TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Business Information Technology

Department of Informatics

Chair of Information Systems

Assessment of integration possibilities of the TREsPASS toolset into the ISKE Tool.

Bachelor's Thesis

Student: Jelena Plehhanova

Student kood: 073757IABB

Supervisor: Aleksandr Lenin, M.Sc.

Tallinn

2015

Hereby I declare that I am the sole author of this thesis. The work is original and has not been submitted for any degree or diploma at any other university. I further declare that the material obtained from other sources has been duly acknowledged in the thesis.

……………………………………. ………………………………

(*date)* *(signature)*

Table of Contents

ANNOTATION

The thesis consists of 43 pages with 22 figures and 2 tables.

The topic of the thesis is „Assesment of integration possibilities of the TREsPASS toolset into ISKE Tool". The main purpose is to research possibility of integration, comparing and analysing TREsPASS and ISKE Tool components.

The work consists of introduction, 3 chapters, conclusion and list of references. In the work are depicted: ISKE Tool screenshots, figures made by myself with the help of Microsoft Visio 2010 and figures of TREsPASS project review demo from presentation Brussels 2014.

For solving this task I should to study the ISKE Tool and the TREsPASS toolset and compare data these systems contain. As the result I detect that such data like processes and policies cannot be provided on such level of detalization, which is required by the TREsPASS toolset. Attacker Profile is missing in ISKE Tool. From Libraries we can get policies and processes, but they should be created by experts. Attacker Profile can be made by user.

The result of the thesis I assume that integration requires more effort and creation of additional external components.

ANNOTATSIOON

Bakalaureusetöö koosneb 43 leheküljest, töös on illustreeriva materjalina kasutatud 22 joonist ja 2 tabelit.

Bakalaureusetöö teema on „TREsPASS rakendustööriistade integreerimise võimaluste hindamine ISKE rakendustööriistasse“. Töö eesmärgiks on uurida integratsiooni võimalusi, võrreldes ja analüüsides TREsPASS rakendustööriistade ja ISKE rakendustööriista osi.

Töö koosneb sissejuhatusest, kolmest peatükist, kokkuvõttest ja kasutatud kirjanduse loetelust. Töös on kujutatud: ISKE rakendustööriista ekraanipiltide visandid, ise tehtud kujundid Microsoft Visio 2010 programmis ning kasutatud TREsPASS projekti demo kujundeid Brusseli presentatsioonist 2014 a.

Et minu problemi lahendada ma õppisin ISKE rakendustööriista ja TREsPASS rakendustööriistud ja võrdlesin milliseid andmeid need sisaldavad. Tulemisena ma identifitseerisin, et sellised andmed nagu protsessid ja poliitikad ei saa esitada sellises detailses tasemes, nagu vajab TREsPASS rakendustööriist. Ründaja Profiil puudub ISKE rakendustööriistas. Me võime võtta poliitikad ja protsessid Raamatukogudest, aga eksperdid peaksid need Raamatukogud tegema. Kasutaja võib iseseisvalt teha Ründaja Profiili.

Minu töö tulemuses ma arvan, et selline integreerimine nõuab rohkem pingutust ja on vaja luua täiendavat väliseid komponente.

ACKNOWLEDGEMENT

The material used in this thesis is part of the EU FP7 project TREsPASS (ICT-318003). This thesis contains only the author views and the Union is not liable for any use that may be made of the information contained herein.

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Many times ago computers fixedly came in our life. They fundamentally changed the world around us and the opportunity of people. Always computer is with us: at work, at home, in a trip.

It is impossible to assure a stabilized work of the computer and safety of your data without good security of the system against attacks. At the moment protection against virus attacks is probably a very important task in computer industry. Damage from computer virus attacks can be very significant. Antivirus programs and security risk analysis tools can be used to analyze the security of the system and deploy defensive measures in a rational way.

TREsPASS project is trying to create security risk analysis system. But any scientific achievement has a valuation only when it can be verified in practice. Accordingly, one of the most interesting tasks for research is how we can apply this security risk analysis system in Estonia. In our country we have such standard like ISKE, which corresponding ISKE Tool. ISKE is an informational security standard that is developed for the Estonian public sector. For example for such system like E-Health [5] and also such systems like SAP, Lotus Notes. Accordingly, all public sectors should use ISKE Tool I offer to research these integration possibilities. I suppose TREsPASS analysis system from the socio-technical perspective is useful supplement in ISKE Tool. In this thesis I do not regard ISKE Tool like standalone program, but like placeholder for integration analysis system.

In this thesis I research assesment of integration possibilities of the TREsPASS toolset into ISKE Tool. Is this integration possible. What is for integration needed.

Tasks of this thesis are:

1. To learn TREsPASS project and it’s developed system architecture.
2. To learn ISKE Tool.
3. To assess integration possibilities of TREsPASS toolset as plugin into ISKE Tool.

3.1 Determine, which data TREsPASS toolset need to operate and document it.

3.2 To determine does this data is available in ISKE Tool.

3.3 To assess integration possibilities of TREsPASS toolset as plugin into ISKE Tool.

For assesment of integration possibilities I determine data, which is needed for TREsPASS toolset work. This data I compared with data, which can be extracted for ISKE Tool. Was detected that some needed data for TREsPASS is missing in ISKE Tool. Making special libraries can be possible solution for finding missing data. So I suppose that integration on this stage is impossible, because special libraries (library of policies and library of proccesses) are needed and extra effort is required to design this libraries.

Additionaly we should display results of security analyze in ISKE Tool, but generally in ISKE Tool is not provided to display what ever data. Consequently, I offer to add TREsPASS toolset user interface.

The outline of the thesis is following:

Section 1 describes the TREsPASS toolset: it’s workflow and it’s system model.

Section 2 describes the ISKE Tool:

- it’s theoretical background, what is ISKE,
- it’s shortcomings and
- table of ISKE security assets.

Section 3 describes possibilities of integration:

- how should work “integrated” TREsPASS,
- updated ISKE Tool interface,
- all requirements for integration,
- assessment of integration possibilities, which components are similar in ISKE and which one should be added.

1. TREsPASS

“Information security threats for organisations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Successful attacks cost society billions a year, influencing on vital services and the economy. For example StuxNet, which used infected USB sticks to sabotage nuclear plants, or the DigiNotar attack, using fake digital certificates to spy on website traffic.“ [11]

Nowadays is project that is an EU FP7 project running from November 2012 till October 2016 and involving 17 partners across Europe, whom name is TREsPASS[1]. TREsPASS goals are predict, prioritise, and prevent complex attacks systematically: [11]

- Predict difficult attack scenarios in digital, physical and social engineering steps.
- Prioritise steps of scenario with tool of planning, which will help defenders analyse where they should expect the most serious attacks.
- Prevent attacks with the help of calculating and comparing cost effectiveness of countermeasures.

„The aim of the project is to build a semi-automated risk assessment framework and a tool which could be used to describe and analyse security of real-life socio-technical systems.“[3] By integrating European expertise in socio-technical security into a widely applicable and standardised framework, TREsPASS aims at reducing security incidents in Europe, and allowing organisations and their customers to make informed decisions about security investments.

Flowchart (Fig.1.1) of TREsPASS working process consists of several steps. The flowchart describes a system in intelligible for ordinary person view. Then TREsPASS extracts the model in the way, that is suitible for automating prossessing. On this step TREsPASS uses Navigator Map and adds Attacker Profile, which futher will help to generate attacks. Next step is generating of attack scenario in the way like attack tree or attack-defense tree. After that take place analysing of attack scenario with the help of security risk analysis tools and showing of results in understandable for person view.

[1] Reffered as **T**echnology-supported **R**isk **Es**timation by **P**redictive **A**ssessment of **S**ocio-technical **S**ecurity

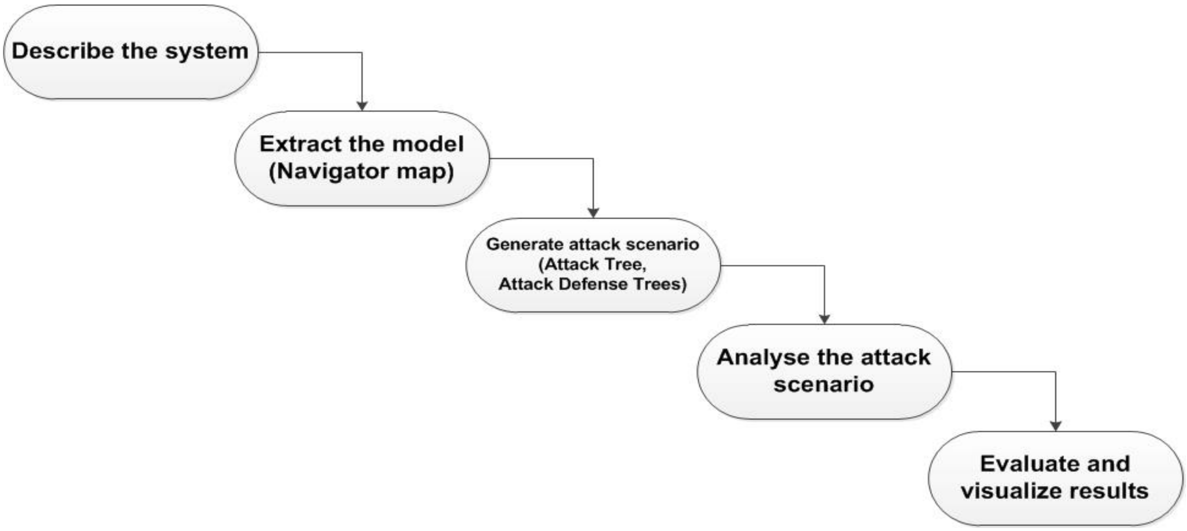

Describe the system
Extract the model (Navigator map)
Generate attack scenario (Attack Tree, Attack Defense Trees)
Analyse the attack scenario
Evaluate and visualize results

Figure 1.1 General workflow.

1.1.TREsPASS workflow

Workflow, which is a whole process consists of several steps. It is shown in Fig. 1.1.

Step 1. Describe the system.

Here we may use any tool, which allows to conviniently model the target infrastructure. It is comfortable for users, because system is described in understandable for person view. On this step can be used any program, but here we represent BiZZdesign Architect BiZZdesign Architect [4](Fig. 1.2). Modelling language similar to UML.

