without any extra charges. This applies also for business customers who have several branches in different places. Thus, the type of service changes the way the customer behaves. Conversely, if the customer frequently needs, for example, a roaming access to a landline telephone while the customer is away from his home network, he might be charged a higher price while being connected. This might cause the customer to migrate to another operator. Nevertheless, for such groups of customers the telecom company might have to modify their contracts either by having a flat rate roaming charge or something more reasonable. Therefore, the customers' need could lead to a change in the types of telecommunication service contracts.

Generally, the telecommunication sector is dependent on time, customers' needs, legislations (e.g. from standard organisations), technological evolution, market completion and company-level factors. Thus, change in the elements of telecommunication will remain dynamic.

The dynamic aspects of the Telco scenario in Figure 2.2 are summarised in Table 3.2 and an indication of whether the TPL language is able to support each aspect.

The TRE$_S$PASS model handles most of the static features of the telco scenarios e.g. the virtual connection between the TSPs, the properties of entities in the scenario, the fixed locations and ordinary processes through out the TSPs. However, a few of the identified dynamic aspects of the telco scenario are not currently handled. The above-mentioned table is important for further developing the TRE$_S$PASS model.

To handle the very specific requirements of the Telco case study, namely the focus on value transfers instead of the socio-technical architecture, an alternative modelling and analysis approach was developed. This approach is designed to also cover (most of) the dynamic features listed in the table above. The e3fraud modelling language and tool are described in Section 2.3.2 of D1.3.2 (The TRE$_S$PASS Project, D1.3.2, 2015), while the e3fraud risk assessment process is presented in Section 6 of D5.1.2. (The TRE$_S$PASS Project, D5.1.2, 2015).

3.1.3. Cloud

In the Cloud Infrastructure case study, the infrastructure is the part with the highest dynamism. This is strongly driven by the promise of cloud providers to offer quick provi-

sioning and scaling on demand. Demands can change due to a variety of reasons, be it regular fluctuation due to the time of day, or special events like Superbowl in the US or special promotions of companies, e.g., around the Christmas time. But also other factors can drive quick changes in the cloud environment, e.g. migration of virtual machines (VM) between different physical hosts (or even data centres) due to workload requirements (VMs with higher loads moving to more lightly-loaded physical servers), or driven by cooling requirements in the data centre (moving VMs with high loads from hot to cooler parts of the data centre), or to reduce overall power requirements (consolidating active VMs to fewer physical servers, allowing to shut down some of the physical servers). Lastly, also problems with the physical infrastructure like failing harddisks or physical servers will lead to a quick reconfiguration, to ideally minimise the impact of the outages. This leads to a high dynamism mostly in the virtualised infrastructure: within seconds, virtual servers can be created, destroyed or moved, with corresponding network changes and reconfigurations.

All this can be captured in the notion of *Software Defined Environments* (SDEs): more and more things traditionally requiring hardware and cabling changes, on the timescale of days, can now occur in the virtual environment by just *redefining* the virtual environment within seconds.

Not all changes of course happen on this very short timescale. As pointed out in Section 2.3, besides the potentially extremely fast changes in the infrastructure, physical and social realms are of importance and interest in this context, too. Changes to the physical environment, as well as operator actions and human interactions happen of course on slower timescales.

The cloud scenario is interested in investigating the 'howtos' and trade-offs of handling the risks on these different timescales, where, for example, checking/enforcing compliance rules ('no network path may exist between certain network domains') has to take place on all timescales, whereas support of risk-analysis and planning including social and physical elements, like the value of introducing a new authentication mechanism for system administrators, will consider completely different timescales and will not require all details and changes happening at the level of the virtual compute infrastructure.

Similarly, besides the timescales of changes, the different realms are different with respect to the volume of available data and its precision: due to the properties of the virtual environment being mostly described in the form of configuration settings (as a Software Defined Environment), it is possible to get very rich, highly detailed, timely and accurate information about the (mostly virtual) infrastructure - with a high volume of extremely detailed data. Social parts, on the other hand, are harder and slower to obtain, less precise, but also the volume of data is much smaller. Note, though, that some parts of the interaction between social/human and infrastructure spheres can be captured electronically, i.e. access control levels and data logging operator actions, and therefore are available quickly and comprehensively.

Of course, changes to the entire infrastructure still happen mostly in smaller incremental steps over time, though potentially on a short timescale of minutes or seconds. Where one wants or requires to follow these changes in real-time, processes in the tool chain

from data collection to analysis results need to be aware of this dynamic nature and must be triggered by changes and ideally happen in an incremental fashion, due to constraints in the volume of data and time available for processing (Bleikertz, Vogel, & Groß, 2014).

It remains to be seen how to do risk analysis in this environment with widely varying timescales and levels of detail in knowledge and the TRESPASS project needs to include work to investigate where it makes sense to take data and analyse in real-time and where not.

Dynamic aspects of the Cloud case study are summarized in Table 3.3 and an indication of whether the TPL language is able to support each aspect.

3.1.4. ATM

The ATM case study aims to deliver a risk evaluation over the territory taking into consideration i) technical, ii) social, iii) environmental and iv) historical data. Out of these four, the historical data is the only one that does not change over time, everything else is dynamic in the sense that it is constantly changing. Firstly, the ATM network is dynamic since every year new machines are deployed, and existing machines are replaced or removed. Secondly, from the technical perspective, an ATM network is a network of computers running software (including the operating system) over hardware. Different ATMs are built of different software/hardware versions, which also change considerably over time. Thirdly, the population and social context surrounding the network can also change over time. Usually this change does not happen rapidly, except on very specific situations, which usually include changes in the environment, which is also mapped here.

The TRESPASS model is able cope with dynamic features in the sense that it is able to describe the technical aspects of an ATM network. The ability to describe a social context is something that needs further analysis within the case study. Environmental and historical data needs also need to be validated. Currently not present in the TRESPASS model are geographic capabilities, from geographic data representation to geographic data processing, although it can be included as an extension/add-on to the model to be handled outside. In other words, geographic data could be collected, represented, pre-processed outside the TRESPASS model, and transformed to a format that complies the TRESPASS model.

One of the most interesting features of this case study is that it is able to represent the criminal dynamics over time, and it allows to understand the correlations between technical, social, environmental changes, and the criminal occurrences. For example, if a certain environmental event happens that changes a certain territorial landscape (i.e. the construction of a certain big commercial area; or, more recently in Lisbon, a big harbor cruise ships, etc.), that will most probably affect the social context over time, and consequently the criminal dynamics. We expect this to also impact crimes against ATMs.

The dynamic aspects of the four case studies are summarized in Table 3.4 and an indication of whether the TPL language is able to support each aspect.

3.1.5. Summary of Dynamic Features

Dynamic aspects of the ATM case study is summarized in Table 3.5. and an indication of whether the TPL language is able to support each aspect.

Table 3.1.: Summary of dynamic features in the IPTV case study

ID	Description	Details	TPL
I1	Technological Landscaping	The technology landscape changes rapidly, everything is in the cloud and on smartphones. These are hugely integrated into our daily lives. However, the interplay with technology is deceptive, it gives us the illusion of being in full control. In the case study, there are significant trust issues around providing a service via the TV interface.	Y
I2	Technological Threats	Genuinely new attacks are extremely rare, most are old attacks that are adapted to the new technological landscape. Attacks that were initially theoretical attacks described by academia are now feasible and practical, thanks to increases in processing power and interconnectivity.	Y
I3	Social Attacks	Change of who is in control of the system. In order to achieve cost savings, many organisations expect their customers to transact online by default. This results in demographic changes to the online community, introducing potentially less experienced users who may become easy targets.	Y
I4	Social Landscaping	Where particular services or discounts are only available online, people may feel obliged to access these digitally. Service providers, both commercial and social, have a great incentive to cut costs by providing services online in preference to in-person or by telephone. There has been a softening in recent years of the 'digital by default' approach to delivery of certain public services, recognising that this is not appropriate for all clients. Another significant change is the effect of off-shoring, outsourcing call centres to lower cost countries. This can introduce a degree of unfamiliarity and discomfort to the telephone environment, potentially introducing different kinds of vulnerability. This may be heightened where there are language issues.	Y
I5	Financial Landscaping	Changes in regulation may encourage banks to take a greater degree of responsibility for issues concerning payments i) recognising that the responsibility may not lie with the customer and ii) checking whether the financial commitments of their customers are realistic (e.g. not over-extending credit card limits).	N
I6	Financial Attacks	Contactless is one of the latest innovative methods of quick and convenient payment. It is now in widespread use and the upper limit for contactless payments recently increased by 50% from 20 to 30 Pounds. As the acceptance of contactless becomes more widespread and the payments amounts increase, there is a greater incentive for attackers to shift their focus to this technique. This same principle can be witnessed in the statistical increase in cyber crime, while traditional crime levels diminish. The nature of these crimes, and therefore appropriate countermeasures, are constantly evolving.	Y
I7	Roles	Give a person a function or role in the system (e.g. caregiver, technician and patient)	Y
I8	Individual and Cultural Characteristics	The behavioural characteristics a person has (e.g. personality) and how they live their life. Trust in the authorities is a characteristic that varies between countries, knowledge of this property can be valuable in planning an attack.	Y
I9	Trust Relations	There are 2 kinds of trust relations in the IPTV case study: i) trust between two people and ii) trust between a person and an organisation. For the trust between people, there is a start and an end point (an engineer comes to the door to fix something, then leaves at a later point in time). Person to organisation is established initially via a person to person relation. By trust in the organisation, trust in one of their employees is implied.	Y

TPL = Supported by the TPL language
N=No, Y=Yes.

