predict
prioritise
prevent

TREsPASS

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

Deliverable D6.4.2

TREsPASS tools handbook

Project:	TREsPASS
Project Number:	ICT-318003
Deliverable:	D6.4.2
Title:	TREsPASS tools handbook
Version:	2.0
Confidentiality:	Public
Editor:	M. Martins, itrust consulting
Cont. Authors:	A. McKinnon, B. Jager
Date:	2015/10/30

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

Document History

Authors		
Partner	**Name**	**Chapters**
ITR	Alex McKinnon	1-4
ITR	Benoît Jager	1-4
ITR	Miguel Martins	1-4

Quality assurance		
Role	**Name**	**Date**
Editor	Miguel Martins	2015-10-30
Reviewer	Zaruhi Aslanyan	2015-10-15
Reviewer	Frederic Brodbeck,	2015-10-02
Coordinator	Pieter Hartel	2015-10-30
WP leader	Miguel Martins	2015-10-30
Task leader	Miguel Martins	2015-10-30

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

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

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

Management Summary

Key takeaways:

- This document is guide for the possible interactions with the TREsPASS platform from the administration point of view. It is made available to the interested parties.

This document is the TREsPASS tools handbook. This purpose of this document is to act as a manual for integration, deployment and maintenance of the tools platform. It describes the features that are available for users and administrators and how administrators can perform their tasks.

According to the project Description of Work, Deliverable D6.4.3 (TREsPASS deployment and maintenance plan) due in M48 will contain a revised version of the present (D6.4.2) deliverable.

Table of Contents

List of Figures

1 Introduction

Appendix A provides the context for this deliverable in the TRES PASS project. It describes the overall summary of the project and the TRES PASS workflow.

1.1 Goals

This document serves the following purposes:

- Manual for integration: The integration of new tools, both on the user interface and on the software server, is described
- Manual for deployment: On the one hand we describe how tools are made available for internal purposes and, on the other hand, how the entire platform is used in consultancy missions after the project.
- Manual for maintenance: The maintenance of the platform consists of keeping up-to-date software packages, applying bug fixes to the platform and individual tools, and the execution of functional tests after maintenance operations.

1.2 Foreground and background

The content of this document is foreground of TREsPASS.

1.3 Structure of the document

The remaining of this document is structured as follows. Chapter 2 is a guide for the TREsPASS platform and chapter 3 describes the integration and deployment of the TREsPASS platform.

2 Guide for the TREsPASS platform

2.1 General description

The TREsPASS platform is an environment where the tools developed within the project can be viewed and executed. The platform is available 24/7, except during short maintenance periods. For the detailed description of each tool, its capabilities and limitations, the user is advised to refer to the documentation produced by the respective work package/publisher.

The platform and most of its tools are not mature enough to be used in a real scenario with huge sets of data or requiring significant processing power. The platform shall only be used for the prototypes in the scope of the project.

The following tools, grouped by publisher and in no specific order, are included in the platform:

itrust consulting:

- TRICK Service: Trick service assesses quantitative risks and fulfils risk treatment operations according to the user-configured referential standards (ISO 27001, 27002, etc.). It outputs the risk treatment plan which prioritises the implementation of security measures according to their Return On Security Investment (ROSI), risk specificities and feasibility.
- Software Checker: Determines if specific software versions contain any public vulnerabilities indexed by reliable databases such as CVE (http://nvd.nist.gov/).

Cybernetica:

- AttackTreeAnalyzer: The attack tree computation tool can be used to calculate optimal attack vector (from the attacker point of view) taking attacker profile into account.
- Converter: This converter is used to convert the output format of the TREsPASS model (XML) into the input format understandable by the ApproxTree+ tool.
- Failure-free Model: This tool is able to assess if a system is secure against rational gain-oriented attackers. It takes an attack tree (with parameters for atomic actions) as the input.
- Attack Pattern Library (APL): The Attack Pattern Library (APL) is intended to promote the reuse of modular elements to improve the process of model development.

University of Luxembourg:

- ADTool: The Attack-Defense Tree Tool (ADTool) allows users to model and analyse attack-defense scenarios represented with attack-defense trees and attack-defense terms. It supports the methodology developed within the ATREES project.