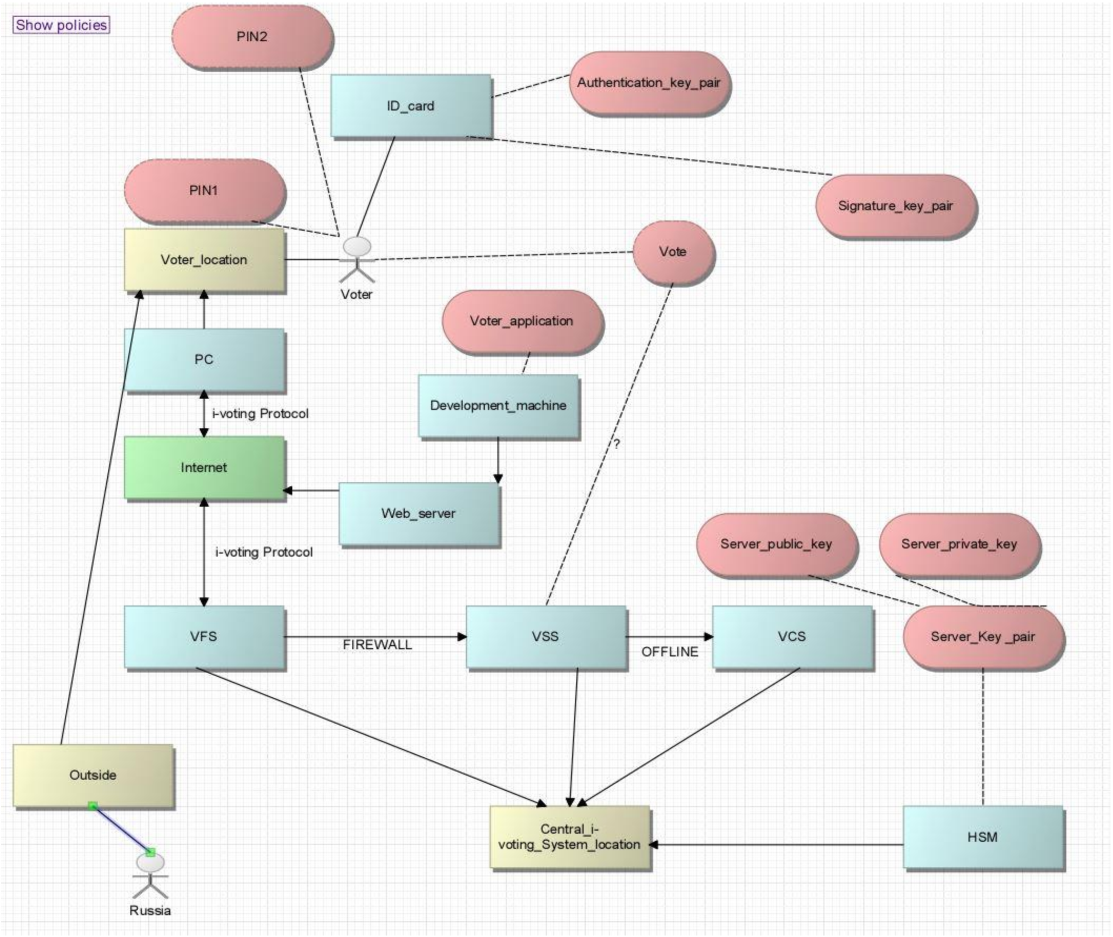


Figure 1.2 BiZZdesign Architect, graffical view of system. [3]

<u>Step 2.</u> Extract the model. (Fig. 1.3)

The Navigator Map is extracted from the highlevel description of the system at step 1.

BiZZdesign Architect is capable of generating the Navigator Map from the model. „*Navigator map (socio-tehnical model) consists of*

- *Locations(physical, network)*
- *Policies(global policies and access policies)*
- *Processes*
- *Edges*
- *Assets*
- *Actors*
- *Libraries(Attack Pattern Library, Model Pattern Library)*“[3]

Navigator Map can be stored in xml format like a universal presentation of the system and re-used when needed.

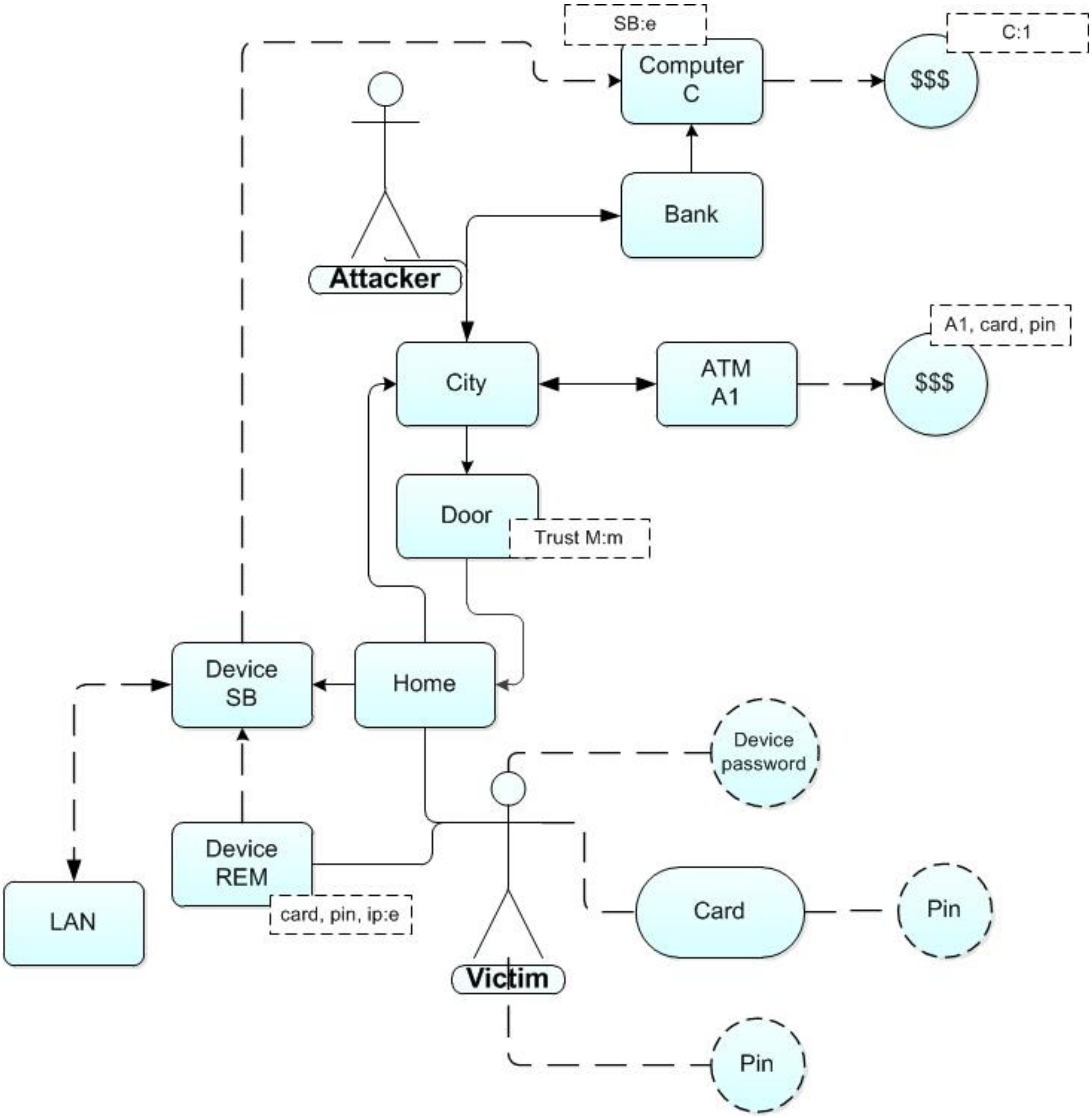


Figure 1.3 Organisation model. Graffical representation of Navigator Map.

From Navigator Map we can generate the attack scenario in required form.

Figure 1.3 describes that Attacker is in the town. Victim is in the same town at home. Between Victim and town is door. In the town is bank where is computer C. At home is Victim, who use system of 2 devices: LAN, which has network access and connection in bank with computer C. Victim has card with pin-password. Attacker is in town and wants to get Victim’s money.

Step 3. Generate attack scenario.

Attack scenario can be created in different forms, such as

- *Attack Trees(Fig. 1.3), Attack DAG-s*[2]
- *Attack-Defence Trees*
- *Timed Automata*

„Attack generation procedure is based on incremental policy invalidation."[3] I will discribe the excample of incremental policy invalidation. All starts with global policy – Attacker mustn't get Victim's money. (Fig. 1.4)

