OpenSecurity

open source solution for public institutions

Project: OpenSecurity
Requirements specification

Document Control Page

Creator	X-NET
Editor	Wolfgang Eibner
Subject	OpenSecurity – Requirements specification
Meeting date(s)	
Meeting location	
Publisher	OpenSecurity consortium
Type	Text
Format	Application/msword
Language	EN-US
Creation date	2013-07-04
Rights	© Copyright “OpenSecurity consortium”.
Audience	☒ internal
Review status	☐ draft ☒ final
Action requested	☐ to be checked by partners present at the meeting

Revision history

Version	Date	Modified by	Comments
0.1	2013-07-04	Wolfgang Eibner	Initial outline
0.2	2013-07-09	Wolfgang Eibner	Some work on Chapter 1
0.3	2013-07-15	Wolfgang Eibner	Some work on Chapter 2
0.4	2013-07-17	Wolfgang Eibner	Interview section in Chapter 2
0.5	2013-07-22	Wolfgang Eibner	Rework and corrections
0.6	2013-07-24	Wolfgang Eibner	Some work on Chapter 3
0.7	2013-07-25	Wolfgang Eibner	Some work on Chapter 3
0.8	2013-07-26	Wolfgang Eibner	Some work on Chapter 3 and 4
0.9	2013-07-28	Wolfgang Eibner	Some work on Chapter 3 and 4
0.10	2013-07-29	Wolfgang Eibner	Final draft
1.00	2013-07-30	Wolfgang Eibner	Fixed typos, etc.; Final version
1.01	2014-09-08	Michela Vignoli	Fixed typos, wording, etc.

Table of contents

1 Introduction

1.1 About this document

This document provides a summarized view on the requirements of the OpenSecurity project. They were identified and evaluated at the first part of work package 2 “Bedarf und Anwendung” (“demand and scope of application”) and should be the origin for OpenSecurity's architecture and software design.

1.2 About the OpenSecurity project

Synopsis of the OpenSecurity project presented at the proposal for KIRAS[i]:

“Open Security should prevent the loss and (un)intentional misuse of sensitive, citizen-related data held by public bodies. The aim of our research is to achieve a higher level of data security and availability, while reducing effort.

To this end, the feasibility and possible implementation of a centralized security layer will be examined based on our experience with intensive computing, anti-virus and encryption. This layer will control, verify, and encrypt any and all communication that takes place on client devices [...].

Open Security will be provided under a license that allows both public verification and customization within heterogeneous ICT-system landscapes.”

The OpenSecurity consortium includes two stakeholders: The “IKT Linz Infrastruktur GmbH” (IKTL) and the “Bundesministerium für Landesverteidigung und Sport” (BMLVS).

1.3 Approach

At a first phase we identified risks and scenarios of data loss, data misuse and malware infection. Based on these scenarios we generated a questionnaire that included both, an inquiry of the currently used data protection mechanism and workflows at the stakeholders as well as questions on the future demand and requirements which should be covered by the OpenSecurity project. Supplementary the questionnaire also dealt with topics concerning the work package 4 “Verschlüsselung” (“encryption”).

The questionnaire was completed with both stakeholders on an interview at 22.02.2013. After that we summarized the results and identified key aspects of the OpenSecurity architecture. With inputs from the consortium meetings in March and June these key aspects were rendered more precisely and constraints and limitations of the architecture were delimited.

Subsequently we generated a list of requirements describing our stakeholders' needs in respect to the key aspects and constraints.

1.4 Further structure of this document

In Chapter 2 the evaluation of demand including the scenarios, the questionnaire, the interview and its findings are covered.

Based on these results key aspects and important use-cases were refined. They and also some constraints and limitations will be discussed in Chapter 3.

Chapter 4 lists the requirements on OpenSecurity architecture which have been generated from the evaluation of demand.

2 Evaluation of demand

2.1 Identified risks and scenarios

Because the OpenSecurity layer should “control, verify, and encrypt any and all communication that takes place on client devices” we decided to identify these risks by looking on possible I/O channels and attached (network) devices (see Figure 1 for an overview).