T. University of Denmark:

- Model: This tool generates an attack tree in the XML format that can be used for analyses, visualisation, and for the TREsPASS process. It takes as input the model file.
- Treemaker: This tool generates an attack tree in the XML format that can be used for analyses, visualisation, and for the TREsPASS process. It takes as input the description of the model in XML format.
- ATree Evaluator: Computes the Pareto set of pairs with maximum probability and minimum cost, if costs are provided. The tool addresses multi-parameter optimisation of attack trees in terms of Pareto efficiency.

GMV Portugal:

- RawDataProcessing: The Raw Data Converter tool is composed of a number of modules. The goal of these modules is to become the root of a general tool which converts raw data from several data sources into Trespass input data (WP1 input data).

University of Twente:

- ATCalc: ATCalc is a tool for efficient Attack Tree Analysis. It computes the system unreliability for each mission time, i.e. the probability that the system fails within the mission time. Further it is capable of computing the mean time to failure (MTTF), i.e. the expected time that the system will fail. ATCalc uses CADP, a proprietary software owned by Inria.
- Arg. Spreadsheets: An Excel-based tool which supports documenting the structured arguments and defensibility relationships elicited as part of an informal argumentation game. In addition it recursively computes argument states and tags arguments with the components or assets they refer to.
- RDFparser: A small Java tool which acts as an extension to the e3value toolkit. It takes as input (.rdf) e3value models and outputs profitability graphs based on selected parameters.

BiZZdesign:

- Architect: Architect is a leading software tool for Enterprise Architecture. Architect is compliant with ArchiMate and TOGAF, the open standards for Enterprise Architecture, maintained by The Open Group. The access to Architect is through RDP (natively supported on Windows, MRD for Mac, Remmina on Linux).

2.2 Installation

2.2.1 Creating an account

In order to gain access to the TREsPASS integration platform, users are permitted to register at the following address: http://trespass.itrust.lu.

Figure 1: TREsPASS platform login screen

By clicking on the “Sign up” button (highlighted in Figure 1) users will be taken to the registration screen shown in Figure 2.

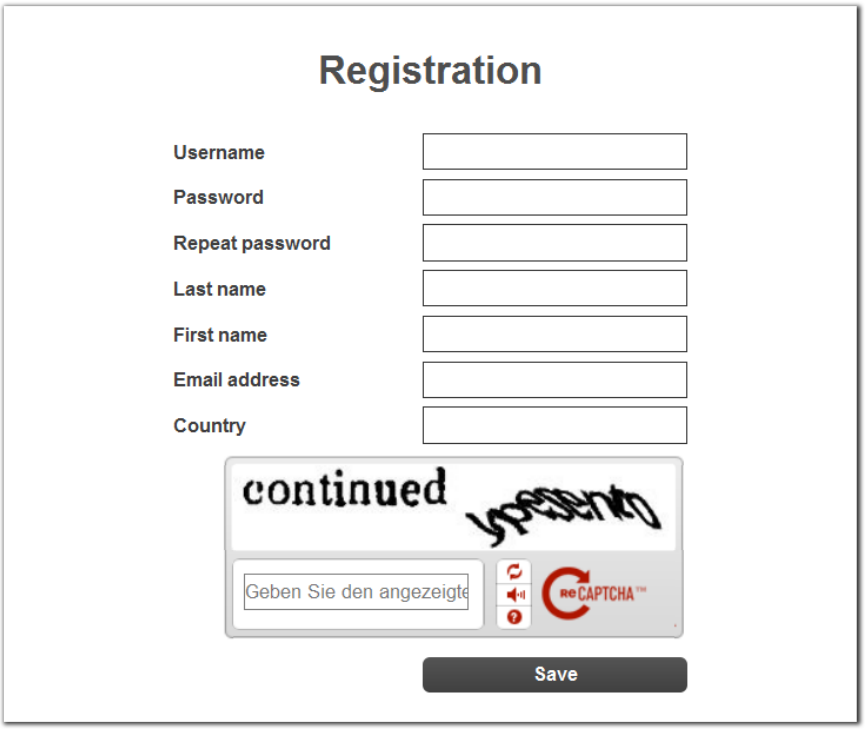

Figure 2: Registration screen

All of the following fields shown in Figure 2 must be correctly completed in order to create an account. Once the user has filled in all fields, they should click on the “Save” button to create an account.

Once an Administrator has validated the request for an account, a confirmation containing a web link will be sent to the email address provided by the user. To complete the registration process, the user must click on this link which will forward them to the log in page. The user can then enter their credentials to gain access to the TREsPASS platform.