[2] Reffered as Directed Acyclic Graphs

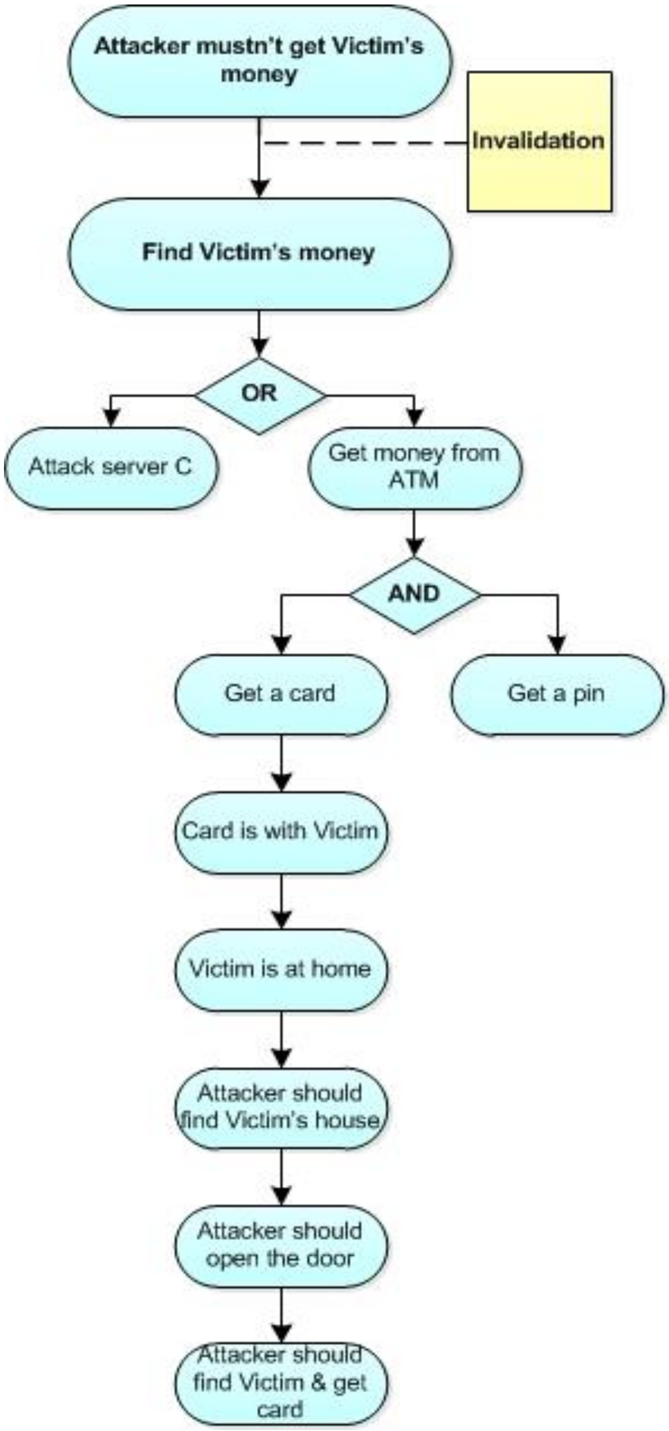

Attacker mustn't get Victim's money
Invalidation
Find Victim's money
OR
Attack server C
Get money from ATM
AND
Get a card
Get a pin
Card is with Victim
Victim is at home
Attacker should find Victim's house
Attacker should open the door
Attacker should find Victim & get card

Figure 1.4 Incremental policy invalidation.

As the result of TREsPASS workflow generate attack scenario. (Fig.1.5)

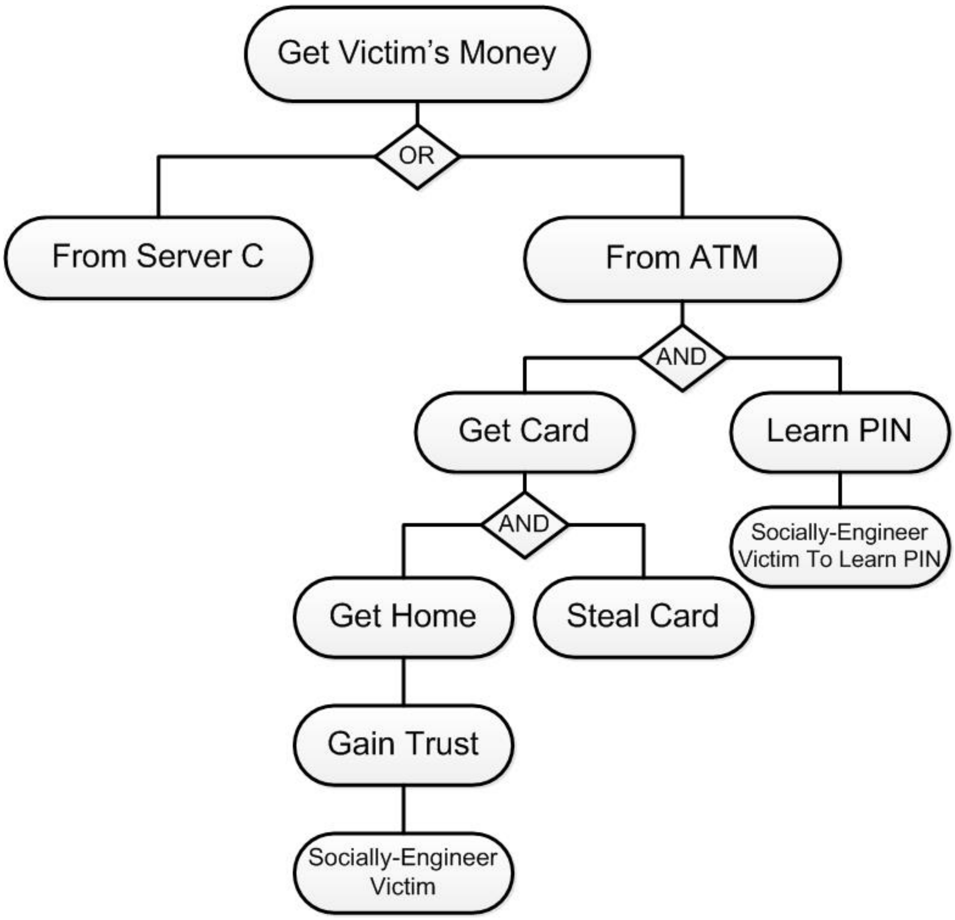


Figure 1.5 Attack scenario describes how attacker can get victim money.

Step 4. Analyse the attack scenario.

Attack scenario is input data for risk analysis programs.

The project has developped a set of tools for quantative operational security risk analysis.

- ApproxTree+[3]

  ApproxTree+ analysis tool is a new tool for quantitative assessment of operational security risks. ApproxTree+ is elaborated and maintained by Cybernetica AS. ApproxTree+ is counting an expected attacker utility. If an utility is negative, we may say that a system is sufficiently safe. If possitive, a system is unsafe. Attacker can not run repeated attack.

- Failure-Free analysis tools[1,2]

This is similar to AppoxTree+ and is elaborated and maintained by Cybernetica AS too. Only differense is if analyse is runing unsuccessfully in Failure-Free analysis tools attacker can run repeated failed attacks. Scenario is described in attack tree view.

- ADTool[12]

This analysis tool was made by The University of Luxembourg. This is classic analysis of Attack Defense Trees. One may analyse only one parameter at time (Min/Avg/Max of cost or probability or complexity or time).

- Pareto efficient solution for ADTs

This analysis tool was made by The Tehnical University of Denmark. Pareto efficient solution for ADTs works with attack trees. Optimizes unmatching/opposing parameters, suggests the best attack vectors.

- DFTCalc[8]

This analysis tool was made by an Aalborg University of Technology. DFTCalc is Time-dependent analysis. This tool explores how probability of attack success changes in different time(Timed-Automata).

The output data of these tools may be helpful for the integration process.

Step 5. Evaluate and visualize results. (Fig.1.6, Fig. 1.7) The TREsPASS demonstration.

This is a final step, we need to outline analysis results in human friendly way to the analysis.

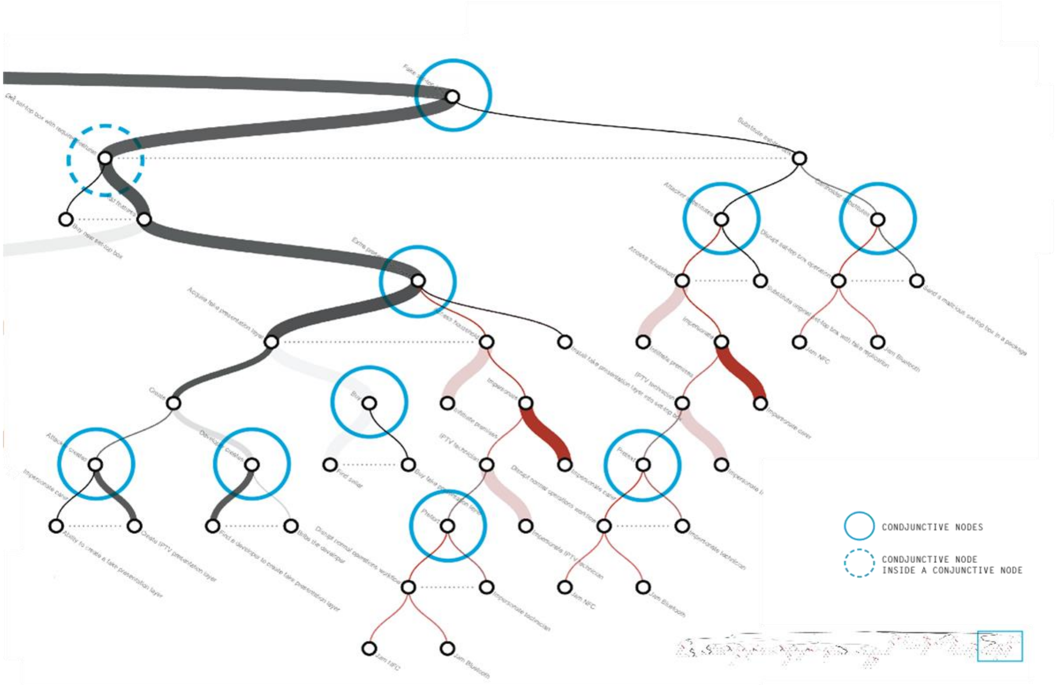


Figure 1.6 Example of analysis results on an attack tree. (TREsPASS project review demo, Brussels 2014)

Figures 1.6 and 1.7 illustrate the most profitable attack path shown in an attack scenario in the form of attack tree. Various visual effects, such as thickness of line, color, fill pattern, transparency may be used to depict various parameters of attacks.

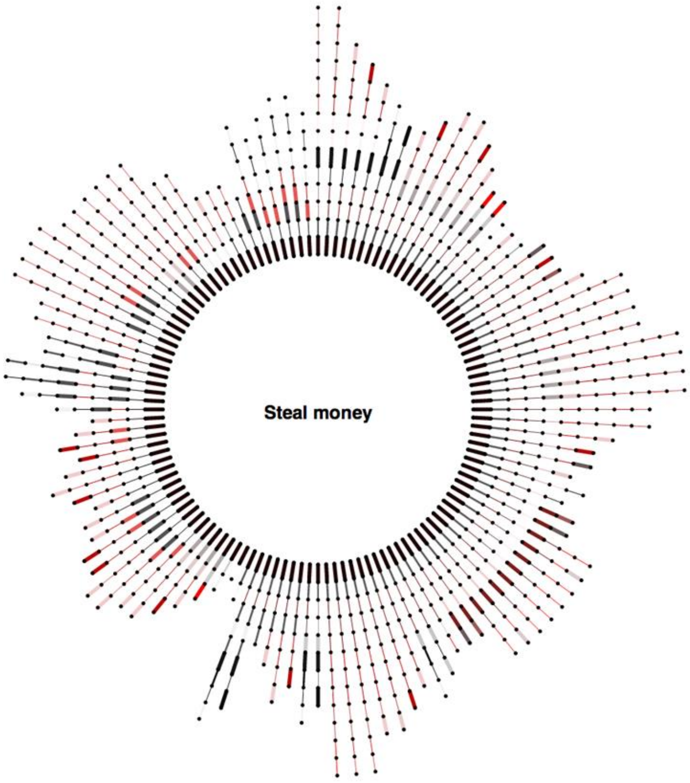


Figure 1.7 Example of analysis result.

