

Ftp server in a data diode

Rusu George, Boulif Ilias, Orinx Cédric

December 6, 2017

Contents

| | | |
|----------|--|-----------|
| 1 | Concept of operations | 3 |
| 1.1 | Introduction to the problem | 3 |
| 1.2 | Our solution | 3 |
| 1.3 | Our System description | 4 |
| 1.3.1 | Hardware | 4 |
| 1.3.2 | Software | 4 |
| 1.3.3 | First overview on the project implementation | 5 |
| 1.4 | Users | 5 |
| 1.5 | User Interface | 6 |
| 1.6 | Usage of the WEB UI | 9 |
| 1.6.1 | General usage | 9 |
| 1.6.2 | A Technical file transfer usage | 9 |
| 1.6.3 | Configuration panel for the admin | 10 |
| 1.6.4 | Installation | 11 |
| 2 | Risk Analysis | 12 |
| 2.1 | Introduction to the risk analysis | 12 |
| 2.1.1 | Physical Assets | 12 |
| 2.1.2 | Logical Assets | 12 |
| 2.1.3 | Persons involved into the company | 13 |
| 2.2 | Threat Sources | 13 |
| 2.2.1 | Unpredictable events | 13 |
| 2.2.2 | Predictable events | 14 |
| 2.3 | Risks assessment | 14 |
| 2.3.1 | Levels of impact, likelihood and risk | 14 |
| 2.3.2 | Threats affecting physical assets | 15 |
| 2.3.3 | Threats affecting logical assets | 17 |
| 2.3.4 | Threats affecting persons | 19 |
| 2.3.5 | Summary table | 20 |
| 2.4 | Countermeasures | 20 |
| 2.5 | Residual risk | 21 |
| 3 | Implementation | 22 |
| 3.1 | Simulation of the data diode | 22 |
| 3.1.1 | Machine installations | 22 |
| 3.1.2 | simulation un seul sens | 22 |
| 3.2 | deployeibt de bftp | 22 |
| 3.3 | interface Web data diode | 22 |
| 3.3.1 | interface de configuration | 22 |
| 3.3.2 | ajout de vftp dans l'interface | 23 |
| 3.4 | control recommendation | 23 |
| 4 | Test and demo scenario | 23 |

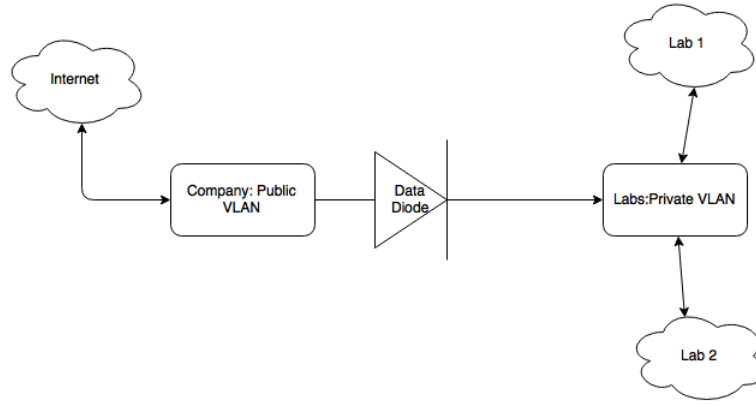


Figure 1: The schema of the usage of a data diode in a company network.

1 Concept of operations

1.1 Introduction to the problem

Our client would want to prevent his research and development labs against industrial espionage and confidential information leaking. He wants to divide the company network in order to maintain the labs in an isolated environment. Thus, the critical data could not leave the company using the network. But how to be able to transfer files or to assure that all the operating systems are up-to-date? This could be achieved using manual operations where an employee would manually copy the files or the updates on a mass-storage device¹ and then used them or install them on every node from the isolated network. However, this is not the most optimized way and for sure it is not cost less and timeless for the company, without mentioning that there could be dependency problems for applications or updates. This method is also prone to human errors and this could generate security vulnerabilities.

1.2 Our solution

In order to address this problem we are going to implement a data diode. In electronic, a diode is a component which conduct the current in one direction. Thus the term of data diode is a set of components that only let the data to travel in an unidirectional way. An example of use case is illustrated in Figure 1, letting the data pass from a low risk LAN to a high risk LAN but not the way around.

A data diode is made using one transmitter(Tx) and one receiver(Rx) both linked using only one fiber cable. Thus, when a digital data is sent through, every bit will be converted² into an electrical pulse which will be convert in light pulse using a LED³. Then, the output light will pass trough the fiber cable and as soon as the photons are reaching the receiver, they will be converted firstly into an electrical pulse by a photo diode and then in bits⁴. Since there is only one fiber, data can only travel in one way.

One major problem of this system is the network transport protocols(layer 4 in the OSI model) that applications are using. The most used transportation protocol nowadays is TCP. However, TCP is a bi-directional protocol which need the 3 way handshake in order to start a connection, thus there must be at least two fiber cables. In contradiction, UDP does not require a handshake process because it does not provide reliability, ordering, data integrity and does not set up a dedicated end-to-end connection automatically. Thus, UDP protocol does not necessary require a bi-directional data transfer. Therefore, the use of such a protocol is recommended when dealing with applications that are not sensitive to data loss or that implements an error checking system. Hence, the use of the UDP protocol within the data diode.

It seems obvious now that the transport protocol used between the transmitter and the receiver of the data diode is UDP. However, this brings multiple problems. One of the problems is how to be able to use applications that requires TCP. Another problem could be the reliability of the digital data transfer in the data diode, how can we ensure that there will not be any data loss during the transfer. We will address to those questions further down in this document.

¹A USB-key for instance.

²Using a Digital-to-analog converter (DAC).

³Light Emitting Diode.

⁴Using an analog to digital converter (ADC).



Figure 2: Data logical path within the data diode.

Furthermore, system administrators would dispose of a file transmission mechanism from the low level to the high level in order to maintain all the computers up to date. This will be done using the FTP protocol and will be explained in the next section.

1.3 Our System description

The data diode concept is well orchestrated combination between hardware and software. The data diode is composed of two servers: a transmitter and a receiver. We could consider that the transmitter server is connected to the low security risk LAN where a connection to the internet is made and where all the employees are connected. The receiver is connected to the high security risk LAN where all the labs are connected and where critical informations are stored.

The transmission of the information will be from the low side to the high side and blocked the way around as shown in Figure 2.

1.3.1 Hardware

The following table presents the components used for the data diode implementation. We should mention that both transmitter and receiver possess two NICs⁵: one for the communication within the LAN and one for the data diode.

| Components | Description |
|------------------------------------|---|
| Transmitter server | a physical machine or a virtual machine. The NIC for the data diode will be set in transmission mode only. |
| Receiver server | a physical machine or a virtual machine. Similar to the transmission, the NIC will only be set in a receiver mode. |
| One fiber cable | This optical fiber allows communication between the low server and the high server. |
| Two fiber NIC and two UTP/RJ45 NIC | On each side, there will be one fiber NIC for the data diode and one UTP/RJ45 NIC for the communication in the LAN. |

Table 1: Components description

1.3.2 Software

The Linux distribution which will be used in our project will be Ubuntu 16.04 LTS. We will have two linux machines, one on the transmitter side and one on the receiver side.