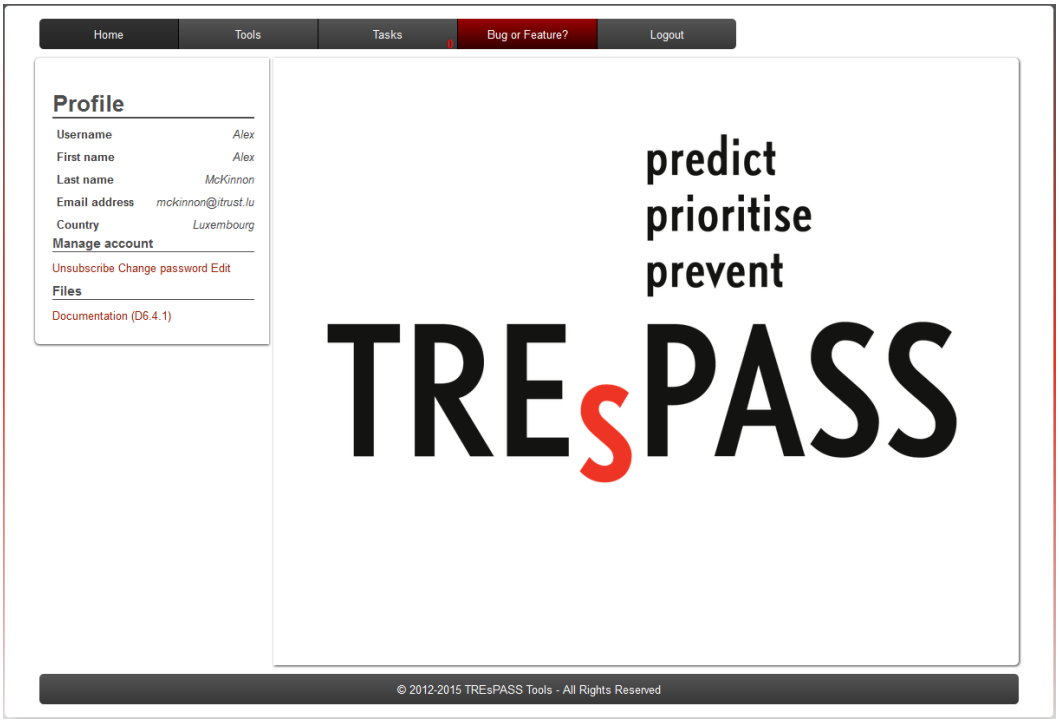

Figure 3: TREsPASS platform home page

2.2.2 Migration of the TREsPASS platform to a virtual machine

The TREsPASS platform is envisaged as a set of tools to be used by an operator in client's premises, with real data from the organisation. This data is likely to be confidential and according to security policies operators are not allowed to send data to an external server, or even to connect a network cable.

Based on this, most of the tools can be packed in a virtual machine that is able to run on a laptop and be used without any network connection. Tools that are hosted on external servers cannot be integrated. Its use in a real scenario is subject to a special authorisation by the organisation that is being investigated.

The virtual machine will be provided as the final deliverable of this task.

2.3 Configuration

2.3.1 Management interface (Admin view)

The figure below shows the TREsPASS platform home page, as seen by an Administrator.