The same results, which are described above, presented in another format.

1.2.The TREsPASS System Model

In this section describes core of TREsPASS is the so-called Attack Navigator, which is a set of interconnected locations. Actors and data can move along connections. In physical domain move actors and in network domain moves data. Actors move along edges and perform certain actions at certain locations proccesses pass data accross locations. Assets in the model is an any kind of data that is relevant for this model. Data in assets can be presented like a value or a metric. Actions in the model describe operations that actors are able to do. Data input and output is usual actions in the model. Also actions are used for moving within domains, for example when user is starting any process on a computer. Actions have a target. For exapmle, input/output/move/execute work on locations, or social engineering works on actors. Policies outline the required credentials to perform the action. For excample, location policy of door – we should have key or victim trust to execute action - pass the door. Policy credentials can be location, identity, asset or data.

Infrastructure of TREsPASS consists of two main components: a Navigator Map and several profiles of attackers. [2,14] Navigator Map (Fig. 1.8) contains of a formal description of the target infrastructure as a socio-technical system, which consists of several layers – physical infrastructure (Fig. 1.10), social infrastructure (Fig. 1.11) and technical infrastructure (Fig. 1.12). Nowadays not everything is implemented, but it is a work in progress. A set of automated risk analysis tools named TREsPASS toolset works on the base of files like Navigator Map and Attacker Profile. (Fig. 1.9)

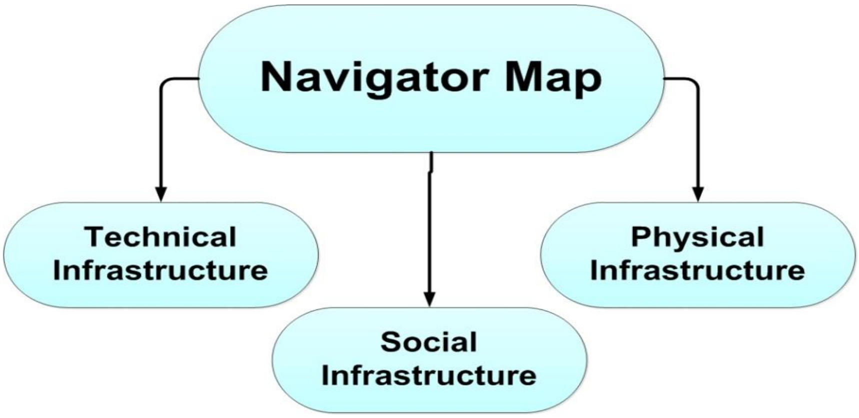


Figure 1.8 Navigator Map overall view.

Navigator Map may be divided into such components like tehnical infrastructure (for example-database), social infrastructure (for example-actor) and physical infrastructure (for example-room).

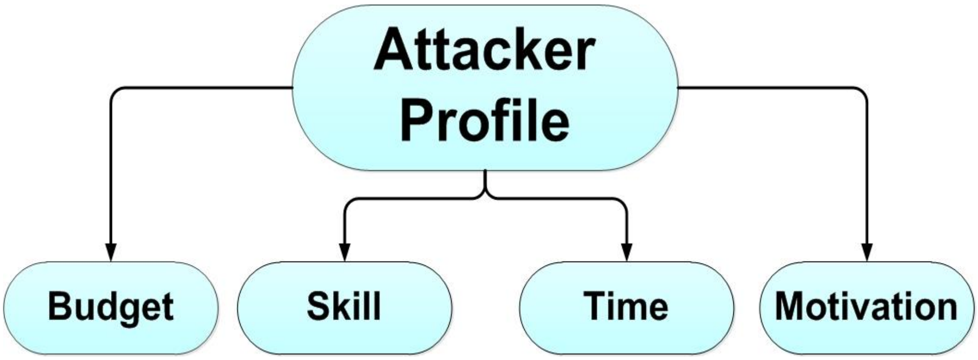


Figure 1.9 Attacker Profile overall view.

Attacker Profile.

An attacker profile give us flexibility in analysis of security risks and is a set of constraints and limitations applied to attacker.

Attacker profile options:

- Budget(€) – the amount of money Attacker invest into attacking;
- Skill(Low/Med/High/Very high) – which skills Attacker have;
- Time(sec/min/hour/day) – the amount of time Attacker can spend on attack;
- Motivation(profit/fame/policies/religion etc.) – motivation influences strategical preferences of the adversaries.

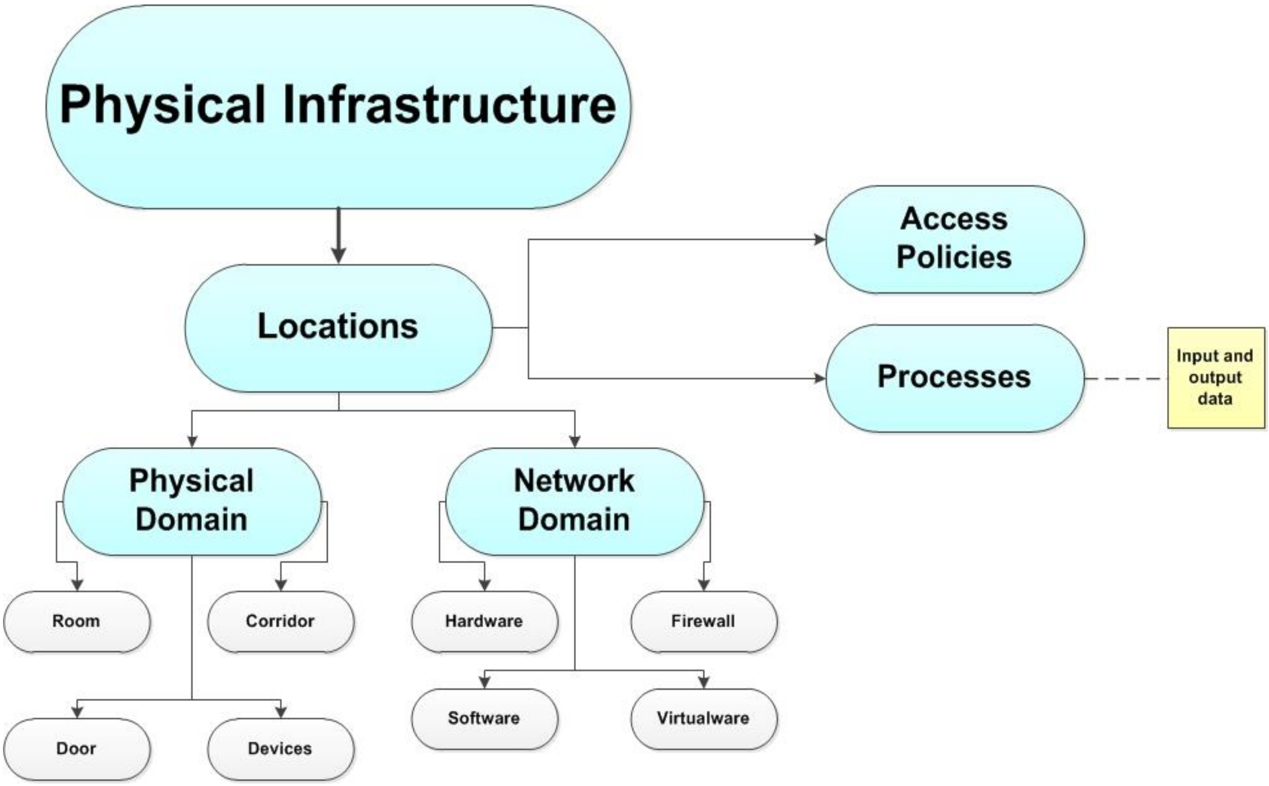


Figure 1.10 Navigator Map, Physical Infrastructure

Edges connect different locations in the model. Actors in a model move along edges connecting locations in physical domain, data moves along edges connecting locations in network domain. Edges define boundaries within which actors and data can move.

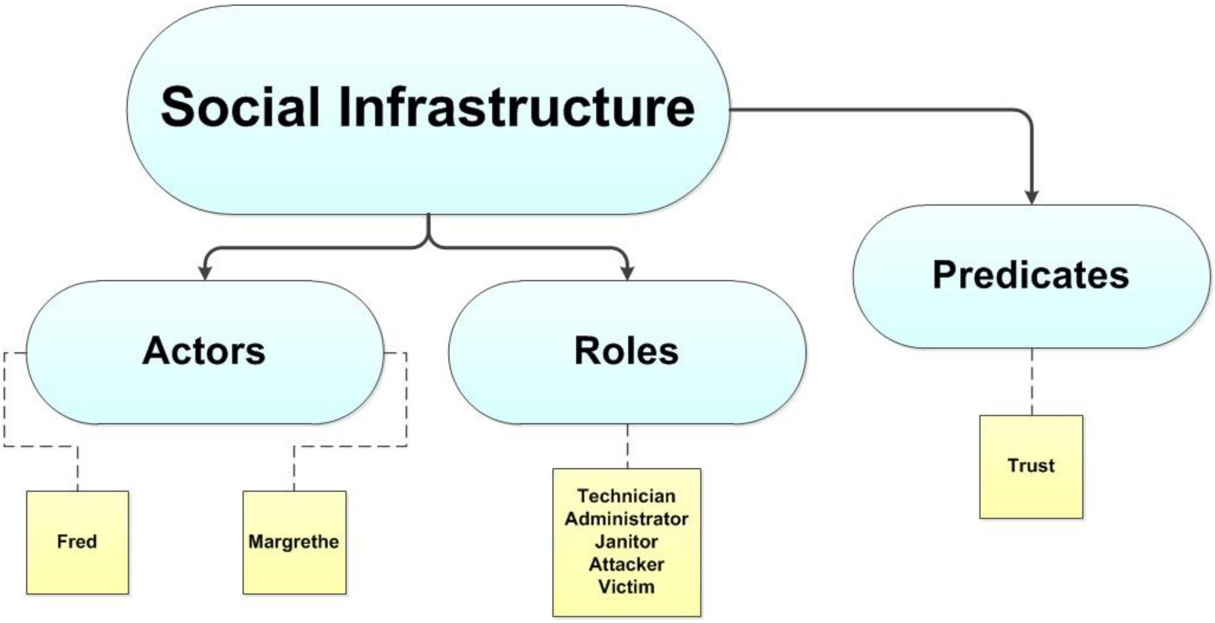


Figure 1.11 Navigator Map, Social Infrastructure

For simplicity, actors may have different roles, for example Margrethe can be a victim. Technical and social infrastructures are not separated, all is conceptually.