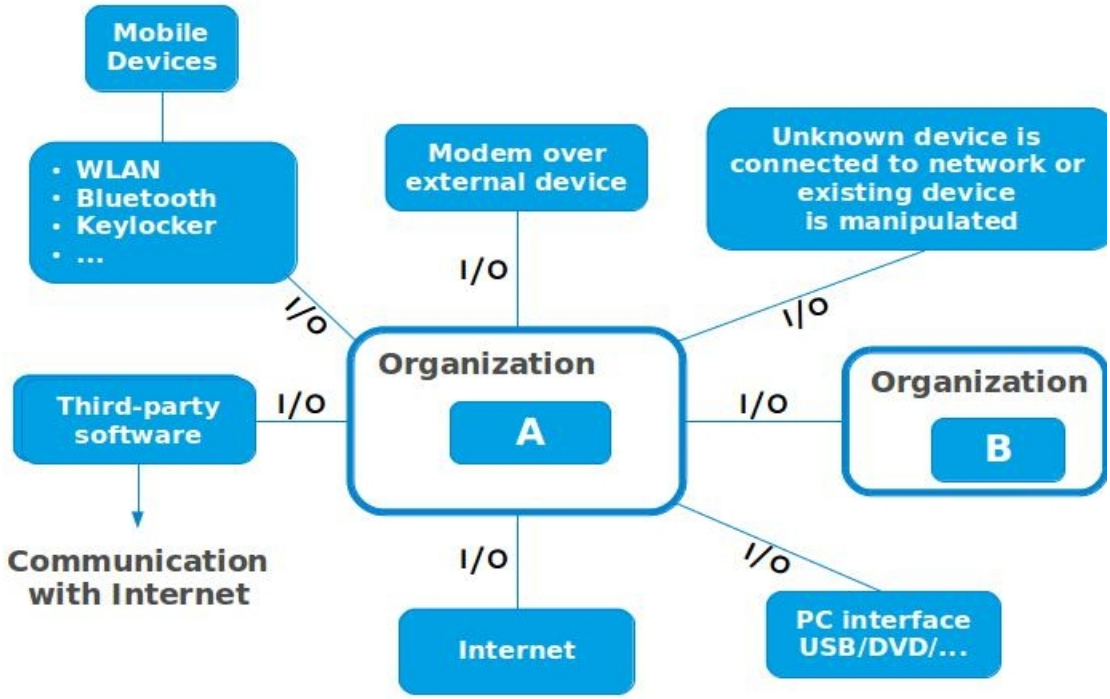

Fig. 1: Identified risks and I/O channels

Based on their primary character of “storage”/device-I/O, the risks can be partitioned into three different groups of risks scenarios (plus a group of remaining ones).

2.1.1 Risk scenario 1 – storage media (USB stick, DVD, Blu-Ray etc.)

- copy and export of data (wilfully/with mischievous intent)
- copy and export of data (on purpose/needfully)
  - loss of storage media
  - third-party misuse (intended transfer and later misuse, unobserved misuse)
  - manipulation of data at transport (break of transmission integrity)

- import of data (on purpose/needfully)
  - permitted
  - not permitted
- import of data (unintentional or with mischievous intent)
  - malware
  - manipulated/erroneous information/content
- boot from storage media (e.g. start of a malicious operating system)

2.1.2 Risk scenario 2 – Internet/(unsafe) LAN connections

- copy/paste/upload
  - by an employee
  - by an application
- sending mail attachments
- download of
  - programs and/or malware
  - manipulated/erroneous information/content
- execution of (already present) malware in the LAN (e.g. from network storages)
- using a smartphone as modem or using alternative Internet connection mechanisms

2.1.3 Risk scenario 3 – usage of mobile devices in- and outside the company

Data is copied without protection while working at the company (on purpose). Afterwards the mobile device (mainly notebooks) is transferred outside the company (e.g. home) and unprotected data is copied to e.g. a UBS stick.

In fact the risks of this scenario are similar to the ones mentioned in scenario 1, but have to be addressed in a different way by the OpenSecurity layer as the mobile device may be used outside to corporate network.