The data diode will be easily administrated using a web interface running on a Django server. The web interfaces will be hosted on both servers according to the server location in the company network (transmission interface on the transmitter server, same for the reception interface). It will be described in more details further in this document.

Every configuration script used by the web interfaces will be a combination of Python language and Bash language.

⁵Network interface controller.

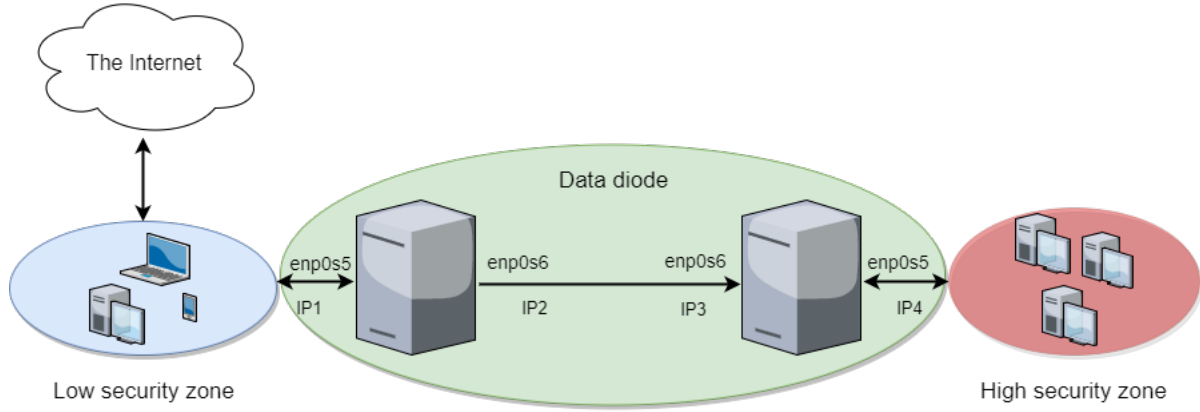


Figure 3: Entire system.

1.3.3 First overview on the project implementation

Let's start by explaining which protocol shall be used in the data diode. Remember that our main goal is to create an isolated environment but also to facilitate the files transfer process to the high security zone. As we mentioned earlier, we are going to use the FTP⁶ protocol. There are some alternatives to FTP such as BlindFTP, SFTP, etc. However FTP and SFTP are using TCP as their transportation layer protocol. Thus, we are going to use between the transmitter and the receiver the BlindFTP which use UDP instead.

BlindFTP is a simple Python script which was especially created for the communication between the two servers over an unidirectional network. It is simply a tool for transferring files from one side to the other. Despite the fact that it uses UDP, there is no acknowledgement of received packets but this is compensated by a redundancy of the data. An other advantage is the language used, as it is written in Python the result code is relatively simple and very portable to Windows, Linux or MacOS.

It is now time to have a look at our entire system, let's have a look in Figure 3.

We should note that between the transmitter and the other peers a TCP connection can be used to communicate (transmitter web interface). And this is the same for the receiver, after the data goes out from the network diode the transportation protocol could be TCP with other computers (receiver web interface). In this way, we are not dealing any more with the problem of application transportation layer.

1.4 Users

In general every employee of a company has a unique ID, a grade, a job title and so on. The company owner or the manager in charge with the security could choose which grade or which person can have access to the administration web interface, of course this exclude the systems administrators. Every user information is managed and stored by the company in their own databases and this is a requirement for the working of the data diode. Despite that this is out of our scope, we will assume that our client has his own users database and we will consider two types of users to make our explanation simpler : the *administrators* and all others *users*.

A *user* is simply an employee of the company. Every employee has limited access into the company's files according to their job title or to the specific rule defined by their supervisor.

An *administrator* is a user in charge of operating and maintaining the data diode. It is the only authorized person to configure or maintain the well operating of the data diode and this is mandatory. He will have to know how the data diode is working, should know how to interact with it using the web interfaces but mostly he should be able to reconfigure it or restore it as quickly as possible in case of a security breach or a system failure. We should not forget to mention that an administrator should not have access to some strict secret files of the company but only to IT department files.

⁶File transfer protocol.

1.5 User Interface

As we mentioned earlier, the administration of our data diode will happen through a web interface. There will be one web interface hosted on the transmitter which will allow to transmit files or update packages from the lower network to the higher network. But, on the other hand there will also be a receiver web interface for each user to manipulate his transferred data more easily.

Each user should log in from both side to use the platform. Here is an overview of our log in page:

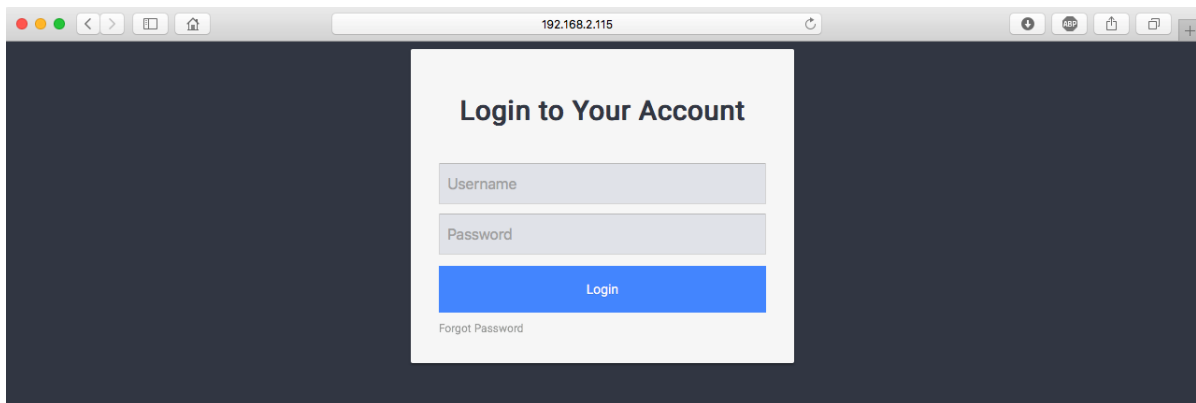


Figure 4: Login page.

Once login is made, the user will be prompted to the web interface of the transmitter or the receiver. The page are shown in Figure 5 and Figure 6.