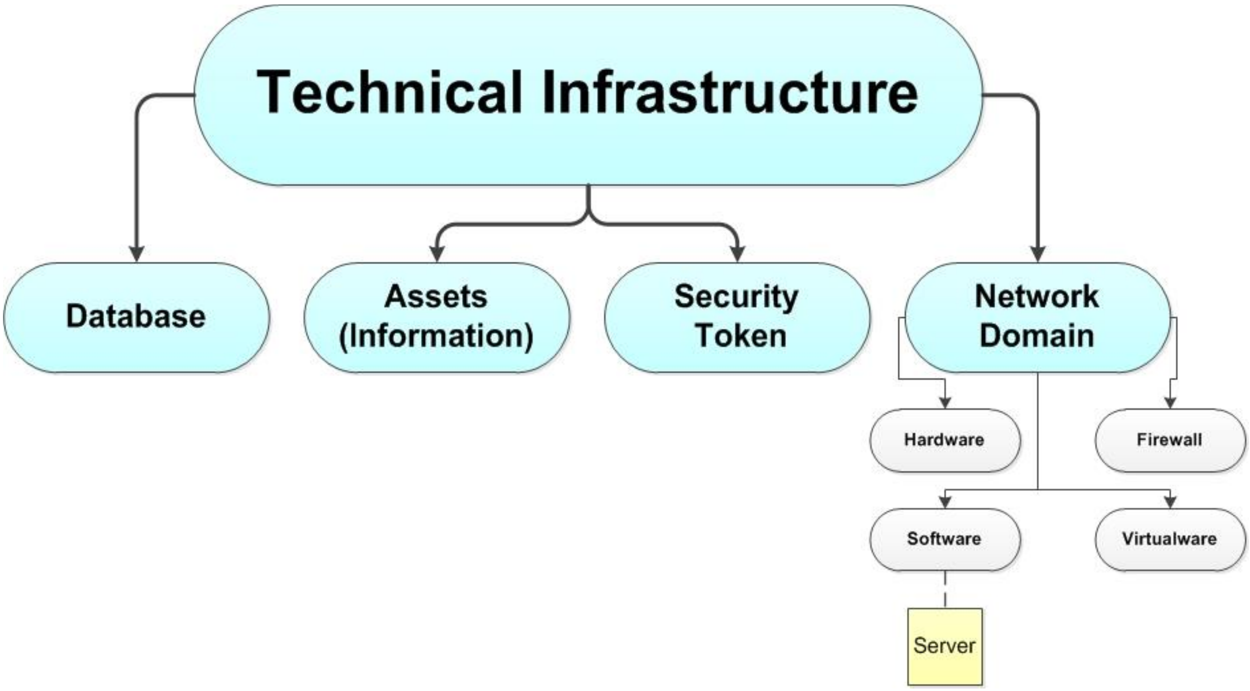


Figure 1.12 Navigator Map, Technical Infrastructure

In technical infrastructure is presented in example by database or assets with information or by security token which should be protected. For example server belongs to technical infrastructure and be a physical location at the same time.

It is hard to classify domains, are they physical or digital or social as domains overlap. They are all interrelated.

For integration of TREsPASS toolset into existing security risk analysis tools it is necessary to determine where and how (deployment environment) you can get the necessary information about all or at least a part of necessary data needed for Navigator Map. Different tools for analysis of security risks require different information, which differs in its detail, accuracy, reliability and so on. For ISKE contains a module that enables experts to enter desired information in table form (as in ISKE[9]) or simulate interactively (as in Trick Light[3][6]). Some of the information comes from experts and it is ready to use. Some data may be missing and in this case it may be obtained from expert estimations.

[3] Reffered as **T**ool for **R**isk management of an **I**SMS based on a **C**entral **K**nowledge base

2. ISKE

2.1.Theoretical background

ISKE[9] is an informational security standard that is developed for the Estonian public sector (Fig. 2.1). The preparation and development of ISKE is based on a German BSI[4][7] information security standard – IT Baseline Protection Manual, which has been adapted to match in the situation Estonian. BSI system has been extensively documented and detailed, and it is regularly updated every year.[10]

ISKE Tool has been created especially for state and local government databases using information systems and their associated information assets secure. ISKE may be used by enterprises to ensure the security of their IT assets. ISKE implementation guide's first versioon was made in October 2003.

The goal of ISKE is to ensure the sufficient security level for data, information and assets processed by IT systems. The necessary security level is achieved by implementing the standard organizational, infrastructural/physical and technical security measures. In accordance with the standard ISKE Tool is designed to reduce the time spent on security threats and directories and to enable implementers of automated forms processing ISKE implementation process.

ISKE as baseline security system is one set security measures, which are applicable to all information assets. "*Contains more than 1,000 security measures."*[3]

Security is based on the grade of the confidentiality of information, integrity of information, time-critical information operability of information allowed for the weight of the consequences of delay.

"The levelled baseline security system is more economical, as there is no need to exercise expensive security measures on data with limited security requirements. Additional expenses on data and information system analysis and for outsourcing the required set of security measures will be applicable to the implementation of a security system of different levels."[3]

[4] BSI- in german, Bundesamt für Sicherheit in der Informationtechnik;
in english Federal Office for Information Security.

ISKE implementation agency is not a one-time project. This is an continious process, because not only IT environments, security risks and measuresis changing, but the implementation guide too. ISKE operational tool for the implementation of it is helpful and supportive tool that allows an organization to use information assets mapping, data capture type module assets, information assets, and the zonal ISKE to monitor implementation.

ISKE Tool is ISKE assisting and supporting implementation, which allows:

- To outline used information assets in enterprises,
- Define security classes and security levels,
- To link information assets with ISKE modules,
- To group and separate information assets into zones,
- To create and to manage plan of implementation, which helps to keep ISKE implementation process.

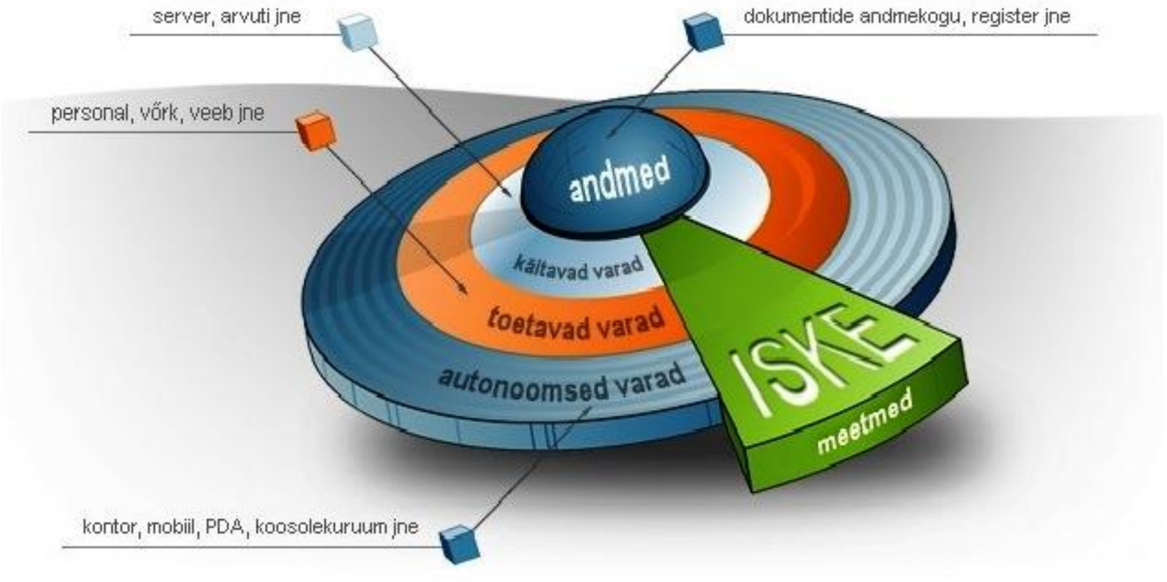


Figure 2.1 ISKE Tool overall view

2.2.ISKE shortcomings

Some negative aspects with which will ordenary user face, if decides to use ISKE Tool.

- ISKE in Estonia is made as an mandatory for government institutions, not as an helpful handbook;

- Is designed for state and local government databases. It is too big for SME[5], but they need security analysis tools too. I wish to mention that TREsPASS was designed with scalability principle in mind and takes SME-s into account;

- For govermental institutions audit is complementary and is a strict requirement. Auditing process is a little bit expensive because it is carried out by CISA[6] certified auditors and not every enterprise can afford this;

- ISKE handbook is over 3000 pages long, and that may be very difficult to understand and not to become confused. That will scare way some people, who wish to use ISKE Tool;

- Treat and vulnerability landscapes change more frequently and the update period of ISKE Tool, which is used currently does not allow to account with these changes in a timely manner.

2.3.ISKE list of security assets.

In ISKE Tool protected system is described using B-module parameters, which we use to discribe the system.

Tabel 2.1 A list of values, which should be protected according to ISKE Tool.