Table 3.2.: Dynamic features of a Telco scenario in Figure 2.2

ID	Description	Details	TPL support	E3-fraud
T1	Number of pre-paid SIM cards	Using more SIM cards will increase the gain, this is limited because it depends on the availability of the SIM cards and on the middleman. There are static costs aassociated with bribing the middleman to buy the SIM cards for you and if this person only can get a limited number of cards, the costs exceed the actual profit.	Y	Y
T2	The tariff rates	Rates differ depending on the types of contract and sometimes based on the location. There are different prices for calling domestically or internationally, this also differs for data roaming. The tariff rates differ among Telecom operators.	Y	N
T3	Number of fraudsters or attackers	'Mr. Clever and friends' can be considered as one or more than one fraudsters. This involves colluding of attackers for TSP A and TSP B. Furthermore, multiple subscriptions for TSP A can be from the same person.	Y	Y
T4	Location of the fraudster or the attacker	The location of where a service is accessed from can vary, this represents the location of the base station routing the phone calls. The location of the base station can differ from the location of the physical SIM cards but this actually does not matter. All traffic that originates from a SIM card can be routed through a particular base station / GSM gateway. By routing a lot of traffic through a base station, the station can be jammed, thus destroying the service availability.	Y	N
T5	Duration of calls	Duration relates to the number of call minutes; by calling more, the gain will increase. However, it is not possible to call for a whole year. The fraud agents look for weird patterns (that deviate from average/regular patterns) in calling behaviour, e.g. calls that exactly have the same duration. By varying in destination numbers, the offenders try to avoid being under the radar.	Y	N
T6	Number of call transactions	This relates to simultaneous calling with multiple SIM cards from one number (parallel calls), or sequential calling. The tactic to be used depends on the tariff rates of TSP B as well.	Y	N
T7	Technical feature set	A SIM card has a set of features that could limit the possibilities for it to operate in a fraudulent situation. One example of such a feature is call divert. If the SIM card is limited to only divert 7 calls and you need at least 100 calls to be diverted, this particular brand or organisation is not suitable for the fraud scenario. These are particular aspects of a description.	Y	N
T8	TSP B is facilitating the attack	One part of the fraud scenario is facilitated by TSP B, since they make money out of it. This depends on the termination fees, which originate in the regulation parties and change yearly. The termination fees are based on the costs for operating the network.	N	Y
T9	Fair use policy	The construction of the description policy can be a restrictive factor. This could for example limit the usage of multiple SIM cards and therefore change the complete configuration of the fraud scenario.	N	N

TPL = Supported by the TPL language
N=No, Y=Yes.

Table 3.3.: Summary of dynamic features in the cloud case study

ID	Description	Details	TPL
C1	Physical infrastructure	Contains everything one can touch. Servers, switches, the building and rooms.	Y
C2	Virtual infrastructure	The digital (simulated) networks that resemble the cloud	Y
C3	Social organizational	The employees and customers of a cloud provider. What are personal characteristics that describe these people, e.g. their roles, skills and vulnerabilities.	Y
C4	Social-technical	This involves access control, which employee can access what part of the organisation. This includes both the physical and digital infrastructure.	Y
C5	Environmental status	Based on sensors and log files (e.g. CPU load or room temperature), this has very high frequency of updating.	Y

TPL = Supported by the TPL language
N=No, Y=Yes

Table 3.4.: Summary of dynamic features in the ATM case study

ID	Description	Details	TPL
A1	Technical data	The ATM network consists of hardware and software	Y
A2	Social data	Details of the people using the ATM machines and being nearby them. The density of population near an ATM will vary considerably for some areas depending on the time of day, day of week, month and possible also for work/school related seasons (e.g. in Lisbon the holiday vs. non-holiday season since it is a highly touristic location).	Y
A3	Environmental data	Details of the surroundings of the ATM machines.	Y
A4	Criminal dynamics	Details of criminal acts performed at the ATM or nearby.	Y

TPL = Supported by the TPL language
N=No, Y=Yes.

Table 3.5.: Summary of dynamic features

ID	Description	TPL	E3-Fraud	TPL Reference
I1	Technological landscaping	Y	-	Assets (§B.4)
I2	Technological threats	Y	-	Part of the Attack Pattern Library
I3	Social attacks	Y	-	Actors (§B.5) and Roles (§B.6)
I4	Social landscaping	Y	-	Can be modelled with the Attack Pattern Library
I5	Financial landscaping	N	-	Part of regulations, legislations and policy making
I6	Financial attacks	Y	-	Assets (§B.4)
I7	Roles	Y	-	Roles (§B.6)
I8	Individual and cultural characteristics	Y	-	Actors (§B.5) and Roles (§B.6)
I9	Trust relations	Y	-	Part of the attack generation
T1	Number of prepaid SIM cards	Y	Y	Assets (§B.4)
T2	The tariff rates	Y	N	Processes (§B.9)
T3	Number of fraudsters or attackers	Y	Y	Actors (§B.5) and Roles (§B.6)
T4	Location of the fraudster or the attacker	Y	N	Edges (§B.3) and Locations (§B.2)
T5	Duration of calls	Y	N	Can be an input for the analysis
T6	Number of call transactions	Y	N	Processes (§B.9)
T7	Technical feature set	Y	N	Processes (§B.9)
T8	TSP B is facilitating the attack	N	Y	Only model the 'own' organisation.
T9	Fair use policy	N	N	This could be an output of e3fraud.
C1	Physical Infrastructure	Y	-	Edges (§B.3) and Locations (§B.2)
C2	Virtual Infrastructure	Y	-	Edges (§B.3) and Locations (§B.2)
C3	Social organizational	Y	-	Actors (§B.5) and Roles (§B.6)
C4	Social-technical	Y	-	Actors (§B.5), Roles (§B.6) and Policies (§B.8)
C5	Environmental status	Y	-	Processes (§B.9)
A1	Technical data	Y	-	Edges (§B.3), Locations (§B.2) and Processes (§B.9)
A2	Social data	Y	-	Actors (§B.5) and Roles (§B.6), missing people properties
A3	Environmental data	Y	-	This comes from the analysis.
A4	Criminal dynamics	Y	-	Data from external source, this is handled in the analysis.

TPL = Supported by the TPL language
N=No, Y=Yes.

3.2. Discussion

Following the identification of dynamic features and their evaluation with regards to the TPL language, we can conclude that there are only a few of the identified dynamic features that the current version of the TPL language can not accommodate.

We also learned that some of the gaps identified differ in nature, their level of detail and time-scale. The identified gaps are not a problem *per se* because a model is an abstraction of reality anyway. However, a strategy for minimising the consequences of having such gaps could be to collect better data and carry out a sensitivity analysis of the WP3 tools. In addition, the project is already analysing the need for model extensions, for results so far see (The TRESPASS Project, D1.3.2, 2015).

4. Emerging Threats

4.1. Introduction

Background

ENISA produced a cyber threat landscape document, which lists information regarding cyber threats, threat agents and attack vectors (Marinos, 2014). Their report is based on 400 sources from industry, Computer Emergency Response Teams (CERTs), professional associations and academia. The key findings of these reports are summarized by ENISA ínto a threat landscape. In the 2014 report, ENISA discusses the top 15 cyber threats, based on their frequency of occurrence in the reports. Table 4.1 summarizes the findings of the ENISA report.

The ENISA report also discusses the emerging threat landscape. Based on the maturity of threats and the technological developments the following emerging threats are considered.

i) *Cyber Physical Systems* refer to Critical Infrastructure Protection;
ii) *Mobile Computing* relates to the increasing role for mobile devices in the near future. Mobile devices are already increasingly targeted and this trend will keep up;
iii) *Cloud Computing* is another important component of next generation computing that will pose challenges to both users and security experts;
iv) *Trust Infrastructure* is the most vital component of cyber security and interesting for cyber attacks;
v) *Big Data* refers to data sets that are so complex that traditional processing applications are inadequate;
vi) *Internet of Things* is the interconnectivity of devices and smart systems in many sectors.

Research Question

A survey was handed out at the CSP forum conference in Brussels in April 2015. The objective of the survey was to answer the following question: “What is the understanding among security practitioners regarding Socio-Technical Cyber Threats?” Two sub-questions were formulated:
Q1) What is perceived as the biggest threats in Socio-Technical Cyber Security in the past 15 years (i.e. since the year 2000)?
Q2) What are the thoughts on the evolution of Socio-Technical Cyber Security threats in the next 5 years (i.e. 2015-2020)?

Table 4.1.: ENISA Threat landscape. For each threat, a short description is given together with the identified current trend (i.e. an increasing (+), stable or decreasing trend(-)).

Threat	Description	Trend
Worm/Trojan	Malicious programs that have the ability to duplicate and redistribute themselves through email, the corporate network or the Internet	+
Web-based attacks	All attacks that are related to redirecting web browsers to malicious websites where further malware infection takes place	+
Web application attacks - injection attacks	Provide malicious inputs or unexpected sequences in order to cause information breaches	+
Botnets	Infected computers that contain a type of malware that allows an attacker to take control over an infected computer	-
(Distributed) denial of service	An attempt to make a network or resource unavailable to its intended users	+
Spam	Unwanted email messages e.g. containing advertisement	-
Phishing	Deception via email or website with the aim to intercept user names plus passwords and financial credentials	+
Exploit kits	Involves automated tools that detect vulnerabilities in user devices and download related exploits	-
Data breaches	Release of information to an untrusted environment, compromising confidential information	+
Physical damage / theft / loss	Physical devices and identity theft	+
Insider threat	People that attack their organisation of employment with detailed knowledge from the inside	stable
Information leakage	Unintentional or maliciously revelation of valuable personal information	+
Identity theft / fraud	Gathering of user identity information including credentials, profiles, PII and financial details	+
Cyber espionage	APT (Advanced Persistent Threat) and Target Attacks, where the attacker is resourceful	+
Ransomeware / Rogueware / Scareware	Malicious software that demands a pay-off to prevent the destruction of your data	-

4.2. Results

In total 44 participants were approached (and included in the data corpus). Details regarding the participants and the methodology that was used is provided in Appendix C.1.4.

4.2.1. Perceived biggest threats in socio-technical cyber security (i.e. 2000-2015)

Regarding Q1: 'What is perceived as the biggest threats in socio-technical cyber security in the past 15 years (i.e. since the year 2000)?', the participants provided 103 answers (*data items*), 88 of which were unique. To get an impression of the responses given by the participants, a word cloud is generated, refer to Figure 4.1. A Thematic Analysis was used to analyse the data, for details regarding this methodology, refer to Appendix C.1.