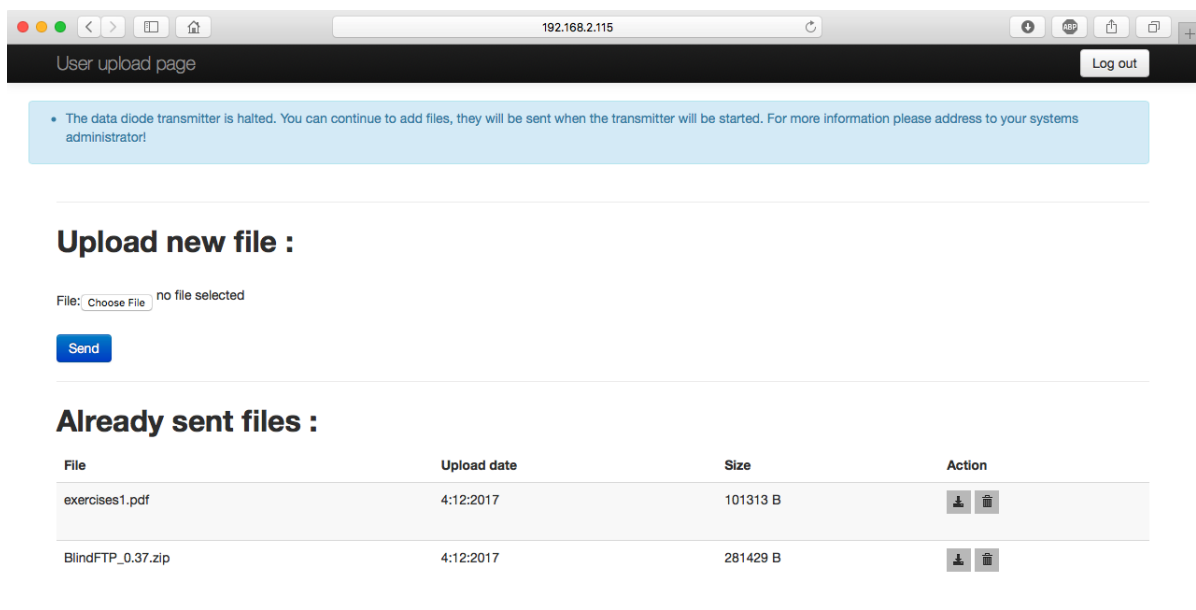


Figure 5: Transmitter user page.

On the other hand, an administrator can transfer files or he can upload an update package from his own computer. The admin. interface is shown in Figure 7 and in Figure 8.

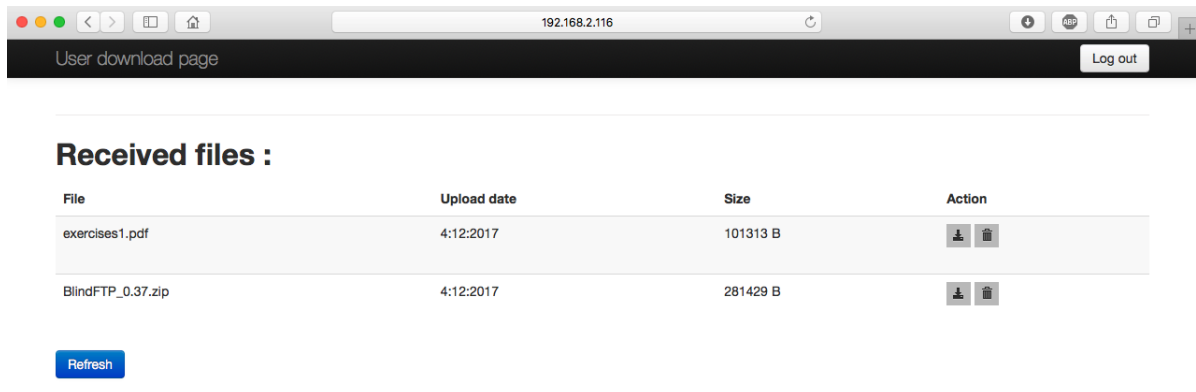


Figure 6: Receiver user page.

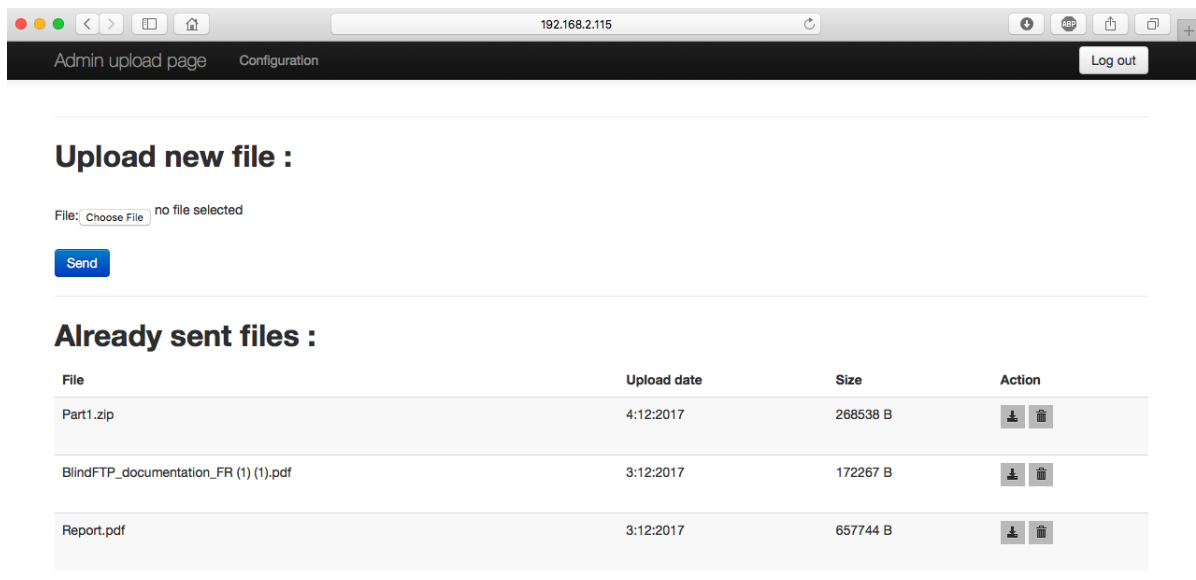


Figure 7: Transmitter admin page.

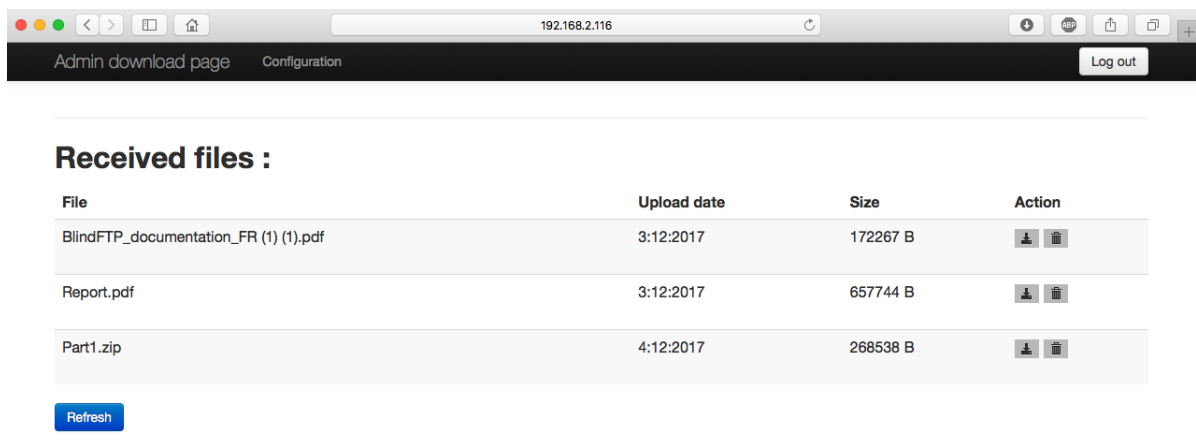


Figure 8: Receiver admin page.