B1 Common components.	**B2 Infrastructure**	**B3 IT-systems**	**B4 Networks**	**B5 IT-applications**
-Information Security management -Organosation	-Buildings -Electrical cabling	-Server -Unix server -Novell Netware	-Heterogeneous networks -Network and system control	-Data Storage based data exchange -Software group

[5] Reffered as Small and Medium Enterprises
[6] Reffered as Certified Information Systems Auditor

B1 Common components.	**B2 Infrastructure**	**B3 IT-systems**	**B4 Networks**	**B5 IT-applications**
-Staff -The concept of emergency preparedness -Data backup policy -Protection of data -The concept of anti-virus -Cryptoconcept -Handling of security incidents -Control of hard- and software -Type of software -Outsourcing -Archiving -Information security awareness and	-Office room -Server room -Archive of media storage - Technical infrastructure room -Safe -Job at home - Computing center -Mobile workplace -Rooms for conference, events and training -IT-cabling	4. server -Windows 2000 server -Mainframes S/390 and zSeries -Windows Server 2003 -Klient -Independent IT-system -Notebook -Unix klient -Windows 2000 klient -Internet-PC -Windows XP klient -Windows Vista klient -Security lock(Firewall) -Routers and	-Modem -Virtual private network -IT-system’s LAN connection by ISDN - Wireless LANs -VoIP -Bluetooth	-Web server -Lotus Notes -Fax server -Database -Remote work -Novell eDirectory -Exchange 2000/Outlook 2000 -SAP system -Mobile Data Storage -Overall directory service -Active Directory -Samba -DNS-server -Internet

B1 Common components.	**B2 Infrastructure**	**B3 IT-systems**	**B4 Networks**	**B5 IT-applications**
training -Security patches and administrative changes -Data deletion and destruction -Administrative requirements		switches -The storage systems and storage area network -Virtualization -Terminal server -PBX -Faks -Cellphone -PDA -Printers, copiers and multifunction devices		

This data is stored in a database in ISKE Tool and this set of data is the “environment” where the TREsPASS toolset is being deployed.

3. INTEGRATION

In this part of my work I assess the possibilities and feasibility of integration of TREsPASS toolset in ISKE Tool. The integration can conceptually be illustrated with Figure 3.1. Integration of TREsPASS will give us opportunity to improve the security of systems against attacks.

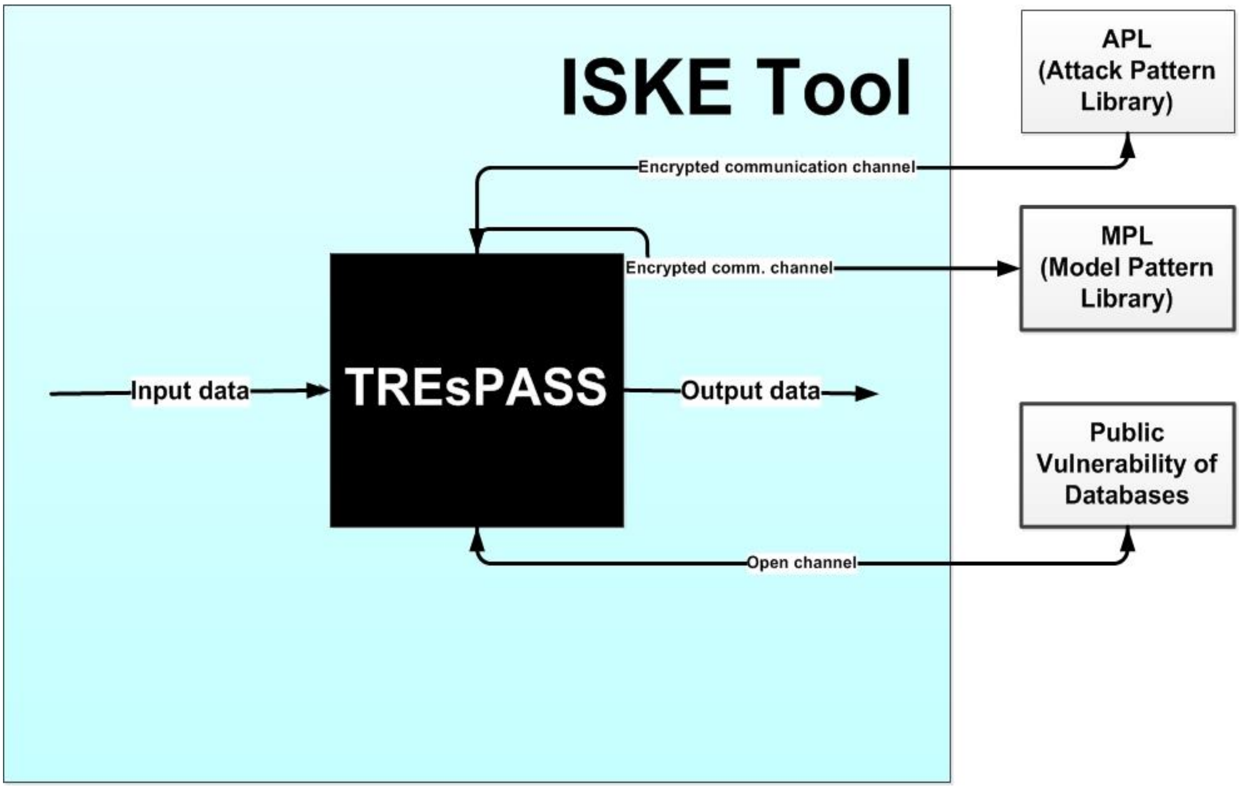

ISKE Tool
APL (Attack Pattern Library)
Encrypted communication channel
MPL (Model Pattern Library)
Encrypted comm. channel
Input data
TREsPASS
Output data
Public Vulnerability of Databases
Open channel

Figure 3.1 Integration of TREsPASS toolset into ISKE Tool.

TREsPASS determines which input data in this integration is required. TREsPASS is for us like BLACK BOX, because it every time changes and we do not know which data it keeps inside. Integrate TREsPASS into ISKE Tool can be made like plugin. TREsPASS toolset communicates with ISKE Tool and with outside. User does not work straightly with TREsPASS toolset, but works directly with ISKE Tool, where TREsPASS toolset is integrated. TREsPASS toolset adds additional functionality – not originally planned in ISKE Tool – GUI[7] needs to be changed. User can use for risk analyze component like Attacker Profile, which is TREsPASS component. For successful integration ISKE Tool should present

[7] Reffered as Graphical User Interface.

all needed data and find a way to display results in the deployment environment. Input data divided into 2 components:

- Static data, which is available in ISKE Tool and is delivered into TREsPASS in automated mode;
- Dynamic data, which is defined by the command control. Dynamic data is represented currently by Attack Profile, which is described in module 1.2 in which we can change:
    - Budget,
    - Skill,
    - Time,
    - Motivation.

For example:

Profile 1.(script-kiddie)

Budget: 100€

Skills: Low

Time: Hours

Motivation: Fame

Profile 1 describes a class of adversaries represented by pupils, who attack only for fun or fame. Representatives of class of attacker as a rule have for this attack a few money and skills are low in this area. Usually such attacks are unsuccessful and attackers quickly lose interest in this. So-called a non-targeted attacks.

Profile 2.(organized crime group)

Budget: 1000000€

Skills: Very high

Time: Days

Motivation: Profit

Profile 2 describes large enterprises or organized crime groups. Trey spend for this attack substantial sums of money and time is measured by days or more. Skills of attackers are as rule very high. If attack with such attacker profile is successful, victim suffers substantial damage.

3.1.The “Integrated” TREsPASS workflow

The process of collecting and processing information in TREsPASS now will be shorter on 1 step (Fig.3.2). This needed information is contained in internal database of ISKE Tool. TREsPASS extracts Navigator Map from ISKE Tool B-module.

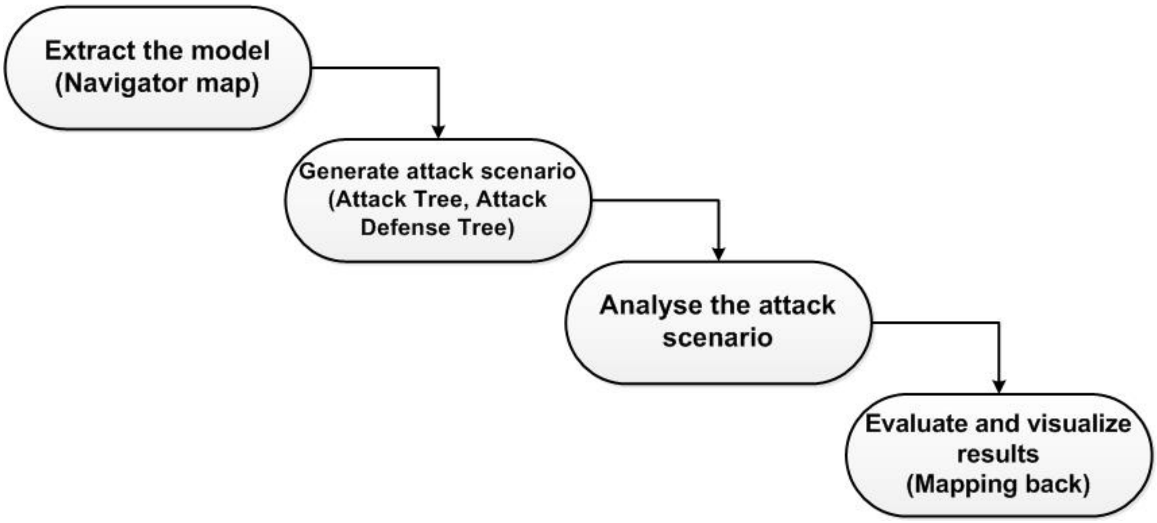

Extract the model (Navigator map)
Generate attack scenario (Attack Tree, Attack Defense Tree)
Analyse the attack scenario
Evaluate and visualize results (Mapping back)