2.1.4 Remaining risks and scenarios

- screenshots / Screencasts
- microphone / Soundcasts
- (web)camera recording, video telephony (e.g. skype)

2.2 Interviews with stakeholders

As mentioned in Section 1.3 we completed our questionnaire[ii] with both stakeholders on an interview at February. The following subsections will cover the results of this interview. A scan of the raw data can be found at [iii].

2.2.1 Data import and export scenario

- data import from and data export to an external storage media should be possible
  - to/from the local client computer
  - to/from a local (secure) network – possibly by temporarily saving the data on the local client computer
- a workflow including a quarantine station/inspection bay is possible, if
  - it can be easily integrated in existing ICT structures
  - all workflows – except errors and security breaches – are automated and do not need supervisor interactions
  - it is simple and fast [IKTL]
  - it can be used without connection to the corporate network and infrastructure – e.g. with reduced features – at mobile devices (offline availability) [BMLVS]

Regarding encryption and decryption of data:

- BMLVS:
  - data should be encrypted before export and (optionally) after import
  - user provides user or group encryption key (this also controls access of privileged persons to the encrypted data)
- IKTL:
  - data should be only encrypted before export
  - imported data will be stored unencrypted on corporate file systems
  - standardized and widely-used encryption algorithms are very important
- importing of data that is already encrypted:
  - no clear opinion by the stakeholders
  - “ask user to decrypt data” sounds like a good option
- logging (especially) data export activities was considered a remarkable feature.

- there should not be any check of transmission integrity (e.g. by hash sums).

2.2.2 Internet/(unsafe) LAN connections scenario

- current and requested situation
  - IKTL: Currently Internet access is given at user workstations controlled by application layer firewalls. Internet access in a possible OpenSecurity environment should still remain easy and fast to use.
  - BMLVS: Currently Internet access is only gained with special client computers outside the corporate network. In future it should be possible to safely access the Internet from the user's workstation.
- after compromise e.g. by malware it should be possible to recover to a clean state easily and fast. But it should be possible to retain user preferences (e.g. bookmarks, cookies) at the Internet access system.
- data import/export from/to the Internet can be done using a quarantine station/inspection bay like at data import/export scenario; however encryption should not be mandatory.
- copy & paste from Internet access to office environment should be possible but possibly be restricted (e.g. only short data).
- e-mails are accessed at the office environment.
- other protocols used which should be considered: FTP, SFTP, FTPS
- how should companies' internal websites (Intranet) be handled? [IKTL]
  - from which environment are internal websites accessed (office or Internet environment/VM)?
  - if Intranet pages link to/use websites, how can they/user gain access to the Internet?

2.2.3 Mobile devices (mainly notebooks) scenario

- mobile workstations:
  - encryption: on principle [BMLVS], mostly not [IKT]
  - offline functionality of OpenSecurity layer requested [BMLVS]
  - during data export handle similarly to external storage devices
- smartphones:
  - no substantial demand at this time [BMLVS]

- already in use and sometimes encrypted [IKTL]

2.2.4 Encryption/Decryption

As already stated the questionnaire also dealt with topics concerning the work package 4 “Verschlüsselung” (“encryption”). The questions basically aimed at evaluating the current situation at stakeholders and their future requirements to encryption features in the OpenSecurity layer.

BMLVS:

- clients and servers are encrypted at filesystem layer
- individual files and folders get encrypted for data transmission
- widely-used and standardized encryption methods have to be secure and certified, e.g. AES and TrueCrypt
- focused on low vulnerability over long time periods (e.g. several years)
- en-/decryption by: certificates and respectively keyfiles and password, public/private keys or smartcards
- used encryption method depends on kind of data and purpose of use (NATO, EU and national guidelines); an in-house algorithm for high security concerns exists

IKTL:

- some mobile clients are encrypted
- partly, individual files and folders get encrypted for data transmission
- focused on practicability at a diversified area of users, thus encryption should be straightforward, fast and easy to apply, e.g. BitLocker and TrueCrypt
- en-/decryption by: password only (mostly)

3 Key aspects and use-cases

3.1.1 Key aspects of the stakeholders

Based on the evaluation of demand in Chapter REF __RefNumPara__176_1832541902 \r \h we identified the following key aspects from our stakeholders:

The focus of BMLVS on OpenSecurity concentrates on guaranteeing long-term security, safe Internet access and a solution with offline functionality for mobile workstations.