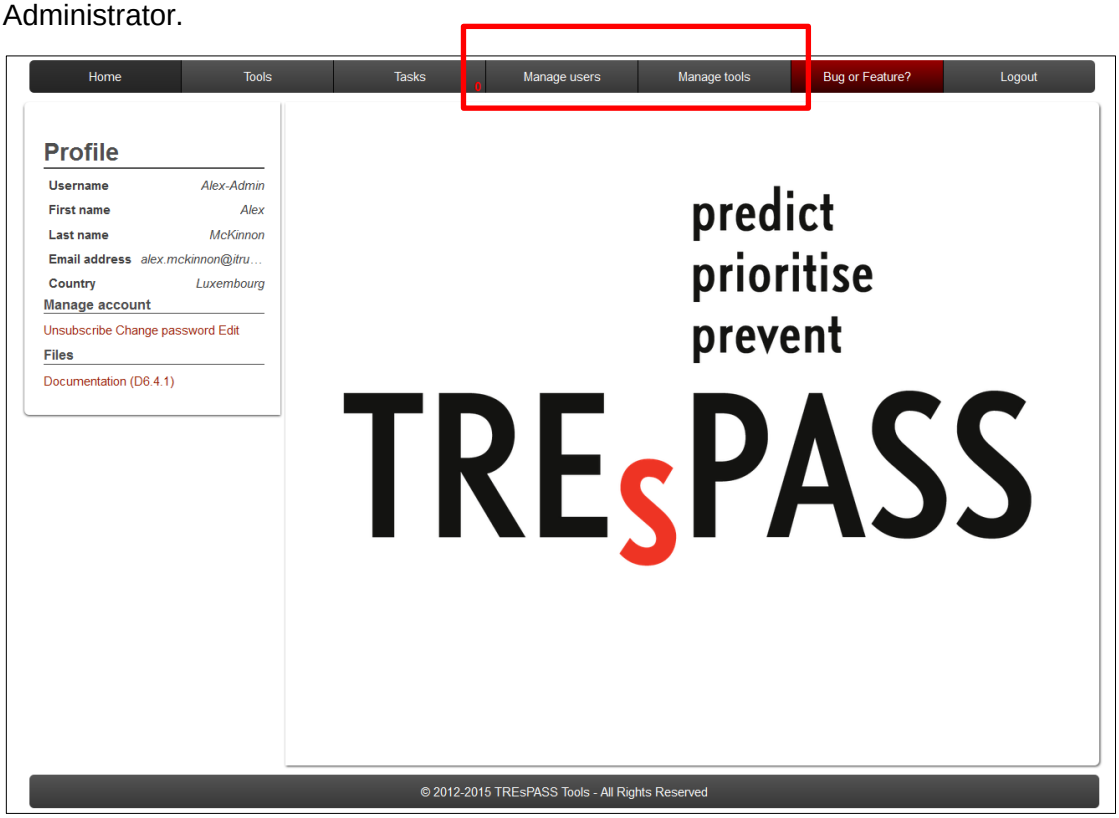

Figure 4: TREsPASS platform home page (Administrator view)

In addition to the regular features that are available to all users, Administrators have access to the following additional features, highlighted in the figure above and described in the following sub-chapters.

2.3.2 Manage users

This page allows Administrators to manage the registered users of the TREsPASS platform. Here, Administrators are able to see the details of all users who are currently registered, modify their access rights or even remove (delete) user accounts.

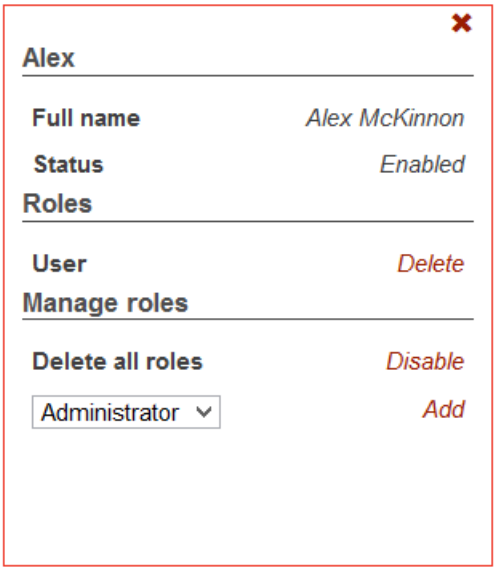

Figure 5: Example user

Users can be assigned the following roles:

- User: is able to use tools, create and use his own toolchains and use global toolchains;
- Administrator: on top of the user role, it is able to manage users, manager tools and manage global toolchains.

2.3.3 Manage tools

On this page, Administrators are able to add, delete and modify tools. We distinguish tools and applications. **Tools** can run:

- on a server managed by itrust (those we call **applications**);
- on an external server and we provide a link to access it;
- on the client's browser and we provide a link to access it.

To add a new tool, the Administrator should select the option from the "Manager" (Figure 7) on the left hand side of the screen.