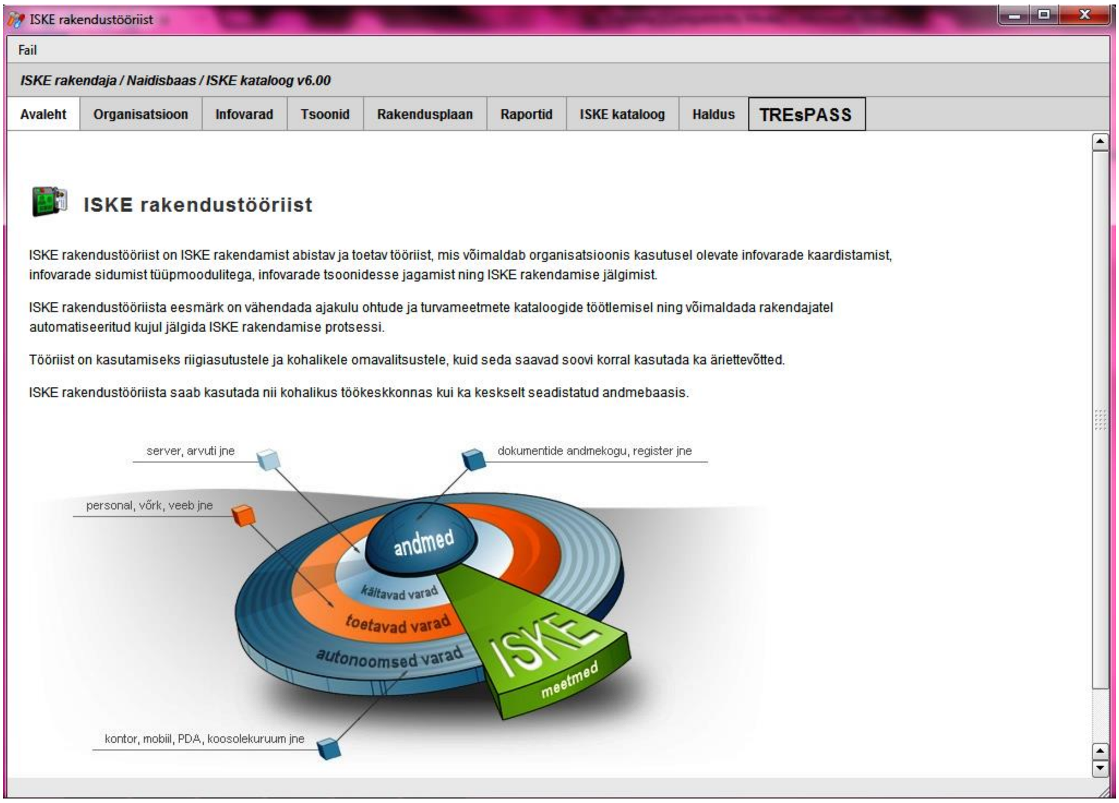
Figure 3.2 TREsPASS workflow, if we integrate it in ISKE Tool.

As TREsPASS needs more information that ISKE Tool can provide integration will require library of components, such as Attack Pattern Library, Model Pattern Library and Public Vulnerability of Databases. ISKE Tool communicates outside with that components.

On the first step we extract the model from the deployment environment to the greatest possible extent. The third and fouth step did not change. And on fifth step we evaluate and visualize the results by means of the deployment environment to a greatest possible extent. Expert should inform, how Attacker Profile has to look like, what data should be changed. Also experts should think, how to show the results of security analysis. For this should be added additional capabilities in GUI.

3.2 Updated ISKE Tool interface.

To map the results back, some changes to the user interface are required with Fig.3.3.



ISKE rakendustööriist

ISKE rakendustööriist on ISKE rakendamist abistav ja toetav tööriist, mis võimaldab organisatsioonis kasutusel olevate infovarade kaardistamist, infovarade sidumist tüüpmoodulitega, infovarade tsoonidesse jagamist ning ISKE rakendamise jälgimist.

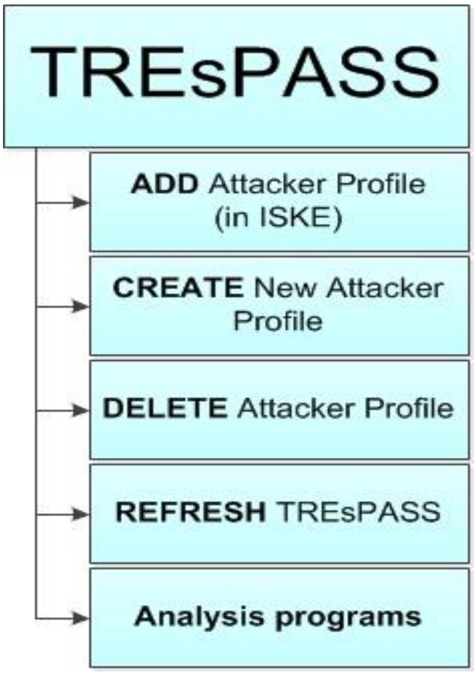
ISKE rakendustööriista eesmärk on vähendada ajakulu ohtude ja turvameetmete kataloogide töötlemisel ning võimaldada rakendajatel automatiseeritud kujul jälgida ISKE rakendamise protsessi.

Tööriist on kasutamiseks riigiasutustele ja kohalikele omavalitsustele, kuid seda saavad soovi korral kasutada ka ärietteõtted.

ISKE rakendustööriista saab kasutada nii kohalikus töökeskkonnas kui ka keskselt seadistatud andmebaasis.

Figure 3.3 Illustration of integration of TREsPASS into ISKE Tool.

Figure 3.3 is represented ISKE Tool desktop, where I offered to add in main menu bar button „TREsPASS“ to have all user interface in one place, using TREsPASS toolset as plugin. The menu of TREsPASS may be like shown Figure 3.4.



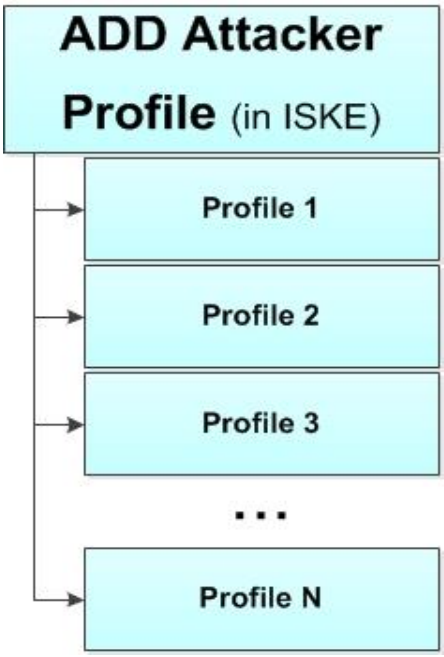
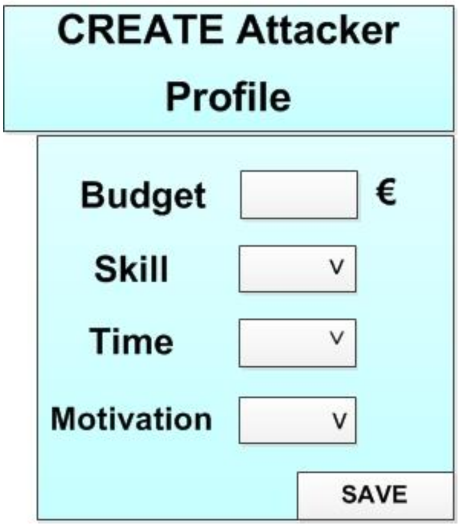


Figure 3.4 TREsPASS menu bar (left).

Figure 3.5 Button “ADD Attacker Profile” in ISKE Tool (right).

The button „ADD Attacker Profile (in ISKE)“ (Fig.3.5) will allow to add already made attacker profile in project made by ISKE Tool and give complementary possibility to make better security analyze for ISKE Tool.

The button „CREATE New Attacker Profile“ (Fig.3.6) will allow to create attacker profile user is needing. In this menu bar user can choose such parameters like budget in euro, skills *(Low/Medium/High/Very high),* time *(sec/min/hour/day)* and motivation *(profit/fame/policies/religion etc.).* Then user should save chosen parameters, giving them special name (Fig.3.7). Attacker profile will be saved only in ISKE Tool folder.



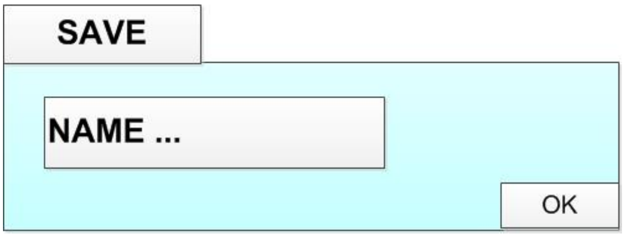


Figure 3.6 Button “CREATE New Attacker Profile” in ISKE Tool (left).

Figure 3.7 Attacker profile saving menu (right).

The button „DELETE Attacker Profile“ (Fig.3.8) will give opportunity to delete not using attacker profile form ISKE Tool folder.

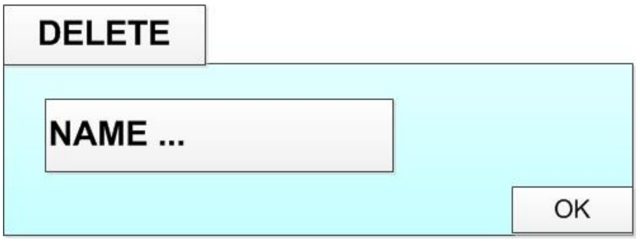


Figure 3.8 The button of removing not used attacker profile from ISKE Tool.

Next button in TREsPASS menu bar is „REFRESH TREsPASS“, which gives opportunity to look for any update of TREsPASS system.

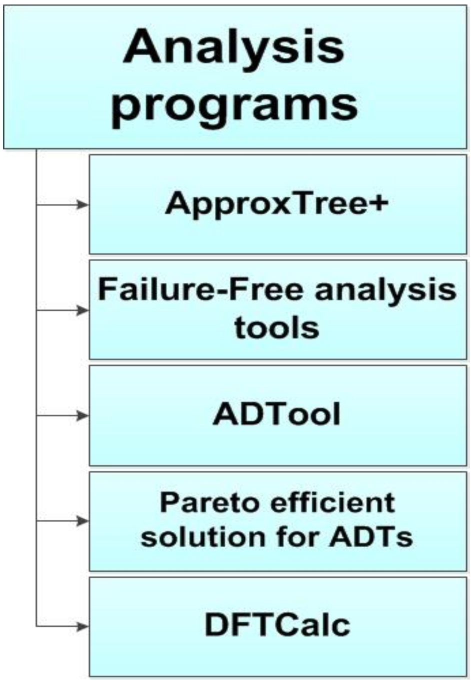

Analysis programs
ApproxTree+
Failure-Free analysis tools
ADTool
Pareto efficient solution for ADTs
DFTCalc

Figure 3.9 Button “Analysis programs” in ISKE Tool.

And the last button in TREsPASS menu bar is „Analysis programs“ will allow to analyze the system with already integrated in TREsPASS analysis programs, such as ApproxTree+, Failure-Free analysis tools, ADTool etc. As the result user will see security analysis program work, which will be displayed like Fig. 1.6 or Fig. 1.7. Basing on such figures experts can make conclusion about how analyzed system is secured from attacks.