Figure 4.1.: Word cloud of survey responses regarding the socio-technical cyber threat themes of the past 15 years (i.e. 2000 - 2015).

The researchers identified 3 main themes: i) What is used by the offender, ii) What makes an attack succeed and iii) The goal of the offender. An overview of all themes is provided in Figure 4.2 and a qualitative description of the themes in Appendix C.2.1.

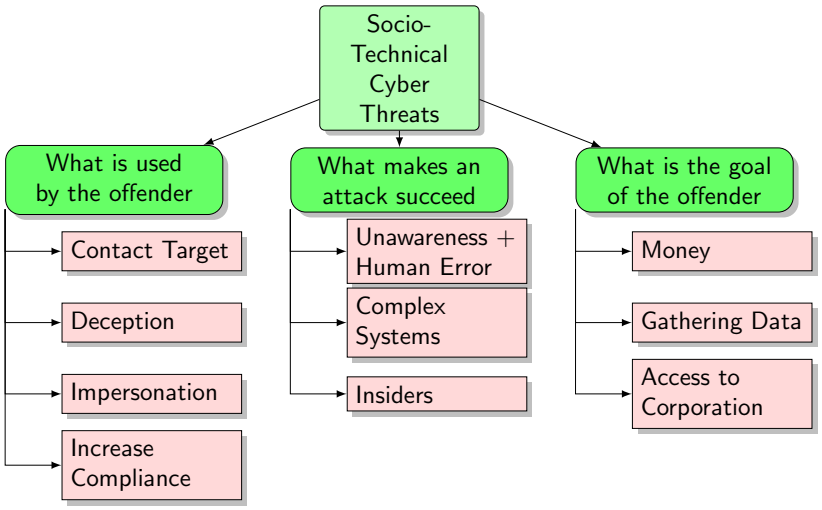

Figure 4.2.: Overview of socio-technical cyber threat themes of the past 15 years (i.e. 2000 - 2015) based on survey.

4.2.2. Perceived future socio-technical cyber threats (i.e. 2015-2020)

Regarding, Q2: How will the socio-technical cyber threats evolve in the next 5 year (i.e. 2015-2020), there were 100 Socio-Technical Cyber Threats (*data items*) reported by the participants, 92 of which were unique entries. To get an impression of the responses given by the participants, a word cloud was generated, refer to Figure 4.3.

Figure 4.3.: Word cloud of survey responses regarding the socio-technical cyber threat themes of the next 5 years (i.e. 2015 - 2020).

The researchers identified 3 main themes: i) Who is involved in an attack, ii) What is beneficial for an offender and iii) What is used in an attack. An overview of all themes is provided in Figure 4.4 and a qualitative description of the themes in Appendix C.2.2.

4.2.3. Comparison of past and future threats.

A comparison is made between the past and future (sub-)themes and is presented in Table 4.2. Themes that describe similar concepts are matched with one another. There is no one-to-one mapping between past and future, since some (sub)theme have changed in size. They are therefore either i) split into separated themes or ii) merged into a more general theme. The remaining themes that are not in the table could not be matched.

4.3. Discussion

This study investigated what the perception is regarding the changes in Socio-Technical Cyber Threats in the future 5 years, compared to the past 15 years.

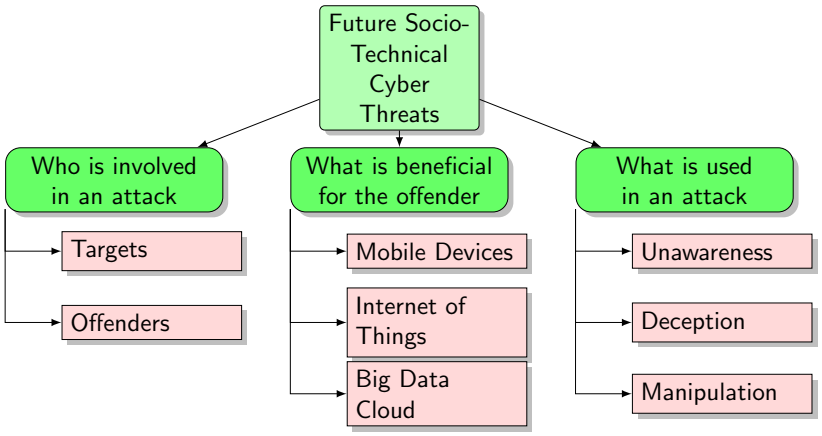

Figure 4.4.: Overview of socio-technical cyber threat themes expected to emerge within the next 5 years (2015 - 2020).

Table 4.2.: Results summary: the themes from the past 15 years that are similar to those for the future 5 years are matched. For each theme the most common threat present in both groups is mentioned.

Past	most common theme	**Future**
(1) Contact target	Phishing emails	(6) Manipulation
(2) Deception	Malware use	(7) Deception
(3) Impersonation	ID theft	(7) Deception
(5) Unawareness + Human error	Unaware users	(8) Unawareness
(7) Insiders	Insider employee	(2) Offenders
(9) Gathering data	Social media	(5) Big Data cloud

This study gives an overview of the thoughts of experts in the field cyber security, being either in industry or academia. The threats that are mentioned, for both past and future, were coded, structured, categorized, grouped into themes and sub-themes. The final result are two theme-trees that resemble the Socio-Technical Cyber Threats of both the past and future.

The results of the two questions that the survey aimed to answer are compared against the results of (Marinos, 2014).

4.3.1. Biggest threats in socio-technical cyber security during the last 15 years (i.e. 2000-2015)

The main survey finding is that the participants discuss three topics:

- 'What is used by the offender'
- 'What makes an attack succeed', and

- 'What is the goal of the offender'.

These results have some similarities with the ENISA report on cyber crime (Marinos, 2014). It must be noted that the scope of ENISA report is on cyber crime in general, whereas the participants were bound to the Socio-Technical context. We next compare each of the resulting sub-themes against the ENISA report, an overview is provided in Table 4.3.

The theme **'What is used by the offender'** has four sub-themes. The first sub-theme 'Contact Target' discusses how the offender approaches the target. It is mentioned that this happens by email (e.g. phishing attack) and by phone (e.g. social engineering attack). This relates both to the 'Spam' and 'Phishing' threat described by ENISA, although the focus is on phishing. The sub-themes Deception, Impersonation and Increase Compliance discuss how the phishing mails are made effective.

The 'Deception' sub-theme discusses four examples: i) fake emails, ii) fake advertisements, iii) fake URLs and iv) USB malware, which all involve getting something one did not expect or asked for. Related to USB malware is the ENISA threat 'malware', which is their number 1 threat in the landscape. In the report a brief description of the functionalities and threats of the malware is discussed. There is no discussion about how this malware is delivered in the first place. However, the distribution of malware is discussed in 'Web-based attacks' and it is stated that the main source of infections are vulnerabilities in the Java framework and browser exploits.

The sub-theme 'Impersonation' discusses how the use of another identity can increase the probability of success in an attack. One of the aspects that discussed by the participants is identity theft in either the digital or physical world. In the ENISA report Identity theft / fraud is discussed, including the collection of PII, financial information / credentials and access codes (Marinos, 2014). The latter part comes back in the 'Gathering Data' sub-theme.

The fourth sub-theme discusses what an offender can use to 'increase compliance'. Among mentioned methods are 'just asking for it', and some of Cialdini's persuasion principles. However, the ENISA threat landscape mainly focusses on the technical threats and not on the social interactions between target and offender.

The second theme **'What makes an attack succeed'** describes what goes 'wrong' on the target side of an attack. This theme contains 3 sub-themes. The first sub-theme 'Unawareness + Human Error' discusses the knowledge shortcomings regarding Socio-Technical Cyber Threats. In the ENISA report, awareness is among those mentioned as one of the ground factors that contribute to new attacks. Furthermore, the report discusses that awareness could help to increase the situational awareness (Marinos, 2014).

The 'Complex Systems' sub-theme relates to usability of systems that hamper the execution of safe-behaviour. This threat is not discussed in the ENISA threat landscape (Marinos, 2014).

The 'insider' threat discussed by the participants relates to both current and former employees who have detailed knowledge of the organisation that will be used to seek vengeance on their (former) employer. ENISA adopted the insider threat after the Snowden revelations and this triggered the investigation into this topic. The report states that a significant

amount of the insider threats are caused by human error, unintentional displacement of information and theft/loss (Marinos, 2014).

The third theme **'What is the goal of an attacker'** discusses what the offender wants to achieve with the attack and it has 3 sub-themes. The sub-theme 'money' refers to financial gain and involves offenders aiming to get access to credit card details or access to bank accounts. In the ENISA report the Ransomeware/Rogueware/Scareware threat refers to this same aim. The difference is that the latter is a technical attack whilst the former is related to as a social threat.

In the third sub-theme 'Gather data' the participants discuss how offenders gather information, as being either i) the goal or ii) the sub-goal of an attack. One aspect involves people putting personal data on mobile devices and those getting sometimes stolen. The threat of stealing devices is discussed in the 'Physical damage/theft/loss' threat of the ENISA 2014 report (Marinos, 2014). The report states that more than 3 million smart phones were stolen in the United States of America. To put the threat into perspective; one third of the device owners does not apply any security controls and about half of the users indicated thay they used their device for business purposes.

The final sub-theme 'Access to Corporation' discusses the flaws in organisations which constitute attacks. This includes awareness, budget, security by design and implementation flaws. This theme is different from the others, since it describes properties of the target / victim, whereas the others describe the offender.

Topics that are in the ENISA report, but are not discussed by the participants include: 'Web application attacks / Injection attacks', 'Botnets', 'Denial of Service', 'Exploit Kits', 'Data Breaches', 'Information leakage' and 'Cyber espionage'.

Table 4.3.: Summary Results

Past	ENISA report
(1) Contact target	Spam + Phishing
(2) Deception	Malware
(3) Impersonation	ID theft
(5) Unawareness + Human error	mentioned
(7) Insiders	Insider threat
(9) Gathering data	ID theft + Physical damage/theft
(4) Increase compliance	-
(6) Complex systems	-
(8) Money	Ransome/Rogue/Scare-ware
(10) Access corporation	-

4.3.2. Future socio-technical cyber security threats (i.e. 2015-2020)

Participants identified three topics:

- 'Who is involved in an attack',
- 'What is beneficial for the offender', and

- 'What is used in an attack'.