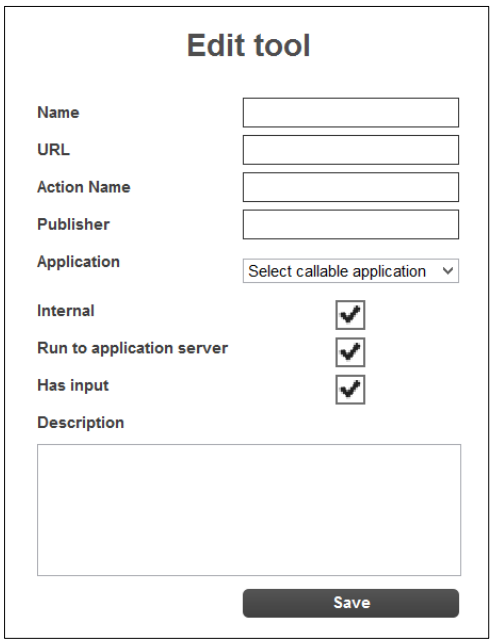

Figure 6: Adding new tool

The administrator provides the following fields:

- Name: The name as shown on the website;
- URL: The link to the tool, either to the internal or to an external server;
- Action Name: The tooltip when hovering the action button (Run it, Go, etc.);
- Publisher: The name of the partner responsible for the development of the tool;
- Application: The name of the application, if it is run on the internal server;
- Internal: If the tool is internal;
- Run on application server: If the tool is run on the internal application server;
- Has input: If the tool receives an input file from a standard upload page.

After setting the configuration, the administrator has to “Push new config” which allows them to push the new configuration to the server.

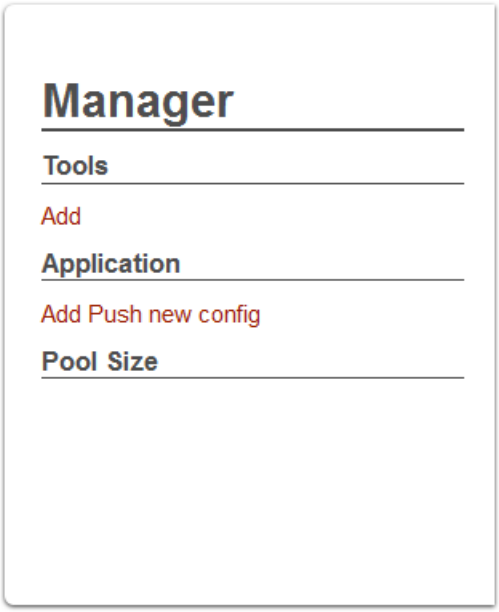

Figure 7: Tool "Manager"

The following information is displayed (Figure 8) for each tool in the TREsPASS platform:

- Path: the path to the executable to be run relative to the root of the tools
- Output file: the name of the main output file
- Required RAM size: the memory needs of the tool to limit the number of simultaneous applications (non-implemented as not needed)
- Required directory: Needs to be selected if the same application is run multiple times to avoid different instances of the same file to be mixed.
- Read from standard out: In case the output of a program is printed to the standard out buffer and not to a file.

For each tool already in the platform, the administrator has the following options:

1. Edit tool: The form for adding a new tool is shown with the data filled in for editing.
2. Delete tool: The tool is deleted from the interface

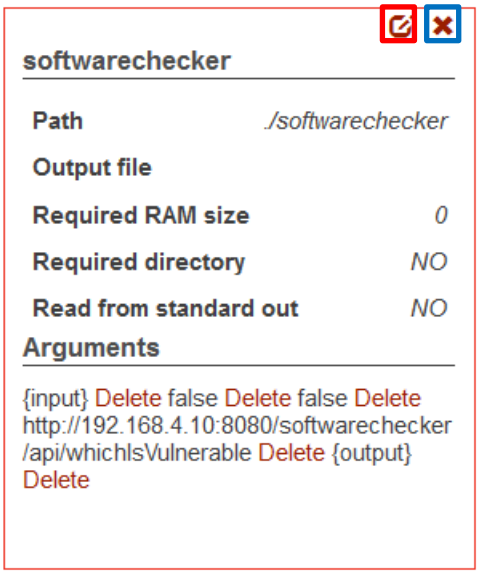

Figure 8: Tool information

Clicking on the Edit tool button allows the Administrator to edit the parameters shown in the figure below.