3.3Integration requirements

In integration TREsPASS into ISKE Tool we should consider such requirements like:

- Work of users must not be disturbed (speed, productivity, work without errors);
- TREsPASS integration into ISKE should enhance the reliability of the result of analysis with ISKE Tool;
- Maintain productivity at least on the same level;
- Price of Toolset should not change;
- Create understandable manual for end-users;
- Possibility of ISKE Tool work without TREsPASS (plugin/pluggable module).

3.4Assessment of integration possibilities

Tabel 3.1. Comparing two columns of this table, where first of columns is based on Table 2.1.

ISKE Tool	TREsPASS toolset
B-module ➢ Common components ➢ Infrastructure ➢ IT-systems ➢ Networks ➢ IT-application	Navigator Map ➢ Locations ➢ Policies ➢ Processes ➢ Edges ➢ Assets ➢ Actors/Roles ➢ Libraries Attacker Profile ➢ Budget ➢ Skills ➢ Time ➢ Motivation

1. The most part of Common components of B-module of ISKE Tool we may give name policies. But the meaning of policies in ISKE Tool and TREsPASS toolset policies is different. TREsPASS „looks“ inside the policy, how it is working and what it is doing. ISKE does not give such data. For ISKE this is binary parameter. TREsPASS has 2 different kinds of policies: access policies and organizational policies. Example of access policy: Door: {key|trust}:{move} and this means that, if you want to open th door you need to have key-asset or predicate-trust. Example of organizational policy - notebook must be encrypted. Exception in Common components is only parameter Staff, which is Role in Navigator Map. Policies can not be taken from database, they are kept in complementary library. In TREsPASS Locations have policies.

2. Infrastructure in B-module of ISKE Tool is the same like Locations in Navigator Map in TREsPASS. So we can take Locations straightly from ISKE Tool database.

3. IT-systems in B-module is Network Locations and Assets in Navigator Map.

4. Networks in ISKE can be named Edges in TREsPASS.

5. Most of IT-applications in B-module of ISKE Tool we may give name processes. Only Internet and Mobile Data are Locations. But the meaning of Processes in ISKE Tool and TREsPASS toolset processes is different. From ISKE Tool this is binary parameter like policies.

Now we may make such conclusion, that a bigger part of parameters, which Navigator Map needs to generate Attack Tree, we can find in ISKE Tool.

In ISKE Tool I could not find such attack parameters of TREsPASS toolset like policies and proccesses on such level of specification like in TREsPASS and Attack Profile. So I offer to add them in ISKE Tool. Policies and proccesse should be made by experts and put into Libraries. Every analyzing enterprise will have specially made Library.

4. CONCLUSION

The aim of my thesis was to research possibilities of integration of the TREsPASS toolset into the ISKE Tool. For solving this task I studied the ISKE Tool and the TREsPASS toolset and compare data these systems contain. Can ISKE Tool provide all needed data for integration of TREsPASS toolset. Integration could be made easily, if all needed data was in ISKE, unfortunately it is not so.

As the result I detect that such data of TREsPASS as Locations, Edges, Assets, Actors/Roles are similar to ISKE Tool and it is ready to use in integration, because in ISKE all data is structurized. In my research I detect that such data like processes and policies cannot be provided on such level of detalization, which is required by the TREsPASS toolset. Attacker Profile is missing in ISKE Tool. Information about policies and processes we may get from Libraries, which will be made by experts for collaborative environment. Also we have not data about Attacker Profile, but it can be user input from end-user estimations. This give us flexibility in analyze of system.

In the future, Libraries should be studied more particularly. How they are kept and how will user communicate with them. At the moment, I assume that integration of the TREsPASS toolset into the ISKE Tool is impossible, because expert should create Libraries of components (policies and processes) of the model and this will require additional researches and creation of external components.

Also, I offered to add in main menu bar button „TREsPASS" to have all user interface in one place, using TREsPASS toolset as plugin. So should be made TREsPASS toolset plugin for integration in ISKE Tool.

Certainly, we should display results of security analyze in ISKE Tool, but generally in ISKE Tool is not provided to display what ever data. Consequently, experts should add GUI to display any analysis programs results, for example, like on the Figure 1.6 and on the Figure 1.7. Basing on such figures experts can make conclusion about how analyzed system is secured from attacks.

And the last one think that I offer to realize is to do benchmarking test of integration solution. This test will give us opportunity to check out are integration requirements saved.

5. KOKKUVÕTE

Minu töö eesmärgiks oli uurida integratsiooni võimalusi TREsPASS rakendustööriistadest ISKE rakendustööriistadesse. Selle ülesanne lahendamiseks õppisin tundma ISKE rakendustööriistu ja TREsPASS rakendustööriistu ning võrdlesin nendes süsteemides olevaid andmeid. Kas võib ISKE rakendustööriist sisaldab kõiki vajalike andmeid TREsPASS rakendustööriistade integreerimise jaoks. Integratsioon võiks olla lihtne, kui ISKE pakuks kogu vajalikku informatsiooni, aga kahjuks see ei ole nii.

Tulemusena ma märkasin, et sellised TREsPASS'i andmed nagu Kohad, Servad, Infovarad, Näitlejad/Rollid on ISKE rakendustööristaga sarnased ja need on valmis integreerimiseks, sest ISKE's kõik andmed on struktureeritud. Ma identifitseerisin, et ISKE ei sisalda sellised andmed nagu protsessid ja poliitikad nii detailselt nagu vajab TREsPASS rakendustööriist. Ründaja Profiil puudub ISKE rakendustööriistas üldse. Me võime võtta informatsiooni poliitikate ja protsesside kohta Raamatukogudest, mida teevad eksperdid koostöö õhkkonnale. Samuti ei ole meil andmeid Ründaja Profiili kohta, kuid lõppkasutaja hinnangute põhjal võib olla see sisend kasutaja tehtud. See annab meile süsteemi analüüsides paindlikkust.

Tulevikus peaks Raamatukogusid uurituma täpsemalt. Kuidas neid hoitakse ja kuidas kasutaja nendega suhelda saab. Praegu ma oletan, et TREsPASS rakendustööriistade ISKE rakendustööriistasse integratsioon on võimatu, sest et ekspert peaks looma Raamatukogude komponentide mudeli (poliitikad ja protsessid) ja see nõuab rohkem uurimustööd ja täiendavate väliste komponentide loomist.

Samuti, ma pakun välja lisada peamenüüsse nupp „TREsPASS", et kõik kasutajad saaksid kommunikeerida ühes kohas, kasutades TREsPASS rakendustööristu nagu plugin. Samuti peaks olema tehtud TREsPASS rakendustööristadele plugin ISKE rakendustöörista integreerimiseks.

Kindlasti me peaksime kuvama tulemusi ISKE rakendustöörista turvalisuse analüüside kohta, kuid üldiselt ISKE rakendustöörist ei ole ettenähtud mingeid andmeid näitama. Järelikult ekspertid peaksid lisama GUI programmi mingite analüüside tulemuste kuvamiseks, näiteks, nagu on Pildil 1.6 ja Pildil 1.7. Eksperdid võivad teha kokkuvõtte selliste pildide põhjal, kuidas analüüsitud süsteem on kaitstud rünnaku vastu.

Ning viimane asi, mis ma realiseerimiseks pakun on teha intergatiooni lahenduse jõudluse test. See test annab meile võimaluse kontrollida, kas integreerimise nõuded on täidetud.

LIST OF REFERENCES

1. Ahto Buldas and Aleksandr Lenin. New efficient utility upper bounds for the fully adaptive model of attack trees. In Decision and Game Theory for Security - 4th International Conference, GameSec 2013, Fort Worth, TX, USA, November 11-12, 2013. Proceedings, pages 192–205, 2013. (20.10.2014)
2. Aleksandr Lenin and Ahto Buldas. Limiting adversarial budget in quantitative security assessment. In Decision and Game Theory for Security - 5th International Conference, GameSec 2014, Los Angeles, CA, USA, November 6-7, 2014. Proceedings, pages 153–172, 2014.
3. Aleksandr Lenin, Jan Willemson, and Dyan Sari. Attacker profiling in quantitative security assessment based on attack trees. In Simone Fischer-Hübner and Karin Bernsmed, editors, 19th Nordic Conference on Secure IT Systems, NordSec 2014, Tromsø, Norway, October 15-17, 2014. Proceedings, volume 8788 of Lecture Notes in Computer Science, pages 199–212. Springer, 2014. (20.10.2014)
4. Anis Ben Othman: Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (TRESPASS) (3.10.2014) - *Joint Estonian-Latvian Theory Days at Ratnieki* [*Online*] http://home.lu.lv/~df/tdays-ratnieki/ettekanded.html (10.10.2014)
5. BiZZdesign [WWW] http://www.bizzdesign.com/tools/bizzdesign-architect/ (12.11.2014)
6. Eesti E-Tervise Sihtasutus [WWW] http://www.e-tervis.ee/index.php/et/ (28.11.2014)
7. European Union Agency for Network and Information Security [WWW] http://rm-inv.enisa.europa.eu/tools/t_trick-light (15.10.2014)
8. Federal Office for Information Security [WWW] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html (16.10.2014)
9. Formal Methods & Tools [WWW] http://fmt.ewi.utwente.nl/tools/dftcalc/ (24.10.2014)
10. ISKE rakendustööriist (Lisatud 26.11.2010, uuendatud 24.04.2013) - Elektrooniline Riigi Infosüsteemi Amet [WWW] https://www.ria.ee/isketooriist/
11. Riigi Kinnisvara (2011) *ISKE Nõuete Rakenamine Riigi ja Kohaliku Omavalitsuse Uusehitistele*, 3-5 [*Online*]

http://www.rkas.ee/files/ISKE%20n%C3%B5uete%20rakendamine%20riigi%20ja%20kohaliku%20omavalitsuse%20uusehitistele.pdf (1.11.2014)

12. The TREsPASS Project [WWW] http://www.trespass-project.eu/ (10.10.2014)
13. The University of Luxembourg [WWW] http://satoss.uni.lu/members/piotr/adtool/ (24.10.2014)
14. Wolter Pieters, Dina Hadžiosmanovich, Aleksandr Lenin, Lorena Montoya, and Jan Willemson. Poster Abstract: TREsPASS: Plug-and-Play Attacker Profiles for Security Risk Analysis. In Proceedings of the 35th IEEE Symposium on Security and Privacy, 2014. Poster and Extended Abstract.