Whereas the IKTL is mainly focused on data misuse and data loss prevention, high usability of the OpenSecurity software and an easy integration into their existing ITC infrastructure.

3.1.2 Security zones

For a better and more precise description of use-cases and requirements we recommend to distinguish two security zones used at the OpenSecurity layer.

Secure zone/safe network: Devices, files and workflows respectively within the stakeholders' corporate network. This is where the sensitive information, which OpenSecurity should protect from misuse and manipulation, resides.
This zone in principle is serviced and supervised by the institutions ICT department and operates within well-defined operating parameters and workflows.

Insecure zone/unsafe network: All devices, files, networks and workflows outside the secure zone. E.g. the Internet (and requests to it), private UBS sticks brought in from home, mobile workstations which were meanwhile connected to “unknown” and unsafe networks belong to this zone.
The insecure zone is not – or only to a minimum – under supervision of a stakeholders’ ICT department and thus there can be various unknown or unexpected events and outcomes.

One of the main challenges of the OpenSecurity project is enabling the users, inside a closed and secure local network, to safely work with external resources. Currently the user is on the one hand limited to the institutional safe network dealing with sensitive information within a secure network, which is isolated from the outside world. On the other hand he/she can access the unsafe networks and resources easily, which results in several security threats to the sensitive information.

OpenSecurity tries to control and supervise the data flow between this two zones, enabling the user to work and interact with resources in both zones without losing protection of sensitive data.

3.2 Use-cases

After a detailed discussion of our results we believe that OpenSecurity's architecture should distinguish and deal with three security relevant use-cases[1].

- interaction with removable storage devices (data import/export)
- safe Internet access
- mobile workstations (notebooks)

The next subsections will give an overview about these three use-cases and their major threats according to the risks at Section REF __RefNumPara__218_1832541902 \r \h . Afterwards in Chapter REF __RefNumPara__242_1832541902 \r \h 4 we list requirements to OpenSecurity architecture aiming to avoid these threats.

3.2.1 Interaction with removable storage devices (data import/export)

Workflow description: This workflow deals with the import and export of data from and to a removable storage device like USB sticks, optical media (CD, DVD, Blu-Ray...) and so on. Typically these devices are directly connected to the workstation/client pc of the user which is located in the secure zone. But their origin (at data import) or destination (at data export) resides in the insecure zone.

Major threats at this workflow are:

- Data imported from removable storage devices may be infected by malware which the secure zone should be protected from. This gets even more difficult if the device or parts of it are already encrypted and thus not directly available for virus scanning.
- Data exported to removable storage devices reveals sensitive information to insecure zones making it available to e.g. loss or theft.

User story: The user wants to access a file, residing on an external storage device (e.g. USB memory stick), modify it using a computer within the safe network and save it back to the same device for transport or to a local network share.

The file can – but does not necessarily have to – contain sensitive information. Considering the first more sensitive scenario certain files or the entire content of the storage device might be encrypted. At the same time the storage device could contain harmful code that should be identified and, if possible, be removed or the containing files should be quarantined.
The user might choose to encrypt his data upon saving (exporting) to an external storage device.

[1] In fact they are similar to the three risk scenarios at Section .

3.2.2 Safe Internet access

Workflow description: The second workflow deals with user requests to the Internet and involved actions like file down- and uploads. At BMLVS this is currently done via special workstations which are not connected to safe network. Future solutions should enable users to directly use their office workstations in order to raise usability. At IKTL Internet access currently occurs directly from office workstations within the secure zone.

Major threats at this workflow are:

- Connecting the secure zone with insecure ones like the Internet.
- A possible infection with malware or the import of unwanted data and programs into the secure zone.
- Data misuse and loss through export of sensitive information from secure zone to the Internet (e.g. at upload or by copy & paste).
- Applications communicating (hidden in background processes) and thus a unregulated data flow to third-parties.

User story: The user wants to retrieve a resource from the unsafe network and process it on the safe network. The user has to be able to use a web browser in order to locate, download, store or copy the resource to the clipboard.