1.6 Usage of the WEB UI

In this section we will explain how to use our web interfaces from different point of views.

1.6.1 General usage

In both cases, all users have to identify themselves through the login page with their credentials. They must fill in the form with their own username and password (Figure 4). Once the form is submitted, the authentication will bring them respectively to their dedicated page.

In the case of a user connection, he will be redirected to the user transmission page according to his network location: if he is in the low security zone he will be prompted to use the transmission interface (Figure 5) or he will get the receiver interface page (Figure 6) if he stand on the high security zone (after the data diode).

On the transmission page the user can choose among his own documents a file to send through the data diode by using the *send* button. On the reception page, the user has a list of all the received files which he can refresh, download or delete.

When an administrator will log in, similarly to the user mechanism, he will be redirected according to his network location : on the transmission interface or on the receiver interface, respectively Figure 7 and Figure 8.

On the transmission page, in addition to a simple user, the administrator has the power to configure the data diode, this will be presented later in this document.

On the reception page, the administrator has access to only his transferred files through the data diode. In this way, we are sure that the confidentiality is preserved by the administrator.

If an administrator wants to maintain (updates) the company's computers he could download on his machine the needed update packages and transfer them easily to the high security zone. All this is made possible thanks our interface and file transfer system. He can then update all the machines using some Linux script or to use the web interface to download each update package manually on the desired machine. Of course the latter method is not the most optimal but it could serve in case of a need for a system downgrade or an application downgrade on a workstation.

1.6.2 A Technical file transfer usage

We have said earlier that there will be a web interface running on both side of the data diode. When a user will want to send a file, he would have to first log in. The log in page will use the database of the company in order to authenticate users and to verify each user permissions. However, on the high security zone, the database would not be reachable because of the unidirectional data diode. Thus, once a user would want to send a file to the other side, there will be a daemon which will create a permission and ownership system in order for the other side to recognize to whom the file belongs to:

- For *UserX* the folder will be named $\triangleright SHA256(UserX+isAdmin);PBKF2SHA256(password)$.
- For every *UserX*'s file, it will be copied in the *UserX*'s folder and renamed $\triangleright timestampUpload;filename$.

On the other side, there will be of course another receiver daemon which will according to all received folders create the database. Indeed, when the *UserX* has already sent a file, the receiver will get in the receiver folder the corresponding *UserX*'s folder. When the user would want to log in, the daemon will check his credentials with the folder name. If it is a match, then the user *UserX* will be inserted in the receiver database. He will then have access to the web platform and to his sent files. Of course there is also a second daemon which for every user's folder will read and list all the files properly to the user:

- The received file *timestampUpload;filename* will be shown to his owner as $\triangleright filename$ and with others property such as the size and the date when the file was uploaded into the data diode.

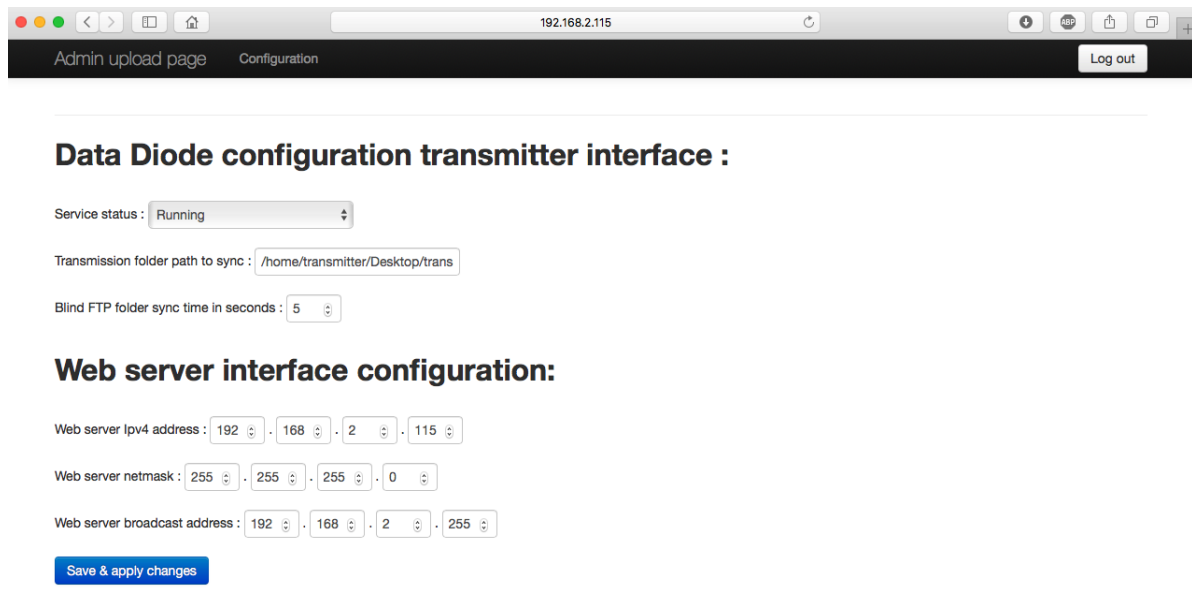
In this way, the main verification will take place on the transmitter side where the database can be accessed : if a user has the permission to transfer a file, he will be able to transfer the file from the transmitter side. Thus, if the file is transmitted to the receiver side, it means that the user has an access granted on the security zone and thus he has already been verified. However, if a user has not yet used the transmission system of the data diode, he will not be able to connect to the interface from the receiver

side. Once the user has been added to the security zone database, then the log in process will no longer use the folder checking daemon but instead will query directly the database as usually.

It is very important to mention that employee's name and password will not be shared in clear text, a hash of SHA-256 will be used for the employee's name and the isAdmin property and a PBKF2SHA256 will be used for the password.

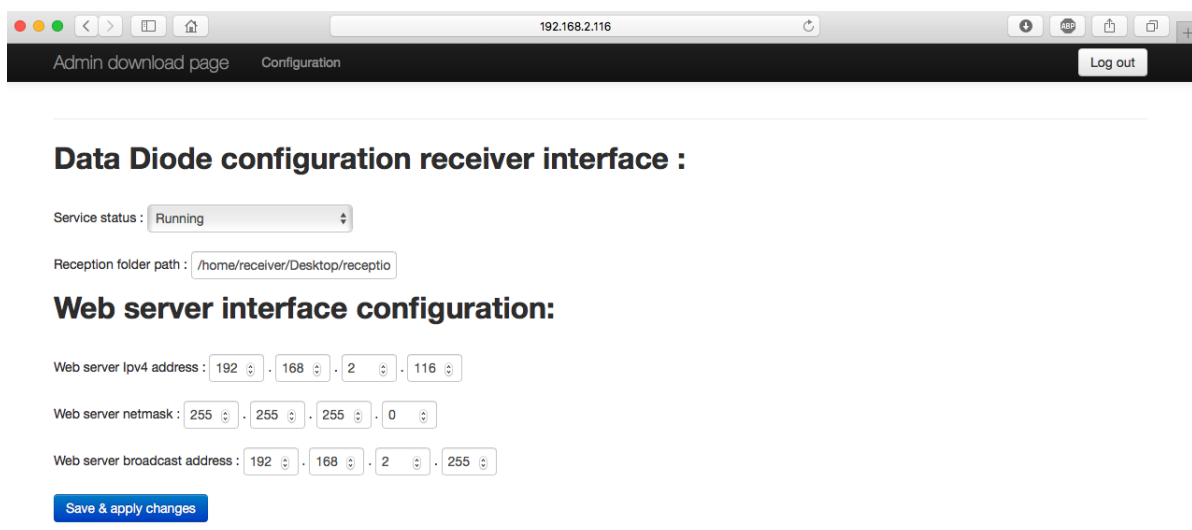
1.6.3 Configuration panel for the admin

The admin can configure the IP address of both the transmitter and the receiver. In this case, we are not talking about the communication within the data diode but about the communication to other peers of the network. Furthermore, he has the power to configure the data diode : he can start/stop the file transfer protocol and change the transmission/reception folder.