These results have some similarities with what is in the emerging threats section in the ENISA reports (Marinos, 2014). It must be noted that the scope of ENISA report is on cyber crime in general, whereas the participants were bound to the Socio-Technical context. Each sub-theme from the results is contrasted against the ENISA report, an overview is provided in Table 4.4.

The theme **'Who is involved in an attack'** has 2 sub-themes. The sub-theme 'targets' discusses who is thought of to be a target in the future. The participants mention 3 possible targets, one of them being SCADA or Cyber Physical Systems. SCADA systems are connected to critical infrastructures and successful attacks cause major impact. In the ENISA report the Cyber Physical Systems and Critical Infra Structure Protection figures as the number 1 emerging treat.

The second sub-theme 'Offenders' discusses who are potentially the future offenders of socio-technical cyber crimes. The participants came up with a list of 5, ranging from individual attackers (e.g. insiders) to nation states attacking other nations. In the ENISA report the offenders are discussed in the overview of threat agents and in the context of cloud computing.

The second theme **'What is beneficial for an offender'** has 3 sub-themes and discusses what can benefit an offender to make an attack successful. The first sub-theme 'Mobile Devices' is focused on the increasing number of small portable mobile devices for everyday use. It is suggested by the participants that mobile devices are becoming an object of increased interest for offenders. This trend is also picked up by ENISA and is ranked second in their emerging threat landscape. The participants and the ENSIA report bear a great resemblance regarding this topic. They both discuss threats involving storing data in the cloud, attacking apps and mobile malware.

The second sub-theme discusses the 'Internet of Things', based on providing all electronics with a network interface, processor and sensors that an intelligent network can be built on. In the ENISA report the Internet of Things is discussed in the perspective of difficulty securing against the growing attack potential in general, whereas the participants discuss threats involving monitoring and surveillance.

The final them, 'Big Data Cloud', describes the data an offender can use prior to the attack. The participants discuss the threat of publicly available data on social media, combining data (dossier effect) including health data and civilian surveillance on the phone and Internet. The ENISA report mentions the similar concerns in the 'Cloud Computing' threat (civilian surveillance, combining information) and 'Big Data' threat (combining data sources) (Marinos, 2014).

The third theme **'What is used in an attack'** has 3 sub-themes and describes some attack mechanisms that are thought to become of interest in the future (i.e. Manipulation, Deception and Unawareness). None of the sub-themes is discussed in the ENISA emerging threats section.

Table 4.4.: Summary results

Future	ENISA report
(1) Targets	Cyber physical systems and Critical infrastructure protection
(2) Offenders	Threat agents for cloud are discussed
(3) Mobile devices	Mobile devices, attacking mobile apps and mobile malware
(4) Internet of Things	Internet of Things has a great attack potential
(5) Big Data cloud	Cloud computing (surveillance) and Big Data (combining data sources)

4.3.3. Comparison between past and future threats (i.e. 2000-2015 vs 2015-2015)

The survey among academics and practitioners seems to suggest that the following is the list of expected changes that will take place in the field of Socio-Technical Cyber Threats during the next 5 years:

- There is more focus on the potential targets of Socio-Technical Cyber Threats in the sub-theme: '*Targets*'. In this sub-theme there is specific focus on SCADA systems and specific social groups. Regarding the past 15 years, there was only mention of insiders; organisations and owners of banking details were not explicitly mentioned.
- There is a sub-theme devoted to the different types of offenders. New potential offenders are the multinationals, government and organised crime whilst only insiders were mentioned as specific offenders involved in the past.
- The participants expect a shift towards mobile devices and smart phones and all related to this (e.g. mobile apps, data storage on mobile devices and cloud storage). This is mentioned in the themes '*What is beneficial for the offender*' and '*What is used in an attack*'. Only phones and email were mentioned as used in the past.
- A whole new category is the '*Internet of Things*', this was not mentioned in the context of Socio-Technical Cyber Threats of the past 15 years. The Internet of Things emerges due to the technical evolution involving making devices smaller and equipping them with processors and network interfaces.
- The sub-theme '*Big Data Cloud*' is to some extent comparable to the sub-theme '*Gather Data*'. A new aspect here is the specific mention of combining data from different sources (e.g. social media, social network or health data).
- '*Unawareness*' of people is a consistent theme. The difference is that in the Socio-Technical Cyber Threats of the future the participants did not mention human error.
- The '*Deception*' theme of the expected future threats relates to obtaining something one did not expect (e.g. someone who impersonates, identity theft or malware infected files). This is a broad theme consists of parts from the '*Deception*' and '*Impersonation*' theme from the Socio-Technical Cyber Threats of the past 15 years.

- The sub-theme '*Manipulation*' is new, although its components were already mentioned in the Socio-Technical Cyber Threats of the past 15 years and can be seen as a combination of '*Contact Targets*' and '*Impersonation*'.

Sub-themes that were only mentioned in the threats of the past 15 years are: '*Increase Compliance*', '*Complex Systems*' and '*Access to organisation*'. The '*Increase Compliance*' sub-theme was a real specific theme that focused on what operational details of an attack were used to make the target comply to a request of the offender. This is based on past experiences and it is almost impossible to come up with something similar for the future. The '*Complex Systems*' sub-theme relates to the ambiguity of security policies and the effort a user has to invest to be secure. One possible reason for the absence of this theme is that the users are by now used to the security policies and act accordingly. Finally, '*Access to an organisation*' was only mentioned in relation to Socio-Technical Cyber Threats of the past 15 years. It is a broad sub-theme involving flaws in an organisation that constitute attacks. The essence of the theme is that there is a need for corporate awareness and budget to reduce the risk of becoming a victim. Although we believe that this will be applicable in the future as well, there was no mention of this in the expected Socio-Technical Cyber Threats of the future 5 years.

4.4. Implication for the TRESPASS model

Regarding whether we envisage challenges for the TRESPASS model regarding the emerging threats identified for the coming 5 years (i.e. 2015-2020), we believe that perhaps the Internet of Things (IoT) would cause the need for a considerable increase in the granularity of the modelling since the IoT implies that for example, a lamp can have an IP address. A similar case is that of mobile devices, since much more assets would have to be modelled.

Regarding what the emerging threats mean for the TPL language, the TPL language is particularly suitable to model BYOD since it can handle mobility and policies. Since the BYOD relies on cloud storage because of the devices' limited storage capacity, the TPL can handle this as it is already being developed for the cloud.

Finally, we acknowledge that this research on emerging threats could have two limitations; namely that i) the participants that answered the questionnaire could be biased, since all participants were picked from one event and that ii) the thematic analysis was performed by only one researcher.

5. Conclusions

The overall objective of Deliverable D.1.3.3, *Dynamic features of socio-technical security models*, is to develop support for dynamic features in socio-technical security models. These features are based on the requirements from the case studies, especially taking into account the results from WP7, based on the validation of the model in the case studies.

The specific objectives of this deliverable are:

- To make an inventory of the dynamic features of the four case studies and evaluate whether the TRE$_S$PASS model can accommodate them, and
- To compare threats from 15 years ago to those predicted for the next 5 years and to identify which of those emerging threats could have implications for the TRE$_S$PASS model.

Regarding the inventory of dynamic features, we found a large range of dynamic features differing in nature, level of detail and time scale. The dynamic features identified for the different case studies occupy different positions along each of these scales.

We identified a few instances of dynamic features that the present version of the TPL model is not able to accomodate. Our view is that the identified gaps are not a problem per se because a model is an abstraction of reality. A strategy to compensate for the identified gaps might involve collecting higher quality data and carrying out a sensitivity analysis of the WP3 tools. In addition, the project is already analysing the need for model extensions, for results so far see (The TRE$_S$PASS Project, D1.3.2, 2015).

Regarding the comparison between past and predicted Socio-Technical Cyber Threats, we found that some past threats don't seem to be regarded as an issue for the future. In addition, we also identified several new threat items; for example with regard to new offender types (e.g. multinationals, government and organised crime) and facilitators (e.g. Internet of Things, big data, cloud). We found commonalities but also some differences with the report of (Marinos, 2014); however, the latter has a slightly different focus.

Finally we discussed whether we envisage challenges for the TRE$_S$PASS model regarding the emerging threats identified for the coming 5 years (i.e. 2015-2020). Our conclusion is that perhaps the clearest example is that of the Internet of Things (IoT), which will probably cause the need for a considerable increase in the granularity of the modelling since the IoT implies that for example, an object such as a lamp can have an IP address. We believe that the TPL language is capable of dealing with emerging threats, e.g. it can model BYOD as it can deal with mobility and policies. Since BYOD relies on cloud storage due to the devices' limited storage capacity, the TPL language is well suited to dealing with these types of emerging threats, as shown by its effective handling of the cloud case study.

References

Armstrong, D., Gosling, A., Weinman, J., & Marteau, T. (1997). The place of inter-rater reliability in qualitative research: An empirical study. *Sociology*, *31*(3), 597-606. doi: 10.1177/0038038597031003015

Bleikertz, S., Vogel, C., & Groß, T. (2014, December). Cloud radar: Near real-time detection of security failures in dynamic virtualized infrastructures. In *Annual computer security applications conference, acsac 2014.* New York, NY, USA: ACM.

Boeije, H. (2009). *Analysis in qualitative research*. SAGE Publications.

Cialdini, R. (2009). *Influence*. HarperCollins.

Cloud Security Alliance. (2010). *Top threats to cloud computing v1.0.* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

Egelman, S., Brush, A. B., & Inkpen, K. M. (2008). Family accounts: a new paradigm for user accounts within the home environment. In *Proceedings of the 2008 acm conference on computer supported cooperative work* (pp. 669–678). New York, NY, USA: ACM. doi: 10.1145/1460563.1460666

ENISA. (2009). *Cloud Computing Risk Assessment* (Tech. Rep.). Author.