3.2.3 Mobile workstations (notebooks)

Workflow description: The third security relevant use-case is dedicated to mobile workstations. These workstations (mainly notebooks) are run by stakeholder employees inside the secure zone as well as in insecure zones (e.g. home working, field service). Through mobile use and changing between security zones there are different requirements for securing Internet and storage access.

Major threats at this workflow are:

- Export of sensitive data inside secure zone to the mobile workstation and subsequent use/transfer in insecure zones afterwards.
- Import of maybe malicious data in insecure zone to the mobile workstation. Afterwards the mobile workstation and also its data gets (re-)connected to the secure zone.
- The mobile workstation is not under control and supervision of the stakeholder's ICT department while it is being used in insecure zones. Additionally a possible OpenSecurity solution could lack functionality if it relies on central components located at the stakeholder's network.

User story: After working outside the institutional boundaries (connected to untrusted networks) and being exposed to various threats, the user's notebook eventually re-joins the safe network.

Due to the high risk of external networks the machine is assumed to be compromised and needs to be malware checked and declared secure prior to allowing access to the safe network.

3.3 Constraints and limitations

The OpenSecurity project will be limited to the three use-cases presented above. Therefore e.g. risks like screenshots, manipulations with direct physical access to a workstation (e.g. keylogger devices) and booting malicious systems from removable media will not be addressed by the project. Most of them can be prevented by access restrictions (e.g. BIOS password) or other policies.

Security of mobile devices (smartphones, tablets, etc.) is not in the scope of the project as these devices use a plethora of proprietary software and no generic solution can be implemented. We will still consider the smartphone as storage or network device.

Usability and non-functional requirements at workflows and user interfaces are only partially handled in this document as they are part of work package 6 "sozial-relevante Forschungsfragen" ("social-relevant research issues").

4 Requirements

4.1 Interaction with removable storage devices (data import/export)

#	Description
1	**Interaction with removable storage devices**
1.1	Device must not be connected/must not be available (natively) to secure zone in order to prevent execution or insertion of malicious code.
1.1.1	At any time it is strictly forbidden that a user gains access to the device and its data inside secure zone without using OpenSecurity client and its workflow.
1.1.2	Device shall be connected to a system that ideally cannot natively execute code residing on the device.
1.2	Users shall be instructed to connect the device following a predefined workflow and use OpenSecurity client to import/export data from/to device.

2	**Data import from removable storage device into secure zone**
2.1	User should be able to select device and data for import and if necessary, destination to store imported files.
2.1.1	Selection of destination should be possible from client's local filesystem as well as from (connected) network shares inside secure zone.
2.2	If a device or specific data on it seems to be encrypted the user should be prompted to decrypt the data prior to starting the import workflow.
2.2.1	If decryption is not possible or the user refuses it, encrypted data may not be imported to secure zone.
2.2.2	Unencrypted data should be quarantined and checked by a supervisor.
2.3	Data must be virus-checked prior to import.
2.3.1	Virus check has to be performed after a maybe necessary decryption.
2.3.2	Data failing virus check should be quarantined and checked by a supervisor.
2.4	At the end of import workflow decrypted and virus-checked data shall be copied to a location which is available to user in secure zone or to destination user has chosen.
2.4.1	[Optional] Prior to copying data to its final destination it should be encrypted according to stakeholders' predefined methods.

3	Data export from secure zone to a removable storage device
3.1	User should be able to select data for export and destination (on device) to store exported data.
3.1.1	Selection of data to export should be possible from client's local filesystem as well as from (connected) network shares inside secure zone.
3.2	[Optional] Data should be virus-checked prior to export.
3.2.1	Data failing virus check should be quarantined and checked by a supervisor.
3.3	Data must be encrypted prior to export according to stakeholders' predefined methods.
3.3.1	Data encryption has to be performed after (the optional) virus check.
3.3.2	User has to provide necessary data (e.g. password or key) for encryption.
3.4	Data export should be logged centrally at minimum including timestamp, user and paths of exported data.
3.5	At the end of export workflow data shall (optionally) be virus-checked, and encrypted data shall be copied to device – which will be brought outside secure zone – and destination chosen by the user.