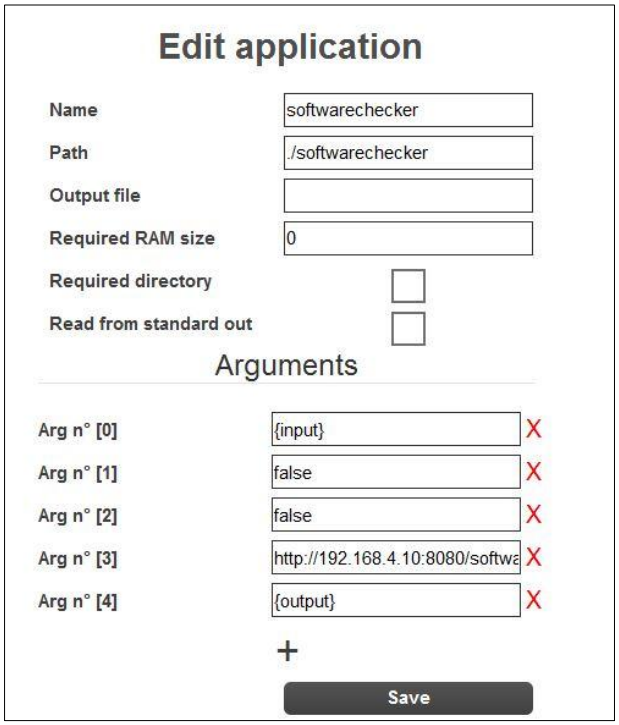

Figure 9: Tool editing screen

2.4 Additional features

In the following sub chapters we describe several other features in place to assist the development and the use of the TREsPASS tools.

2.4.1 Bug and feature tracker

In major collaborative software development projects it is valuable to have a tool to request features and report bugs. An instance of the open-source Redmine tool (www.redmine.org) dedicated to TREsPASS has therefore been configured. Once users have created an account, they can use it to request new features, make suggestions for improvement, or report bugs.

The tool is available at http://trespass-ticket.itrust.lu. There is a link to the tool in the main menu of the application. The tool can also be accessed from login/signup page, so that user can report login/signup problems.

2.4.2 Software versioning

Software versioning solutions (Git, SVN) are included for the development of any individual tools. The purpose of this software versioning function is to:

- allow the collaborative development of the TREsPASS tools;
- allow partners to test their tools on the central platform without needing to ask the integration team to update a binary, dependencies, etc.;
- allow partners to keep their tools up-to-date, add new features, functionalities, etc.

The SVN repository is available at http://trespass-svn.itrust.lu.

2.4.3 Security

The following security elements are included in the TREsPASS platform:

- Access control: TREsPASS tools are only available to authorised users. Users with a valid account are required to create an account and log in with individual credentials before gaining access to any of the tools. Minimum username and password lengths have been defined at 4 and 8 characters, respectively.
- CAPTCHA: In order to prevent attacks from robots, a CAPTCHA system (Completely Automated Public Turing test to tell Computers and Humans Apart) has been applied to the registration form.
- Encryption: All communications between the user's computer and the front-end TREsPASS server are encrypted using HTTPS (SSL/TLS) technology. This prevents the disclosure of access credentials when the server is accessed through insecure networks.

3 Integration and deployment of the TREsPASS platform

3.1 Integration

New tools can be easily integrated. The procedure is slightly different depending on the platform that executes the tool:

- on a server managed by itrust: the application has to be installed before adding the tool.
- on an external server: a link to the external server is provided
- on the client's browser: the tool is provided. Often the tool is written in Java and the jar file is provided. We can define the jnlp file with signature so the client's browser can recognise the tool as trustworthy. Visualisation tools are mainly Javascript web apps that also run in the browser, but these do not need signature.

3.2 Acceptance testing

Functional tests are executed by the administrators and by the tool developers to check that the tool is working as expected.

3.3 Security testing

Regular security tests are applied to the TREsPASS platform.

3.4 Maintenance

The maintenance of the platform consists of keeping up-to-date software packages, applying bug fixes to the platform and individual tools, and the execution of functional tests after maintenance operations. The update and upgrade of the operating system is achieved simply by running standard commands: `# apt-get update && apt-get upgrade`

4 Conclusion

This document is the TREsPASS tools handbook. This purpose of this document is to act as a manual for integration, deployment and maintenance of the tools platform. It describes the features that are available for users and administrators and how administrators can perform their tasks.

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.

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 particularly on visualising elements of the analysis, as this is key to the overall project goal of

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

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 10 shows the architecture diagram and Figure 11 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.