Hay, B., Nance, K., & Bishop, M. (2011). Storm Clouds Rising: Security Challenges for IaaS Cloud Computing. In *Proceedings of the 2011 44th hawaii international conference on system sciences* (pp. 1–7). Washington, DC, USA: IEEE Computer Society.

Intel Corporation. (2013). *Dynamic analysis vs. static analysis* (Vol. 2013) (Web Page No. 14 September). Retrieved from http://www.hpc.ut.ee/dokumendid/ics_2013/inspector_xe/documentation/en/help/GUID-E901AB30-1590-4706-94B1-9CD4736D8D2D.htm

Ionita, D., Wieringa, R., Wolos, L., Gordijn, J., & Pieters, W. (2015). Using value models for business risk analysis in e-service networks. In *The practice of enterprise modeling - 8th IFIP WG 8.1 working conference, poem 2015, valencia, spain, november 10-12, 2015. proceedings* (Vol. 235). Springer.

Marinos, L. (2014). *Enisa threat landscape 2014* (Tech. Rep.). ENISA.

McDunnigan, M. (2015). *The difference between dynamic & static web pages.* http://smallbusiness.chron.com/difference-between-dynamic-static-pages-69951.html. Chron.

Mell, P., & Grance, T. (2009a, October). *Effectively and Securely Using the Cloud Computing Paradigm.*

Mell, P., & Grance, T. (2009b, October). *The NIST Definition of Cloud Computing.*

Pieters, W. (2011). Security and privacy in the clouds: a bird's eye view [Technical Report]. In S. Gutwirth, Y. Poullet, P. De Hert, & R. Leenes (Eds.), *Computers, privacy and data protection: an element of choice* (pp. 445–457). Dordrecht: Springer. http://eprints.eemcs.utwente.nl/19837/.

Probst, C. W., & Hunker, J. (2009). The risk of risk analysis—and its relation to the economics of insider threats. In *Proceedings of the 8^{th} annual workshop on the economics of information security (weis 2009).*

Rouse, M. (2015). *Dynamic and static definition* (Vol. 2015) (Web Page No. 14 September). TechTarget. Retrieved from http://searchnetworking.techtarget.com/definition/dynamic-and-static

The TRESPASS Project, D1.3.2. (2015). *Extensibility of socio-technical security models.* (Deliverable D1.3.2)

The TRESPASS Project, D5.1.2. (2015). *Final requirements for process integration.* (Deliverable D5.1.2)

Wikipedia. (2015). *Dynamics (mechanics)* (Vol. 2015) (Web Page No. 14 September). Author. Retrieved from https://en.wikipedia.org/wiki/Dynamics_(mechanics)

A. Project Summary

This chapter gives an overview of the TRESPASS project and its use cases. The section is shared by the public deliverables to provide the necessary background and to put the current deliverable in context.

Information security threats to organisations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Attacks like StuxNet involve technical and human factors, and they damage physical infrastructure. The recent attack on a German steel mill [1] was a combination of both targeted phishing emails and social engineering attacks. The phishing helped the hackers extract information they used to gain access to the plant's office network and then its production systems. As a result, the technical infrastructure of the mill suffered severe damage.

The attack on the German steel mill illustrates that we need to integrate the social and technical aspects of systems in assessing their security - and we need to do so today. Socio-technical systems pose new challenges by combining parts for which we often understand the security issues; the combined system is however much more complex due to interactions between these parts.

The main innovation of the TRESPASS project is the attack navigator, a tool and metaphor that enables defenders to predict and preventing attacks on socio-technical systems. The attack navigator supports current risk-assessment techniques with the TRESPASS process (developed in Work Package WP5), an analytical approach to identifying attacks and evaluating their impact.

The four main stages in the TRESPASS process are *data collection*, *modelling*, *analysis*, and *visualisation*. Data collection (WP2) is vital to understanding the nature of a scenario and providing input to subsequent tasks of modelling, analysis and visualisation. Within the project, the focus has been on collection and analysis of social, technical and physical data and the ways in which these relate to one another. Within each of these domains, different approaches have been taken to provide different viewpoints on the nature of the organisation being investigated.

The models (WP1) developed in TRESPASS can be adapted to the application scenario. We have developed physical modelling techniques in order to understand where further investigation may usefully be targeted. The TRESPASS model describes relevant aspects of the organisation and their connections. To explore contractual and commercial relationships, the e3value method has been adopted.

[1] BBC News, *Hack attack causes 'massive damage" at steel works*, http://www.bbc.com/news/technology-30575104, last visited October 31, 2015.

The analysis methods (WP3) developed in TRESPASS identify attacks in models and identify the most effective controls to prohibit these attacks. The analyses are supported by tools and together they provide the defender with a comprehensive understanding of properties attacks, *e.g.*, cost for the attacker, required skills, or required time.

The innovative visualisations (WP4) developed in TRESPASS focus focus particularly on visualising elements of the analysis, as this is key to the overall project goal of providing "decision support" to practitioners. However, visualisations contribute also to model development and data gathering.

Practitioners can access the TRESPASS toolkit via the attack navigator map interface, which provides an intuitive means of selecting appropriate tools (WP6) for data gathering, modelling, analysis and visualisation. These can be used, individually or in combination, to strengthen operational and strategic decision-making.

A.1. Case Studies

The TRESPASS process and tools are validated by means of case studies (WP7) in the area of cloud infrastructure, telecommunications infrastructure, ATM infrastructure, and an organisation processing privacy sensitive data.

A cloud infrastructure shares infrastructure within or across organisations, giving the cloud services provider and its employees full physical and logical access to all resources across the different consumers. In TRESPASS we formalise typical components in cloud infrastructures as well as human actors and their interrelationships, to identify their contribution to attacks on the organisation.

In telco infrastructure new products need to be launched under significant time pressure, often opening up loopholes for so-called knowledge insiders who know the market very well, trying to make as much monetary gain from the new products as possible. In TRESPASS we model both the infrastructure and contractual relationships to identify physical and monetary attacks.

The ATM infrastructure connects machines that are composed of a money safe and a computer that controls the ATM's devices. There are well protected ATMs installed inside bank branches, while others are deployed in the street and some are not even embedded in a wall. ATM attacks are common and include classic physical attacks and emerging digital attacks. In TRESPASS we model ATM installations, and identify attack likelihoods using geospatial data.

The organisation processing privacy sensitive data develops a system supporting primarily elderly and disabled people in performing online payments and managing their own money from their home. This case study involves from strictly technical security aspects, such as how information is protected while stored or transmitted, to socio-technical security aspects covering security issues arising from the use of and interaction with the technology. In TRESPASS we identify social-engineering and trust-based attacks on such systems.

A.2. Overview of TRESPASS Integration

The TRESPASS workflow involves several stages with various activities, some of which are optional. Figure A.2 shows the architecture diagram and Figure A.1 shows a visual description of the notation used. In practice, stages may not follow a linear order. For example, depending on the goal of the risk assessment, new data requests may be issued later in the process, or automatic updates of data may be supported.

The **Data collection stage** prepares for analysis and modelling steps, and may require the gathering of one or more of the following kinds of data.

Physical data collection provides knowledge about the physical layout of the organization including locations, buildings, rooms, doors, windows, etc.

Digital data collection gathers information about the organization's IT infrastructure.

Social data collection focuses on organisational and individual data, and results in actor profiles containing, *e.g.*, attributes of employees, stakeholders, or potential attackers.

Commercial data collection gathers information required for *e3fraud* analyses, which focus on potential fraud.

Stakeholder goal collection identifies assets and policies the protection of which is critical to one or more stakeholders.

The **model creation stage** handles the creation of the TRESPASS model and associated actor profiles. The e3value model creation process is complementary to the main TRESPASS model, for cases requiring a more specific financial focus:

TRESPASS model creation is a key activity result in a system model that can be further extended and analysed.

- **Components customization (optional)** takes place before or during the TRESPASS model creation to create specialized custom model components.
- **Attacker profile creation** creates the attacker profile that the TRESPASS model analysis should consider, based on ready-made attacker profiles.
- **Defender/target profile creation** creates similar profiles for the other actors in the model based on the social data gathered in the social data collection activity.

e3value model creation This interactive activity involves using the *e3value toolkit* [2] to create business value models. These models structure the commercial information gathered in the data collection stage in a formal way.

In the **analysis stage** different analyses are possible depending on the model chosen. The analysis of the TRESPASS model involves these steps:

1. In the **attacker profile selection**, the user selects the attacker profile to use in the analysis.

[2] http://e3value.few.vu.nl/tools/

2. The **attacker goals creation** provides the attack generation with the attacker goals. These can be derived by hand from the stakeholder goals or deduced automatically from the selected attacker profiles.
3. The **scenario selection** selects a scenario, consisting of a single pair of attacker and attacker goal, to run the TRESPASS analysis on.
4. To extend attack trees, **attack pattern creation and sharing** provides libraries with known attack steps. The attack tree generation can only reach a certain level of abstraction, which may not be sufficient for quantitative analyses.
5. **Attack generation** transforms the TRESPASS model to an attack tree.
6. **Attack tree annotation & augmentation** then extends the attack tree with attack patterns and decorates leaf nodes with parameter values from the data collection stage for quantitative analysis.
7. The **attack tree analyses** compute quantitative properties of attacks, *e.g.*, utility for the attacker or success probability of the attack.

The analysis of the **e3value model** is complementary to the core TRESPASS analysis and has only one step:

1. For the **fraud model generation**, the user needs select an attacker and an interval of expected occurrence rates of the commercial transactions specified by the e3value model. The e3fraud tool then identifies all possible violations of contracts, the loss for actors, and the delta in profit for the other actors.

The **visualisation stage** can be used continuously to provide practitioners with feedback regarding the results of their activities:

1. **Fraud model visualisation** shows the generated attacks as a ranked list of textual descriptions of the attack steps and displays charts showing the profitability for each actor.
2. **Attack tree visualisation** shows the intermediary attack trees.
3. **Attack tree analysis visualisation** visualises analysis results.