The screenshot shows a web browser window with the address bar displaying 192.168.2.115. The page has a dark header with 'Admin upload page' and 'Configuration' tabs, and a 'Log out' button. The main content area is titled 'Data Diode configuration transmitter interface :'. It includes a 'Service status' dropdown set to 'Running', a 'Transmission folder path to sync' text input field containing '/home/transmitter/Desktop/trans', and a 'Blind FTP folder sync time in seconds' spinner set to 5. Below this is a section titled 'Web server interface configuration:' with three rows of IP address configuration: 'Web server ipv4 address' (192, 168, 2, 115), 'Web server netmask' (255, 255, 255, 0), and 'Web server broadcast address' (192, 168, 2, 255). A blue 'Save & apply changes' button is at the bottom.

Figure 9: Configuration panel for admin on the transmitter side.



The screenshot shows a web browser window with the address bar displaying 192.168.2.116. The page has a dark header with 'Admin download page' and 'Configuration' tabs, and a 'Log out' button. The main content area is titled 'Data Diode configuration receiver interface :'. It includes a 'Service status' dropdown set to 'Running', a 'Reception folder path' text input field containing '/home/receiver/Desktop/receptio', and a section titled 'Web server interface configuration:' with three rows of IP address configuration: 'Web server ipv4 address' (192, 168, 2, 116), 'Web server netmask' (255, 255, 255, 0), and 'Web server broadcast address' (192, 168, 2, 255). A blue 'Save & apply changes' button is at the bottom.

Figure 10: Configuration panel for admin on the receiver side.

1.6.4 Installation

Set up The following steps should be followed in order to have a fully operational data diode:

1. **Network settings** The administrator has to connect to machines using the following credentials:

- On the transmission side ▷ user: transmitter & password: abbaabba
- On the receiver side ▷ user: receiver & password: abbaabba

Once logged in, he should edit the files⁷ according to the company's LANs settings. These files are located at:

- For the transmission side : `/home/transmitter/Desktop/DataDiodeTransmitter/interfaces`
- For the receiver side : `/home/receiver/Desktop/DataDiodeReceiver/interfaces`

Both web interface should be now accessible from a browser on port 8080.

WARNING: The passwords for both machines should be changed!

2. **Linking the company database with the transmitter authentication system** The administrator has to edit the file at `/home/transmitter/Desktop/DataDiodeTransmitter/DataDiode/settings.py` and change the database configuration to the company's database configuration. The authentication on the transmitter side should now be operational.

3. **Enabling *Blindftp* reception on the receiver side** Log in on the receiver side using username: admin & password: admin and enable *Blindftp* reception service.

WARNING AT YOUR OWN RISK: The default account username: admin & password: admin can be disabled in the file located at `/home/receiver/Desktop/DataDiodeReceiver/DataDiode/settings.py` by changing the `ADMINACCOUNT` attribut to 1 instead of 0. However, after a system restart, the data diode reception should manually be enabled if the receiver database is empty

WARNING: The default account will be automatically disabled at first log in.

NOTE: The default account has not the power to see sent files.

4. **Enabling *Blindftp* transmitter on the transmission side** Turn on the transmitter *Blindftp* service and test it by sending a file.
5. **Checking the receiver side reception** On the reception side, the administrator should now be able to connect using his company credentials and he should have received the sent file.

The data diode should be fully operational.

BACKUP OF ALL FILES HIGHLY RECOMMENDED: The administrator should now backup/compress all the files in order to restore the data diode configuration in case of anything goes wrong.

Restoring to factory settings Restoring the data diode to its factory settings could be needed in case of a system failure. We recommend following those steps:

1. **Delete all files related** For this we recommend deleting all files from the directories :

- For the transmission side : `/home/transmitter/Desktop/DataDiodeTransmitter/`
- For the receiver side : `/home/receiver/Desktop/DataDiodeReceiver/`

2. **Deploy a backup** If a backup folder was created according to the installation section, copy it in:

- For the transmission side : `/home/transmitter/Desktop/`
- For the receiver side : `/home/receiver/Desktop/`

Normally the data diode should now be restored at the same point it was after the installation.

SUPPORT For further questions or problems please contact our support center at (+)32 800800.

⁷We are assuming that an administrator should be able of editing the configuration file of a Linux operating system network interfaces.

2 Risk Analysis

2.1 Introduction to the risk analysis

In this section, we are going to assess any risk that could harm or lead to the destruction of our data diode. But first, let's define what is a risk: *A probability or threat of damage, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action*⁸. Generally, the term risk is associated with the probability of occurrence of a damage or a loss during an event. Thus, we can illustrate the risk by the following rule:

$$Risk(e) = impact(e) \times likelihood(e), \forall e \in Events$$

In our risk analysis we will start by defining all the assets of our project. Those assets could be threatened by some hackers which could exploit some vulnerabilities found and harm the entire system. Hence, the need to assess all potential threat sources and all the vulnerabilities and their impact. Finally, we will conclude by presenting some countermeasures.

2.1.1 Physical Assets

An Asset can be physical such as computers or printers. In our client work space, we could have the following components categorized as physical assets:

- All the computers of the low security zone. Those computers could be employee's personal workstations such as laptops but also company's desktop workstations.
- All the company's firewalls systems (routers and switch). Despite the fact that they are not part of our implementation, they could represent a potential asset for malicious persons. This could lead afterwards to the attack of our data diode.
- Our data diode implementation. This comprises our transmitter server and our receiver server.
- Data diode web servers for the web user interface.
- The company database server.
- All the computers within the high security zone.
- All the servers of the company such as Mail servers, FTP servers and other services servers. This comprises the servers in low and high risk networks.

To all those components a stakeholder would want to have physical access in order to harm the well being of our client company. Thus, it is very important that the physical integrity of every equipment shall be preserved. In other words, a physical access to some physical assets such as routers or servers could harm or destabilize the company core system which could easily be done for example by simply cutting the power source cable or by disconnecting the internet cable of the main server, compromising his availability).

2.1.2 Logical Assets

A logical asset could be a sensitive information. A list of logical assets used by our client's company could be:

- The company data base containing sensitive information.
- The data diode web interface.
- Data on the hard drives of every employee personal computer or desktop workstation used for company purpose.
- Data within the research labs.
- Company's storage system.
- Company's operating systems: this contains also every application used within the company. For example the Microsoft Office Suite.