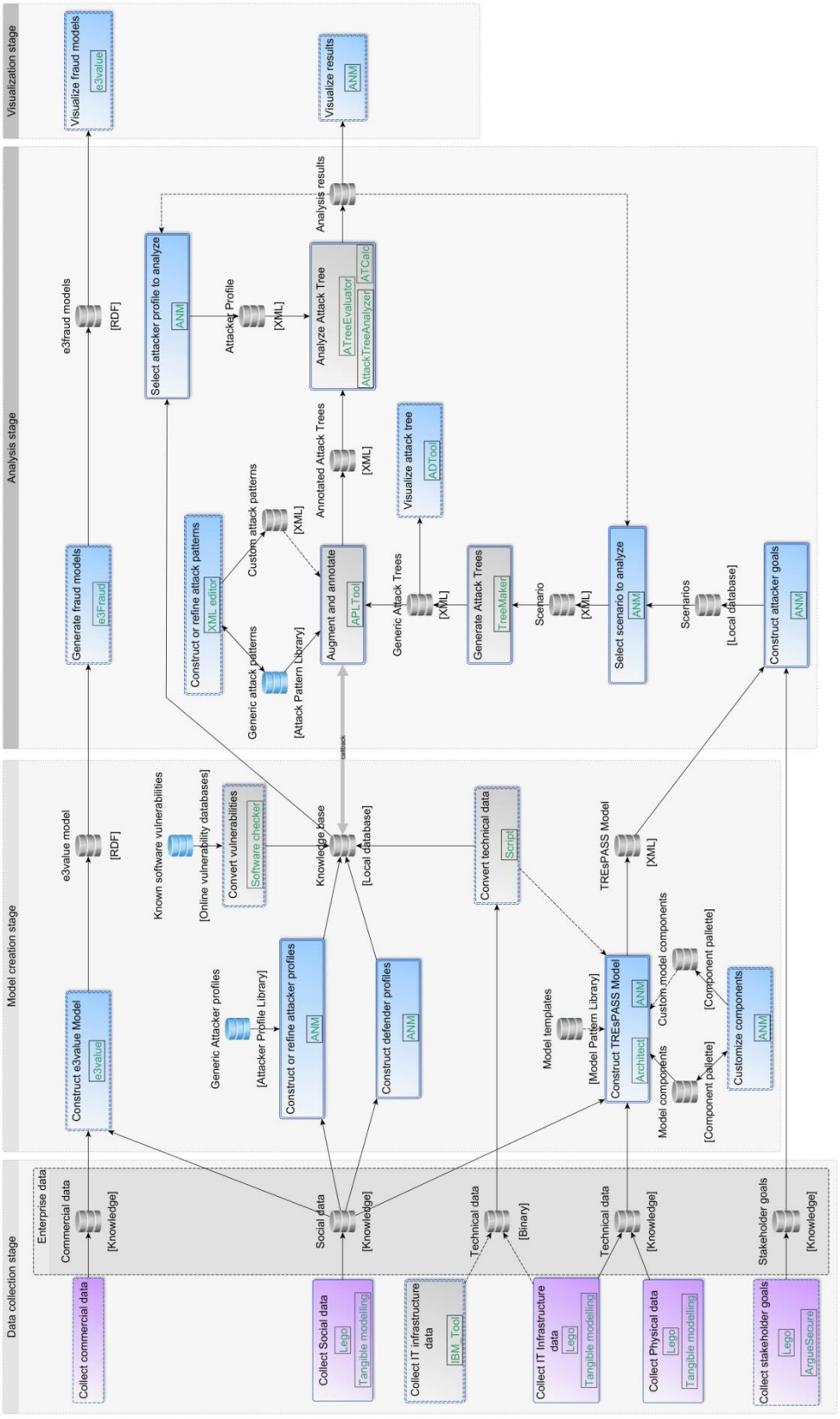

Figure 10: Integration diagram for the TRES PASS project.

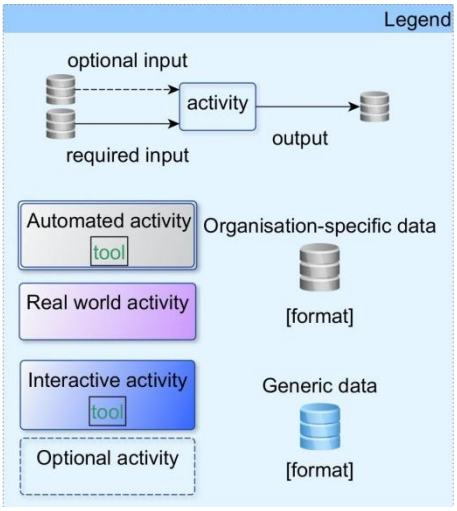

Figure 11: Legend for the Integration diagram

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 *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. 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:

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.

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