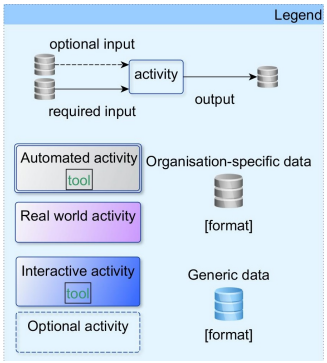

Figure A.1.: Legend for the Integration diagram in Figure A.2.

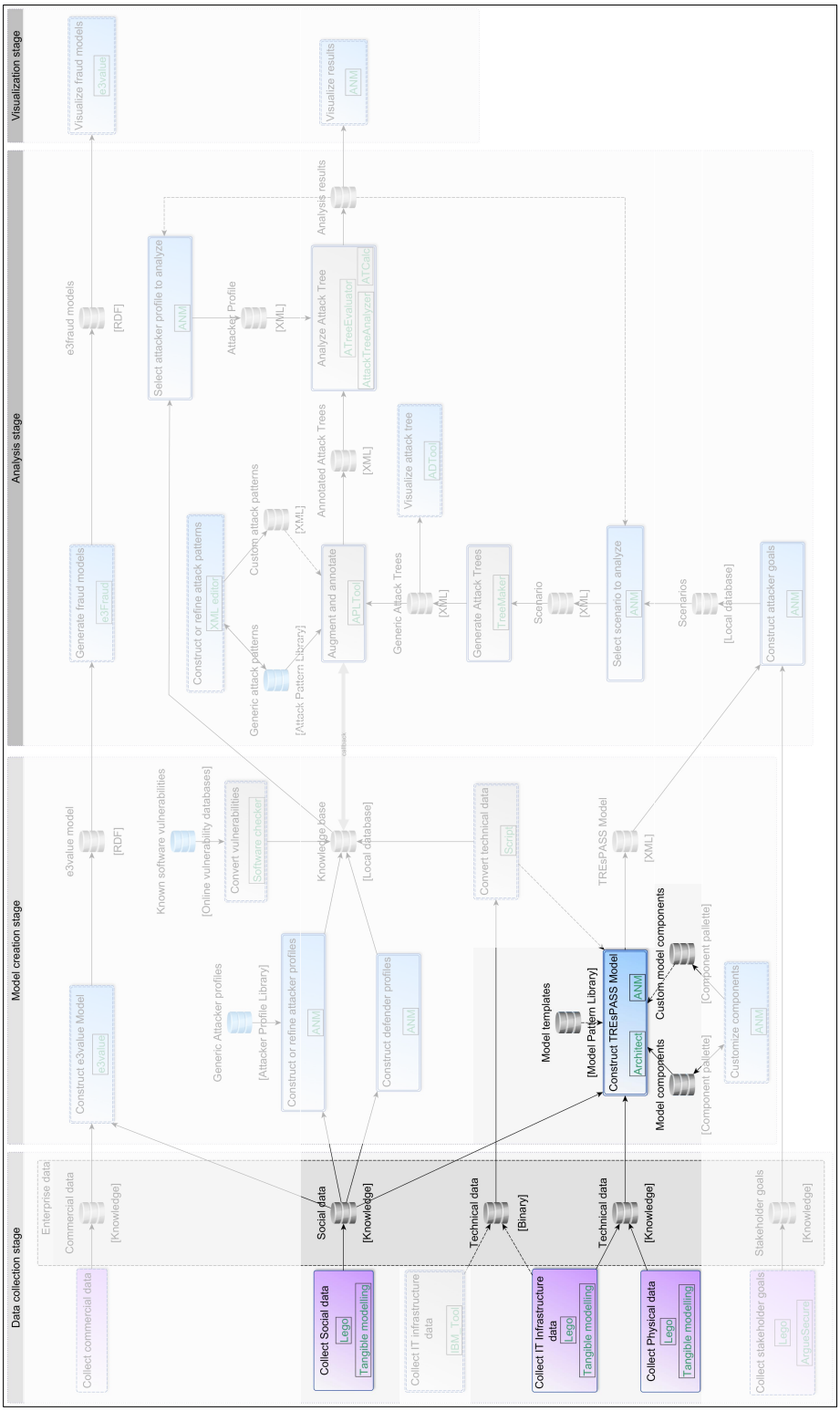

Figure A.2.: Integration diagram for the TRESPASS project.

B. TRESPASS Socio-technical Security Modelling Language (TPL) Summary

This appendix describes the TPL language, which is referred to in the various tables describing the case studies' dynamic features. This language is currently under development so what is presented below does not represent the final language.

The general structure of the model description is the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<system
xmlns="..."
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="..."
author="..."
date="..."
version="...">
<title>...</title>
<locations>...</locations>
<edges>...</edges>
<assets>...</assets>
<actors>...</actors>
<roles>...</roles>
<predicates>...</predicates>
<policies>...</policies>
<processes>...</processes>
</system>
```

B.1. Title

Title is just a string briefly describing the model. For example:

```
<title>IPTV model</title>
```

B.2. Locations

The `<locations>` section describes the locations associated with the model. Each location has an identifier (so that policies can be associated with locations) and a domain. Currently, two types of domains are supported: `physical` and `network`, with the idea that capability to move around in one domain does not automatically mean moving around in

the other (e.g. humans can not move in a network and programs/processes in the physical world). In future, support for location datatypes is also planned.

```
<locations>
    <location id="Home" domain="physical" />
    <location id="Voting_server" domain="network" />
</locations>
```

B.3. Edges

The <edges> section describes existing connections between the locations. Each <edge> will have a <source> and <target>. <source> and <target> may be either an explicitly defined <location> or <item> from the <assets> declarations.

```
<edges>
   <edge>
      <source>home</source>
      <target>city</target>
   </edge>
   <edge>
      <source>PC</source>
      <target>Voting_server</target>
   </edge>
</edges>
```

B.4. Assets

The <assets> section describes the items and data relevant to the model. <item> is something that one can physically have and/or move around, and that possibly has value (chip card, PC, money). <data> represents a piece of knowledge and/or digital asset (PIN, password, cryptographic key, value of a vote, etc.). Computer programs are not typically assets, but rather <processes> running at some items (like PC) or locations (like network servers that one can not physically access).

Assets also have (initial) locations associated with them. These are the places where the assets should "normally" reside. It is neither necessary nor advisable to try to express all the possible locations in the model, since this is the work done by the attack generation procedure, taking into account the <edges> between locations and the respective <policies>. The <atLocations> tag may contain a list of locations separated by whitespaces.

Every asset needs to have a unique id, since there may be various assets with the same name (card, PIN), so the id can be used to distinguish between them. The asset name can in future be interpreted as its type. In general, attribute id is used when a unique object reference is needed, and attribute name is used when different objects may have the same reference.

Example:

```
<assets>
    <item name="Money" id="x001">
        <atLocations>Home</atLocations>
    </item>
    <data name="PIN" id="x009">
        <atLocations>Margrethe card</atLocations>
    </data>
</assets>
```

B.5. Actors

The <actors> section describes the actors relevant to the model. An <actor> may be <atLocations> which is again a whitespace-separated list of locations. And again, this list is meant to be just the initial list of locations (of which there may quite possibly be just one) which the attack generation tool must be able to take care of moving the actors around in the model.

```
<actors>
    <actor id="Margrethe">
        <atLocations>home</atLocations>
    </actor>
    <actor id="Fred">
        <atLocations>city</atLocations>
    </actor>
</actors>
```

B.6. Roles

Many access control policies are actually stated in the terms of roles. To capture that concept, <roles> may also be declared in the TRESPASS model. A role has a unique id and possibly several persons (referenced by <actorID>) fulfilling this role.

Example:

```
<roles>
    <role id="customer">
        <actors>
            <actorID>Margrethe</actorID>
        </actors>
    </role>
    <role id="technician">
        <actors>
            <actorID>Fred</actorID>
            <actorID>Charlie</actorID>
        </actors>
    </role>
</roles>
```

B.7. Predicates

The <predicates> section describes different predicates that hold between the actors. Predicates in TRESPASS are not predefined, so the attack generation will just generate a node stating "Fulfill the predicate ..." and further expansion of this node must come from the Attack Pattern Library.

Example:

```
<predicates>
   <predicate name="trusts">
      <parameterID>Margarethe</parameterID>
      <parameterID>technician</parameterID>
   </predicate>
</predicates>
```

Note that the parameters of a predicate may have different types (Margarethe is an <actor>, whereas technician is a <role>), so attack generation has to take this into account.

B.8. Policies

The <policies> section defines policies that enable certain actions or access to some locations, assuming certain preconditions are met.

A policy consists of three parts: <credentials>, <enabledActions> and <atLocations> declarations. <credentials> describe preconditions that have to be met in order for the policy to allow an action at certain locations. A credential may comprise of one or several of the following:

- be at a certain location,
- be a certain actor,
- have a certain role,
- possess a certain asset (either item ot data),
- fulfil a predicate.

Enabled actions may be one of the following:

- i: input some data,
- o: output some data,
- m: move an actor or a process,
- e: execute a process.

The <atLocations> tag refers to the location where this policy is applied. It is important to understand the difference between the <credLocation> and <atLocations> tags. The former refers to a precondition expressed in the form of being at a location (e.g. in the room that has a door), the latter refers to the actual location of policy enforcement (e.g. the door). It is likely that <atLocations> will often be referring to "virtual" locations that do not correspond directly to our everyday understanding of the term 'location'.

<credItem> and <credPredicate> may have arguments.

<credItem> may have either one or several <credData> or <credItem> instances attached to it. <credData> may either refer to an explicit <value> or <variable>. The degree of recursion required in this context is still subject to ongoing discussion.

Similarly, <credPredicate> may have one or more <argument> tabs which in turn may either contain an explicit <value> (which must refer to a valid id) or a variable.

Variables will be unified by name across different occurrences, and hence provide a way of binding different model components to each other.

Example:

```
<policies>
  <policy>
      <credentials>
          <credLocation id="..."/>
          <credActor id="..."/>
          <credRole id="..."/>
          <credItem name="card">
              <argument>
                  <credData name="pin">
                      <variable>X</variable>
                  </credData>
              </argument>
```