In other words, logical assets represent all the sensitive information which belongs to the company and all the software and applications used by the company's employees.

⁸Definition from the businessdictionary website.

2.1.3 Persons involved into the company

At this point, we should identify every person in the company which could have access to some physical and logical assets. Generally in a company, there are several departments where employees or contractors are working. In order to be able to distinguish every user, we should tag every user with a value according to his loyalty and his hard work for the company. Let's fix 4 valuable stage:

- Very loyal and very hardworking employee.
- Loyal and hardworking employee.
- Not loyal and not hardworking employee.
- Contractors.

It should seem obvious that a very loyal employee which invest a lot of time and work is unlikely to want the destruction or the malfunctioning of the company, because he knows that he will probably lose his job. On the other hand, a non-loyal employee or a contractor could easily want to destabilize the company activities for any kind of reasons such as, an employee could receive a job offer from a competitor, or a contractor who has not been paid yet for his work. Another reason could be industrial espionage, an employee could be a spy.

However, as we do not know every employee of our client's company and because it is out of our scope, we will simplify the picture by mainly focusing on the administrators and in general the other users. Thus, there are two categories of persons :

- The administrators which could have a disastrous impact, they have access to both logical assets and physical assets.
- All other users which could have a moderate impact, they only could have access to physical assets.

Thus, identifying users using a value tag could be very useful when identifying potential threat sources. However, verifying employee loyalty and implication has to be done and pursued only by the company itself.

2.2 Threat Sources

As we mentioned earlier, identifying potential threat sources can be a difficult operation. However, a system failure could be caused by inevitable events or in contrary, it could be caused by a lack of interest (security by obscurity). In order to have a clear view over these kinds of events, we will present all those events using two categories:

- Unpredictable or inevitable events.
- Predictable or avoidable events.

2.2.1 Unpredictable events

Such events could be related to natural disaster which cannot be always predicted in advance. Thus, there is no way in which to prevent the mass destruction, however the company could take some measures in order to minimize the impact. Such events could be:

- Earthquakes.
- Storms.
- Floods.
- Sinkholes.
- Volcanic eruptions.
- Tsunami.
- Wildfires.

However, some event could have a much higher probability of appearance depending on the location where the company has her headquarters. For example, it is more likely to have floods or a tsunami if the company is located near the equator of the globe or in a tropical area, similarly wildfires could occur much often in warm regions. Hence, the importance of the company's location chosen. For example, the company could prevent some of those events by choosing where to host their main servers or by implementing measures such as water or fire sealing doors for the labs.

2.2.2 Predictable events

We can define predictable events as security lacks that we are or not acknowledged about in our system. The administrators could secure the systems by not divulging the vulnerabilities or the backdoors left. This is what *security by obscurity* means, however this is a very bad idea and should be avoided! We defined a list of persons which could be implicated in the hacking action of our client's company system, those persons could be aware of the vulnerabilities of the system or not. Such persons could be:

- Employees or company daily users
- Administrators
- Visitors or unauthorized users
- Script Kiddies
- Skilled Hackers

Each one in this list could be a potential threat source or serve as so. If the company network for example is vulnerable, our data diode could potential be threatened.

Let's assume the following scenarios in which the system could get infected.

After a lot of work and time spent on projects for the company, an administrator or simply an employee could for example make a mistake which could destabilize the entire system. As an example, we could assume that an administrator forget to close a configuration port or an employee could share without his willing his log in credentials. As we said earlier, tagging every user of the company using a value could be a good thing when assessing the threat source. Indeed, a valuable employee despite his tiredness would for sure look twice before finishing his work or sharing some sensitive information of the company. But this is not the same for a newbie which just started on his new job.

Furthermore, having visitor into the company can be a good thing for the image and the brand, however it could be very dangerous. Assuming that a visitor could install a *Femtocell* into the company which could get him full access into the network. Despite the fact that it would be for sure the low security network, the malicious user could sniff every network packet transiting through and thus could steal some information.

For the last two categories, they represent a constant threat for every company. Hence the need for a security policy always up to date and a good strategic network and workstation deployment in order to minimize the risk. Those categories could exploit the vulnerabilities left in the system by administrators using the *security by obscurity* concept.

2.3 Risks assessment

In this section, we will give a set of possible threats that we should take into account in order to secure the most possible our data diode. In order to have a clear view, we will explain every threats by ordering them according to the type of assets that it affects. Therefore, the threats will be divide in three parts, affecting physical assets, affecting logical assets and affecting persons. For each one of this three parts, we will give the possible threats, describe them and give a level of impact, a level of likelihood and the resulting levels of risk.

2.3.1 Levels of impact, likelihood and risk

We define three different types of affection for our client's company:

- Availability: affecting the physical functioning of the system. For instance, if a server is shut-down, his availability is compromised.

- Confidentiality: affecting the sensitive information of the company by sharing them. For example, a server could be infected and could automatically sends some files to a hacker. It should be obvious that only servers located in the low security zone, in which there is an internet connection, could present such a risk.
- Integrity: affecting some sensitive information of the company by alteration. Similarly to the confidentiality level, a hacker could modify or delete some information in order to hide it or to prevent the company in succeeding their projects. This could be the case when a competitor would want to curb the company in order to be the first one on the market selling a same product on which both were working on.

We are also going to assess the risk by associating a level for the impact as well as for the likelihood for every threat.

We define as follow three levels of impact in terms of failure time (availability):

- Low: less than 10 minutes.
- Medium: between 10 minutes and 50 minutes.
- High: more than 50 minutes.

We also define the three levels of likelihood:

- Low: maximum 1 time per year.
- Medium: between 1 and 10 times per year.
- High: more than 10 times per year.

With the impact and the likelihood analysis, we can define the risk level. This is shown in Table 2.

| | Impact | | |
|------------|--------|--------|--------|
| Likelihood | Low | Medium | High |
| Low | Low | Low | Low |
| Medium | Low | Medium | Medium |
| High | Low | Medium | High |

Table 2: Risk level assessment.

2.3.2 Threats affecting physical assets

In this section, we will present the threats affecting only the physical assets of the company:

Threat 1 : Power outage

In the case of a power outage, obviously the data diode system will not work because of the need for an electrical power source, which means it will not be available until the power gets back. A power outage usually does not exceed one hour which mean there is not a high impact.

Weather is responsible for the majority of major power outages that occurs, but there are many others causes such as short circuits, blackouts and so on. Thus power outage has a medium likelihood to happen.

Source : Nature

Affecting level : Availability

Impact : Medium

Likelihood : Medium

Risk Level : Medium

Threat 2 : Fire

Because of a fire in a building in which the data diode is installed or because of too much heat gathered, the data diode system could be harmed, which is then leading to its non-operation.

The impact depends on the damages caused by the fire. The data diode can suffer significant or irreparable damages which could lead to the replacement of the hardware.

A fire can occur due to several causes, however the probability of having a fire is in general low.