4.2 Safe Internet access

4	Safe Internet access
4.1	As Internet access and Internet is considered insecure its workflows have to be separated from secure zone.
4.1.1	A user should be able to gain Internet access directly from his/her workstation. Thus he/she should not have to use another workstation in insecure zone or in a demilitarised zone (DMZ).
4.1.2	“Directly from his/her workstation” should be interpreted physically and thus it does not prohibit solutions like VMs, terminal server sessions etc.
4.1.3	At any time all data flows between Internet/insecure zone and secure zone that do not rely on OpenSecurity workflows are strictly forbidden.
4.1.4	Accessing and working with e-mails is not necessarily part of safe Internet access as e-mails are accessed within the office environment.
4.2	After compromise e.g. by malware it should be possible to recover to a clean state of safe Internet access system/solution easily and fast.
4.2.1	But it should be possible to retain user preferences (e.g. bookmarks, cookies) at the Internet access system.
4.3	Other protocols used which should be considered: FTP, SFTP, FTPS.

4.4	Handling of companies' internal websites (Intranet) should be examined and considered.
4.4.1	From which environment are internal websites accessed (office or Internet environment/VM)? If Intranet pages link to/use websites, how can they/user gain access to the Internet?

5	**Data import/export at safe Internet access**
5.1	The user shall be able to retrieve content, resources or information from the Internet (insecure zone) and process it within the secure zone.
5.2	The user shall be able to upload content, resources or information from secure zone to the Internet.
5.3	Data import/export from/to the Internet can and should be done similar to workflows at REF __RefNumPara__244_2124892175 \r \h 4.1.
5.3.1	Encryption at data export to the Internet should not be mandatory.
5.3.2	Copy & Paste from Internet access to office environment should be possible but possibly be restricted (e.g. only short data).

4.3 Mobile workstations (notebooks)

6	**Mobile workstations (notebooks)**
6.1	In principle mobile workstations and their workflows should be treated like normal user workstations. This includes safe Internet access as well as interaction with removable storage devices.
6.1.1	Workflows from safe Internet access and interactions with removable storage devices should also perform if the notebook is outside the institutional boundaries/secure zone (offline availability).
6.1.2	This offline availability may offer a reduced feature set only.
6.2	If a notebook re-joins the secure zone after being outside the institutional boundaries (connected to unsafe networks) it is assumed to be compromised and therefore needs to pass an OpenSecurity check.
6.2.1	This check shall contain all necessary steps, e.g. malware scanning, to ensure a clean and trustworthy system that cannot compromise the secure zone.
6.2.2	Prior to passing OpenSecurity check no access between the notebook and secure zone is allowed.

4.4 Non-functional requirements

7	Non-functional requirements
7.1	OpenSecurity architecture shall have a modular concept.
7.1.1	Malware scanning should be connectible to different scan-engines.
7.1.2	Malware scanning should be done on local client or on a central server/cluster.
7.1.3	Encryption should be exchangeable to allow different/more-than-one encryption algorithms.
7.2	Used encryption methods should be standardised and widely-used.
7.3	All OpenSecurity workflows – except errors and security breaches – shall be automated and shall not need supervisor interactions.
7.4	All OpenSecurity workflows should be fast and easy to use.
7.5	OpenSecurity layer should incorporate easily into existing ICT structures.

[i] KIRAS_foerderungsansuchen_kooperative_fe-projekte_Open_Security_FINAL.pdf located at http://www.opensecurity.at/projekt/antrag/KIRAS_foerderungsansuchen_kooperative_fe-projekte_Open_Security_FINAL.pdf

[ii] 20130122_Fragebogen_Bedarfserhebung.odt located at http://www.opensecurity.at/arbeitspakte/ap2-bedarf-und-anwendung/bedarfserhebung/20130122_Fragebogen_Bedarfserhebung.odt

[iii] interviews_bedarfserhebung.pdf located at http://www.opensecurity.at/arbeitspakte/ap2-bedarf-und-anwendung/bedarfserhebung/interviews_bedarfserhebung.pdf