```
            </credItem>
            <credData name="pin">
                <variable>X</variable>
            </credData>
            <credPredicate name="isActor">
                <argument>
                    <value>Margrethe</value>
                </argument>
            </credPredicate>
        </credentials>
        <enabledActions>...</enabledActions>
        <atLocations>...</atLocations>
    </policy>
</policies>
```

B.9. Processes

The <processes> section describes the processes running in the TRESPASS model. A <process> runs at (a) certain location(s). After receiving a <signal> (say, as an output of an action run after a successful policy evaluation) it waits for some <inputs> and after receiving them, gives the corresponding <outputs>.

Example:

```
<processes>
    <process id="Encryption">
        <atLocations>PC</atLocations>
        <signal>
            Encrypt
        </signal>
        <inputs>
            <input datatype="vote">X</input>
            <input>Serv_Pub_Key</input>
            <input>owner</input>
        </inputs>
        <outputs>
            <output>Encrypted_vote</output>
            <output>owner</output>
        </outputs>
    </process>
</processes>
```

C. Emerging Threats

C.1. Method

The survey was handed out at the CSP forum conference in Brussels in April 2015 and was answered by 44 participants.

C.1.1. Participants

The participants attending the CSP-forum conference have a self selection bias, meaning that they all i) have an interest in or ii) are related to cyber security. All participants were employed somewhere in Europe[1] and have between 0 and 20 years of experience in the field of cyber security. The job titles of the participants were divided into 10 categories, refer to Figure C.1. An overview of the industries, in which the participants are active is shown in Figure C.2. In total 70% (31 out of 44) of the participants stated to be familiar with Socio-Technical Cyber Threats.

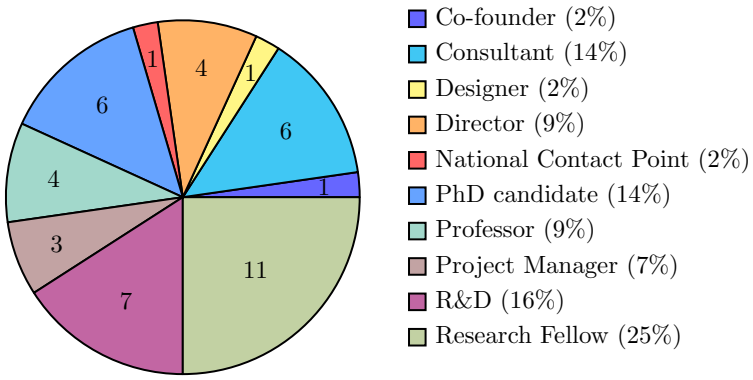

Figure C.1.: participant's job title.

C.1.2. Procedure

The participants at the CSP-forum conference were approached by a researcher from the TRESPASS project and were asked if they would be willing to fill in a short questionnaire.

[1] The participants were employed in: AT, BE, BG, DE, DK, ES, FR, GR, IR, IT, LU, NL, NO, SE, TR and UK.

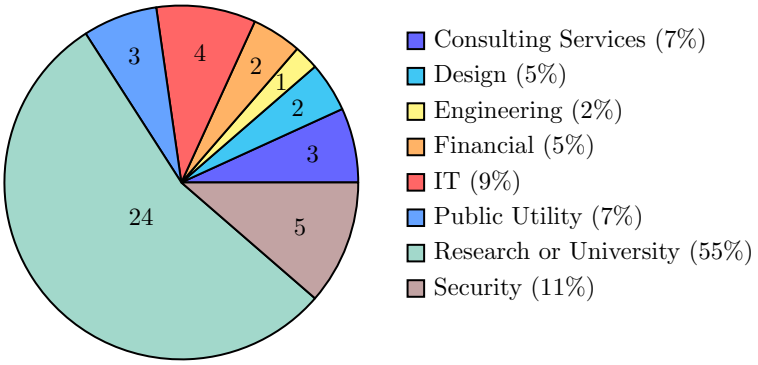

Figure C.2.: Industry in which the participants are employed.

All participants were chosen at random and none of the approached participants refused to help.

Each participant was asked a) to provide some demographic information, b) to state what they perceived as Socio-Technical Cyber Threats in the past 15 years and c) to state how they thought these threats would evolve in the next 5 years. For both past and future, they were asked to provide 3 answers.

C.1.3. Variables

The variables in the analysis were: i) Socio-Technical Cyber Threats from the past and ii) Socio-Technical Cyber Threats of the future. The variables were open questions.

C.1.4. Analysis

The first two questions were answered using Thematic Analysis. The thematic analysis coding system by Boeije consists of 3 steps:
i) '*Open Coding*' is the process of breaking down an item into fragments, examining each fragment, conceptualizing each fragment with a code and categorizing the data. In this stage, no selection of relevance is made. Using open coding contributes to the organisation and structuring of the data. The output of Open Coding is a list of codes and annotations (Boeije, 2009, pp. 96-108).
ii) '*Axial Coding*' or 'focused coding' re-assembles the codes from Open Coding into different categories. A distinction is made between important and less important categories, this process also reduces and organizes the data set, by crossing out or merging synonyms and redundant codes. Axial Coding therefore achieves categorization, such categories to be described and distinctions made between main and sub-categories (Boeije, 2009, pp. 108-115).
iii) '*Selective Coding*' or 're-assembling' finds connections between dominant categories

and makes a model. One possible approach is to define a 'core-concept' which constitutes the heart of the model since such concept appears frequently in the data and other categories are linked to it. Selective coding is the final phase of the research and results in a description of the most important concepts, a coherent story where the relation between the concepts is described and provides the answer to the research question (Boeije, 2009, pp. 115-118).

A snippet of data analysis is presented. One answer from a participant was: "Social manipulation by fake on-line content". In the *Open Coding* phase this was described as: 'Deceptive action', 'Impersonation', 'Obtain information from target', 'Fake content' and 'Scam on website'. In the *Axial Coding* these codes are grouped into categories. 'Deceptive action', 'Impersonation' and 'Fake content' are categorized as 'Deception', whereas 'Obtain information from target' was categorized with similar codes as 'Gathering Data'. In the final phase *Selective Coding* the categories are grouped into themes; Deception is part of the theme 'What is used by the offender' and Gathering Data is part of the theme 'What is the goal of the offender'.

Qualitative analysis is a form of interpretation of data by the researcher and thereby the researcher's view has an important effect on the outcome. The consistency of qualitative results was demonstraated by comparing the work of 6 qualitative researchers (Armstrong, Gosling, Weinman, & Marteau, 1997). The six researchers independently had to analyse a focus group interview transcribed into 13500 words. 5 out of the 6 researchers identified 5 important main themes, whereas 1 researcher identified 4 main themes. Overall, the 6 researchers identified similar themes, but the 'packing' showed different configurations. If the researchers had to independently make a ranking of importance of the themes, they would produce comparable orders. The analysts involved in this study all chose to embed the themes they identified into a wider context of other themes. Such context might have reflected geography, discipline or personal differences in experience or views, but the number of analysts was too limited to draw any definite conclusions. The findings of their study did not produce completely divergent interpretations but a concordance at a level of situating themes within a framework. To conclude, thematic analysis is a qualitative research method that involves the interpretation of researchers. The outcome of the methodology is reproducible among different researchers.

C.2. Results

C.2.1. Perceived biggest threats in socio-technical cyber security (i.e. 2000-2015)

'**What is used by the offender**' is a theme that describes the tricks an offender can use to accomplish the goal of the attack. It consists of 4 sub-themes:

- *Contact Target* describes the method used by the offender to contact the target(s). The participants often mention contact via email messages, either in targeted or

mass form, the former is described in the answer: "*Spear Phishing (Tailored attacks)*". Another method mentioned in the survey is the use of the telephone by the offenders: "*Phone caller requests credit card details*".

Furthermore, the use of dating sites or chat rooms to find and contact targets is also mentioned.

- *Deception* refers to the offender using lies and mystification to make the victim comply. The use of fake emails is most often mentioned as method for the offender to deceive a target; this is described in the answer "*Fake emails*". Related to this are the unwanted email (or phone) messages that advertise products, illustrated by the following answer: "*False publicity email or phone call*". This is also referred to as spam messages, a special category relates to those where the receiver is asked to perform an action, which was found in the following answer: "*Spam emails asking for help*". Furthermore, in the answer: "*Social Manipulation by fake URL or online content*, fake content on websites or spoofed websites are mentioned as the forms of deception used by the offender to make the target comply. Finally, deception by physical objects is also mentioned, such as the horse of Troy. The analogy of malware hidden inside an USB devices and dropped in a place likely to be taken by someone and put in a PC is found in answers referring to this attack: *Dropping USB key (with malware)*".:
- *Impersonation* refers to the offender claiming to be someone else to make the target perceive the story as more convincing. Impersonation is mentioned in different degrees. The easiest way to do this is by simply saying that you are someone else; by selecting the right person to impersonate, the strength of an argument can increase. This can both be done over the telephone or in an email as mentioned in this answer: "*False authority email or phone call*". The second approach is to take over the identity of someone, referred to as "*Identity theft*" or "*profile stealing*". Finally, a ghost identity can easily be created on social media and social networks in order to approach the target; this is illustrated by the answer: "*Persons creating fake identities to intercept user credentials*".
- *Increase Compliance* relates to what an offender can use to increase consent. An offender can use the six persuasion principles to strengthen the argument (Cialdini, 2009): "*Peer pressure*" (also known as conformity) and authority are mentioned as persuasion principles which help to increase the strength of an argument. Furthermore, acting helpless relates to the willingness to help other people, in the survey mentioned as: "*Spam emails asking for help*".

'**What makes an offender succeed**' is a theme that describes what goes 'wrong' on the target side of an attack. It consists of 3 sub-themes:

- *Unawareness + Human Error* mainly relates to either users or employees not being aware of the dangers involving SocioTechnical Cyber Threats "*General unawareness and lack of competence about threats*" or to people that don't know what to do to be safe and secure "*User is not trained (does not know about security)*". This category of unawareness is broader, it also includes the negligence towards security

guidelines e.g. password policies "*Weak Passwords*" or users not paying attention "*User is careless*". Furthermore, users sometimes executed unintended behaviour, referred to in the answer "*Human Error (mistakes)*."

- *Complex Systems* relates to the usability and complexity of systems and the actions which have to be executed to be secure. This issue is referred to in the answer: "*(Security) policy is opaque and disjointed from the end-user*".
- *Insiders* discusses the insider-threat. Insiders have the advantage that they know the structure of the organisation, are familiar with the network and are often trusted by their colleagues. However, former employees that seek for vengeance are even more dangerous, which is illustrated in the answer: "*A revenge of employee that introduces malware*".

'**The goal of the offender**' is concerned with the goal of the attack. This theme includes 3 sub-themes:

- *Money* relates to the financial gain of the offender. Frequently mentioned terms are related to credit cards. A answer that fits perfectly in the context of SocioTechnical Cyber Threats is "*Phone caller requests credit card details*". Besides credit card details, monetary loss is also mentioned by the participants in the answer"*Access to private bank accounts*".
- *Gathering Data* describes either i) the goal or ii) a sub-goal of the attack. Offenders can find information of their targets online, which is mentioned in the answer:

  > "*Use of Social Media (e.g. Facebook) to gain personal information about a user which is subsequently used to impersonate the user or find a better target*."

  Among others, Facebook is a rich source of information, providing all kinds of information, one example of what can be found on Facebook is illustrated in the following answer: "*Information about family obtained from Facebook*". The strength and also weakness of social media relates to the minor restrictions regarding what to post. This can potentially result in malicious use of what the users post online, as described in: "*End-users don't know how their data is used*". In case an offender can not find the information he is looking for, other methods can be used to obtain the information of interest. The ubiquity of mobile devices, acting as personal assistants introduce a new threat, as illustrated in the following answer: "*Everyone putting sensitive information on smartphones, laptops. Those get stolen*". Alternatively, an offender can contact the target in order to obtain the information, either by sending a personalized email, mentioned as "*Spear Phishing (Tailored attacks)*" or by asking, described in "*Social Engineering*".
- *Access to Corporation* relates to the flaws in the organisation that constitute attacks. First, the board must be aware of SocioTechincal Cyber Threats, otherwise this message will never reach the employees; this issue is illustrated in the answer: "*Non-familiarity of employer*". Second, if the board is unaware, it will not grant budget to incorporate security into to the core of the organisation / operation / products; this

issue in mentioned in "*No security by design*". Security by design refers to embedding / planning security early rather than adapting based on attacks, *a priori* rather than *a posteriori*. Finally, even if there is awareness and budget to develop secure products and services, there can be a flaw in the implementation, the latter issue is referred to in the answer: "*PayPal - Data Compromise*".

C.2.2. Perceived future socio-technical cyber threats (i.e. 2015-2020)

'**Who is involved in an attack**' describes the actors who are thought to be involved in future attacks. This theme includes 2 sub-themes:

- *Targets* relates to the individuals or groups that are thought to become a victim of the future socio-technical cyber attacks. The first group of targets that is mentioned are those of the critical infrastructures, more specific the SCADA systems controlling these infrastructures. The STUXNET attack on the Iranian nuclear power plant is a prime example of an attack on SCADA systems. This issue is referred to in the answer: "*Cyber Terrorism on Critical Infrastructure Networks*". Other targets that are mentioned are specific groups or their members. A specific target that is mentioned is the radical feminist protest group FEMEN, as in the following answer: "*Platforms like FEMEN*". The final group of targets that is mentioned are organisations, especially those that are attacked by their own employees, this issue is referred to as: "*Insider attacks*". There are various motivations for insiders to attack, e.g. revenge or financial gain. The danger of insiders is that they often have legitimate access to the computer network, detailed knowledge of the organisation and installed protection mechanisms.
- *Offenders* gives a description of who is thought to be performing the attacks in the future. The participants mentioned 5 types of offenders: i) Insiders are referred to as employees who want to harm the organisation they are working for. The threat of insiders is illustrated by the following answer: "*Internal breach*". Insider threat was also mentioned in the 'Targets' sub-theme, where insiders have a specific target (i.e. their employer). ii) Multinational organisations and product developers can be a threat on a larger scale. For example the implementation of a back-door in one of their products, a similar problem is referred to as: "*Deliberately weakened cryptographic protocols*". iii) Governments have almost unlimited funds to pay for a proper attack. The participants are concerned that the government will spy on their people: "*General Loss of Privacy - Government Access to data*" or that they will actively participate in cyber attacks: "*Government-sponsored cyber-terrorism*". iv) Organized Crime sees the benefits of using socio-technical cyber attacks for their business. It is expected by the participants that organized crime will increase their activities in this area. v) Terrorists aim to cause casualties and damage. It is expected that terrorists will shift towards the cyber sphere and try to cause damage there, which is mentioned in the answer: "*Terrorism*".

'**What is beneficial for an offender**' describes what aspects would allow an offender to have a successful attack. This theme includes 3 sub-themes:

- *Mobile devices* describes the integration of mobile devices into our daily life and the shift of threats towards mobile equivalents. Mobile devices become more integrated into our daily life and it is likely that their role in socio-technical attacks will increase, as mentioned in the following answer: "*Mobile & cloud being used in social technical attacks*". It was mentioned by the participants that is likely that offenders will focus on smart devices as a medium for distributing their attacks, as illustrated by the answer: "*Socio-technical cyber threats through smart phones, smart TV*". Furthermore, the participants think that offenders will find a way to abuse security holes in mobile applications: "*Exploit apps in smartphones*" and they in particular will focus on the social and communication apps: "*Direct messaging apps (e.g., WhatsApp[2] and LINE[3]) as targets*". The mobile phone has evolved from a basic mobile communication device to a sophisticated personal assistant, being able to store a considerable amount of content. Your whole life is summarized in your smart phone, which makes this it a valuable target for offenders. This threat is highlighted in the next answer: "*Continuation of putting data on smart phones*". Besides this, mobile devices contain a considerable amount of personal data, which are combined, interpreted and analysed to guide you through your day. An example is GPS data, your phone 'knows' your everyday commute and informs you about a traffic accident on the route or a nearby petrol station. Answers that relate to this situations are: "*Google Now information*" and "*Increased access to personal and private information collected by smart devices*". A final threat mentioned is "*BYOD*" (Bring Your Own Device), which allows offenders to abuse both the organisational and the private context of their target.
- *Internet of Things* relates to the ability to interconnect almost any electronic device. The Internet of Things will be a reality sooner or later and it results from the integration of a micro processor and a network interface in all electronic devices, highlighted in the following answer: "*The ever greater spread of computer devices*". Smartphones and tablets were already loaded with sensor communication interfaces, now this trend continues with smart-watches communicating with mobile phones, glasses pulling information from the internet and running shoes transmitting the pace to your music player. This is all due to the technical innovations, as described in the answer: "*Fast development of lightweight devices*". As mentioned before, the Internet of Things is an interconnected network of sensors and devices. While we are developing this, are we applying what we have learned in the past from the field of Critical Infrastructure and Industrial Control Systems? Concerns related to the Internet of Things involve monitoring and profiling of people, as illustrated in the following answer: "*Internet of Things in security to surveillance*".
- *Big data cloud* illustrates the data an offender can use prior to the attack. The beauty of the Internet is its richness of information and the fact that everyone can contribute to it. Social media are used to share experiences with friends, family and

[2] https://www.whatsapp.com
[3] http://line.me

the rest of the world. This information can be used by offenders in an attack, for example: "*Tweet data*". Other threats related to data mining such as the dossier-effect, combining data-sources, highlighted by the following answer: "*Big-data used for massive info on users*". Furthermore, for hospital automation it is of great value to have digital health records. However, this introduces a new threat of offenders trying to query these databases, as illustrated in the answer "*Access to Health data*". The legislations for ISPs relating to the storing of internet traffic and phone call data will cause the internet to become BigBrother, as described in the answer "*Surveillance and behavioural tracking of internet users*".

'**What is used in an attack**' describes attack methods. This theme includes 3 sub-themes:

- *Unawareness* illustrates that unfamiliarity is still an issue and that this is an important factor that an offender can misuse. The participants in the survey expect that the awareness regarding Socio-Technical Cyber Threats will be a problem in the future. For example, the awareness of this kind of threats in organisations is illustrated in the answer "*Non-familiarity of employees*". Detection of being targeted is one of the most important factors that makes a difference in becoming a victim. Awareness is a process that needs continued attention by a broad audience, hence the following answer: "*Public education on this subject doesn't seem sufficient today*".
- *Deception* discusses the trickery offenders use to perform their attacks. The participants mention impersonation as a socio-technical cyber threat. By using impersonation, the offender claims to be someone else. Impersonation is used in different Socio-Technical Cyber Threats (e.g. social engineering and spear phishing). The next step is taking over someone's complete identity. This can be done in both the digital and the physical sphere, referred to in the answers "*Profile stealing*" and "*Identity theft*" respectively. Online profiles are traditionally protected with a user name and password combination. Passwords are therefore of interest to the offenders (e.g. social engineers and phishers). Humans are creatures of habit, it is likely that for multiple online accounts, the passwords are highly similar. This threat is illustrated by the following answer: "*Same password (i.e. too many passwords)*". Furthermore, the participants are concerned that after a socio-technical attack the offender installs malicious software that can be used either directly or at a later point in time. Trojan horses could be used to install "*Malware*" or "*Ransomware*" on devices in their network. Besides the PCs and laptops in an organisation, the participants are also concerned that the offenders will go after mobile devices as well, this is illustrated by the following answer: "*Trojan programs inside connected devices*".
- *Manipulation* describes the type of attacks a socio-technical offender can use to achieve the objective. The participants expect that offenders will use phishing, social engineering and fake content in their attack. The phishing attacks will be focused on specific targets, as mentioned by this answer: "*More advanced targeted phishing*". Furthermore, the participants mention that there will be "*Email Scams*" and that "*Fake messages shift to mobile platforms*". Regarding social engineering, it is argued by one of the participants that this will be used to commit identity theft: "*Identity theft based on social engineering*".