Source : Nature

Affecting level : Availability

Impact : High

Likelihood : Low

Risk Level : Medium

Threat 3 : Data diode hardware failure

If a failure in the data diode's hardware occurs, such as in the NIC, it can lead to the non-operation of the data diode. In this case, it is the whole operation of the system which can be disturbed. However, the system administrator could easily replace the broken component. Despite the fact that the data diode hardware is well chosen and tested before in order to maintain the failure risk low, hardware failure can still happen. There is no perfect product to last forever in this world.

Source : Nature, Administrators, Employees, Unauthorized user

Affecting level : Availability

Impact : Medium

Likelihood : Low

Risk Level : Low

Threat 4 : Data diode hardware degradation

This threat is possible once an unauthorized person has a physical access to the data diode itself. This could lead to a simple destruction of the data diode or robbery of some element (availability), trying to copy the data from it (confidentiality), or trying to add/modify/delete an element to falsify the data (integrity). There is also a possibility that the hardware degradation is done unintentional (disconnecting a cable, spilling a drink on it). Thus, this threat could affect the three parts of the information security and also lead to non-reversible damage. However, the impact time is according to the broken hardware component.

A clumsiness is always possible (medium). Furthermore, if the access in the room of the data diode is not controlled, this attack is really simple and is likely to happen very often (high).

Source : Nature, Administrators, Employees, Unauthorized user

Affecting level : Availability, Confidentiality, Integrity

Impact : Medium

Likelihood : Medium

Risk Level : Medium

Threat 5 : DDOS attack

A DDOS is a cyberattack in which the hackers want to make a system unavailable to its users by temporarily or indefinitely disrupting the services of the host. The attack is accomplished by flooding the targeted resources with superfluous requests from many different sources from the internet, in an attempt to overload the systems and thus prevent the legitimate requests from being fulfilled. The administration of our data diode happens through a web interface which means that it is vulnerable to DDOS attack. In case of such attack the data diode web server will become unavailable as long as the attack lasts. Hence, the transmission system will be disrupted.

If the website of the data diode suffers from a DDOS attack, the secured network productivity can grid to a total halt if the transfer of important files cannot be done. This can lead to an important cost for the business, it is why a DDOS attack can have a big impact. Furthermore, if the company is popular,

the secured network will be a prime target for the hackers. Therefore, attempts may be numerous because DDOS attacks have grown in scale and have become very popular since their are easy to implement.

Source : Skilled Hacker

Affecting level : Availability

Impact : High

Likelihood : High

Risk Level : High

2.3.3 Threats affecting logical assets

In the same order of idea, lets focus now on the threats affecting the logical assets of the company.

Threat 6 : Zero Day Attack

Since there is always the probability to be attacked by a new and unknown form of cyberattack, this represents a threat due to the fact that the future can not be predicted. Therefore, such attack could affect one or more parts of the company, but it still remains theoretically and unknown until the beginning of such attack. Since we do not know the attack, its impact could be as low as high. This kind of attack is constantly sought after by different people like skilled hacker, but its difficult to find one, and more of this, to find one that can affect our system.

Source : Skilled Hacker

Affecting level : Availability, Confidentiality, Integrity

Impact : High

Likelihood : Medium

Risk Level : Medium

Threat 7 : SQL injection

An SQL injection threat could affect any website that makes use of an SQL-based database. In the case of an attack, it will allow the "attacker" to bypass a web application's authentication or view data contained in the database and alter it. Hence, data confidentiality and integrity are concerned. This represents a threat because our company detain such a database containing sensitive information.

The possible consequences of the SQL injection attacks such as consultation, modification or deletion of the database, correspond to a high risk because it will affect the log in page of the web interface of the data diode. The SQL injection is one of the oldest, most prevalent and most dangerous method to attack systems and steal information from web applications. It can be done on any website, so the likelihood is high.

Source : Skilled Hacker, script kiddies

Affecting level : Confidentiality, Integrity

Impact : High

Likelihood : High

Risk Level : High

Threat 8 : Brute force attack

A hacker could try as many passwords as he wants in order to find the correct password. This could be done using dictionaries attacks on a web log in page or another type of identity check-in systems of the company. In the case of the hacker find or guess a correct password, he would use it as long as he can and it works.

Similarly to the SQL injection, there are tools in order to crack passwords. Since it is easily done, this kind of attack has a high probability to occur.

Source : Skilled Hacker

Affecting level : Availability, Confidentiality

Impact : High
Likelihood : High
Risk Level : High

Threat 9 : Virus and malwares

An infected computer's user could without acknowledgement send a virus through the data diode or could simply spy (*Trojan*) on the user activity. Despite the fact that the communication from the isolated network is not possible, a ransom ware⁹ virus could lead to the destruction or the non availability of data from the labs.

Depending on the type of the virus, the impact is as well depending on the type of the virus: a Trojan virus would not halt the system however confidentiality will be broken.

This kind of attack is really diversified and used. However, this attack could only succeed if a user file is infected which means there are several attacks to do before. Thus, the likelihood remains medium.

Source : Skilled Hacker, Script kiddies, Administrators, Employees
Affecting level : Availability, Integrity

Impact : Medium
Likelihood : Medium
Risk Level : Medium

Threat 10 : Misconfiguration

A misconfiguration of the data diode, which is only possible from the administrator interface, could cause its non-function or malfunction. This threat has a direct impact on the availability and the integrity but could also represent a potential confidential threat.

In this case, a reconfiguration of the data diode will be required. This will not take much in terms of time and will not have a major impact thanks to the administration interface, which allows to reconfigure easily the data diode. Furthermore, a misconfiguration by the administrator occurs rarely on a year.

Source : Administrator
Affecting level : Availability, Integrity

Impact : Low
Likelihood : Low
Risk Level : Low

Threat 11 : Failure in maintenance from the provider

A threat can also be introduced by the provider during the installation of the data diode or by an application update or new release. This is generally caused by a lack of communication or documentation between the company.

In case of failure in maintenance or design the data diode can be non-functional until the problem or bug is fixed. This could lead to a halt of the system for an undetermined period of time. The likelihood of that to happen is extremely low on a year, because generally the product is well tested before being released to the client. Thus, in our case the likelihood is medium.

Source : Provider
Affecting level : Availability, Integrity

Impact : Medium
Likelihood : Low
Risk Level : Low

Threat 12 : Sniffing the network

If a hacker managed somehow to gain access in the company LAN, he could *sniff* every passing through traffic. This could represent a real threat if the communications/transfers within the LAN are not encrypted. In this case, the hacker could sniff the entire passing traffic of the network for months if

⁹This kind of virus could encrypt all the data on a drive and request some money in order to decrypt it.

no one detects him. But it is still very rare that somehow a hacker could get into the network without being discovered by the system administrator.

Source : Skilled hacker

Affecting level : Availability, integrity, confidentiality

Impact : High

Likelihood : Low

Risk Level : Low

2.3.4 Threats affecting persons

Similarly as for the previous sections, we explain the threats affecting persons.

Threat 13 : Social engineering

Social engineering is a practice of manipulating people so they give up confidential information or sensitive data such as their credentials. The most common forms of this kind are the ransomware viruses and phishing techniques.

This method allows a hacker to steal the credentials of a user and then to simply log in and snoop around for sensitive data. Hence, it results in a high risk. But administrators are aware of these techniques so only users are potential victims.

Source : Skilled Hackers, unauthorized users

Affecting level : Confidentiality

Impact : High

Likelihood : Medium

Risk Level : Medium

Threat 14 : Data credentials lost

There is a possibility of a user to lose his credentials which means that he will no longer be able to connect to the data diode. In this case, a user should immediately contact the administrator in order to reset his credentials.

An administrator knows the importance of his role and will take care of the data credentials. In addition, every user of the company are using his credential every day so it very rare and unlikely that an employee could forget his in 24 hours.

Source : Administrator, Employees

Affecting level : Availability

Impact : Medium

Likelihood : Low

Risk Level : Low

Threat 15 : Data credentials theft

Data credentials theft can occur in several ways such as hackers attacks (brute force, social engineering,...) or because of the negligence of a user (easy password, credential stored in a non-secured place such as the office, and so on...) or because of a malicious administrator which has the right to modify the company database (password table)¹⁰

If it is the administrator credentials that are stolen, the attacker can change the data diode administration and it implies a high impact. On the other hand, if it is the user credentials that are stolen, they can use it and transfer what they want and access the data of the users. In both case, the attacker can do what he likes and could prevent the access for legitimate persons such as the administrator.

Source : Skilled Hacker, unauthorized user, Employee, Administrator

Affecting level : Confidentiality

¹⁰This is generally in case of any employee lose his credential, the administrator can reset it or change it manually.

Impact : High
Likelihood : High
Risk Level : High

2.3.5 Summary table

| ID | Threat | Impact | Likelihood | Risk Level |
|----|--|--------|------------|------------|
| 1 | Power outage | Medium | Medium | Medium |
| 2 | Fire | High | Low | Low |
| 3 | Data diode hardware failure | Medium | Low | Low |
| 4 | Data diode hardware degradation | Medium | Medium | Medium |
| 5 | DDOS attack | High | High | High |
| 6 | Zero Day attack | High | Medium | Medium |
| 7 | SQL injection | High | High | High |
| 8 | Brute force attack | High | High | High |
| 9 | Virus and malwares | Medium | Medium | Medium |
| 10 | Misconfiguration | Low | Low | Low |
| 11 | Failure in maintenance from the provider | Medium | Low | Low |
| 12 | Sniffing | High | Low | Low |
| 13 | Social engineering | High | Medium | Medium |
| 14 | Data credentials lost | Medium | Low | Low |
| 15 | Data credentials theft | High | High | High |

Table 3: Summarizing table.

2.4 Countermeasures

In this section we will explain which and how countermeasures could be taken in order to address every threat of the system. We will use the Table 2 in order to adapt our countermeasures accordingly to the risk level of each threat.

Before starting, we should mention that most of the threats nowadays are coming from the internet. Thus, our data diode should not be exposed to such a danger. Despite the fact that the data diode could be installed within a LAN which has an internet connection, it should not be possible to access it from the outside but only from the LAN. In this way, it will be much difficult to a hacker to directly threaten our data diode. In order to succeed his attempts he should therefor, try infecting a computer within the LAN and only then, by redirecting all his traffic through his new bot, try to hack our data diode.

| ID | Threat | Countermeasure(s) |
|----|---------------------------------|---|
| 1 | Power outage | For this threat we accept the possible risks. However the company could prevent this by installing UPS battery backup, thus it is out of our scope. |
| 2 | Fire | The data diode should be placed in a room protected against fire, closed with fire doors to mitigate as much as possible the risk of the data diode being affected by fire or heat. This is out of our scope |
| 3 | Data diode hardware failure | Since an administrator must be ready to intervene in case of any hardware failure, we can accept the risk of this threat. In addition, administrators should use administration tools such as <i>SNMP protocol</i> in order to face the issue as quickly as possible. |
| 4 | Data diode hardware degradation | The data diode should be placed in a closed room locked with a key or locked using access card possessed only by the administrators or authorized employees. A camera could also be installed in order to monitor activity into the room. Since there are only few persons who have access in the room, the risk is limited to a clumsiness of the administrator. Again, this is also out of our scope. |

| | | |
|----|--|--|
| 5 | DDOS attack | This could be faced by limiting the number of connection to the data diode. It will then be impossible to overload the system and thus to halt it. However, the data diode servers can only be accessed from the LAN. Thus, in order to create a DDOS on the data diode server, all the company's computers should be infected. |
| 6 | Zero Day attack | Due to the fact that we can not be prepared against this kind of attack, we accept the risks of this threat. |
| 7 | SQL injection | In order to avoid the SQL injection, we must use in the code source of the web interface the especially developed functions and methods which prevents the execution of the SQL language. |
| 8 | Brute force attack | In order to stop dictionary password attack, we could implement a number of password trial times before blocking the account. In this way, after 3 wrong password, the account have to be manually reset by an administrator. |
| 9 | Virus and malwares | This threat is out of our scope. The client is responsible for securing access to internal network and so he should use appropriate anti-virus and other anti-malware systems. |
| 10 | Misconfiguration | The configuration is only possible through the administrator interface and by an administrator. Hence, an administrator must be well chosen. However, the company could create for example a modification policy in which a system alteration should be approved by at least two administrator in order to take place. This is out of our scope. |
| 11 | Failure in maintenance from the provider | We test all the features of the data diode (such as the transfer) before providing it to the client. We make sure we always have a well operating version before deploying it to our customers. |
| 12 | Sniffing | There should be log of every path of the data trough the network. Thus, if a person is sniffing the traffic, an administrator can rapidly identify the redirection of the whole traffic. But also the traffic and the communication should be encrypted and thus the sniffer would not be able to read especially confidential information. Using HTTPS protocol |
| 13 | Social engineering | Since it concerns the employees, the company should provide security awareness training in order to avoid social engineering. This is out of our scope. |
| 14 | Data credentials lost | Having more than one administrator is recommended but it is not an imperative countermeasure |
| 15 | Data credentials theft | In order to mitigate the risk of credential theft, employee should not save them into their browser or write them into a secure file and should change it several times. This is out of our scope. |

Table 4: Countermeasure

2.5 Residual risk

In this section we are going to add a new variable, the residual risk. Lets have a look at the following definition :*The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied*¹¹.

$$\text{residual risk} = \text{risk assessed} - \text{countermeasures}$$

The next Table 5 summarize the previous section very well and for each threat, we add the residual risk remained after the implementation of the countermeasures . For this and in the same order of idea, we defined three levels: high, medium and low.

| ID | Threat | Countermeasure | Risk level | Residual risk |
|----|-----------------------------|----------------|------------|---------------|
| 1 | Power outage | Accept | Medium | Medium |
| 2 | Fire | Accept | Low | Low |
| 3 | Data diode hardware failure | Mitigate | Low | Low |

¹¹Definition from Wikipedia.

| | | | | |
|----|--|----------|--------|--------|
| 4 | Data diode hardware degradation | Mitigate | Medium | Low |
| 5 | DDOS attack | Transfer | High | High |
| 6 | Zero Day attack | Accept | Medium | Medium |
| 7 | SQL injection | Avoid | High | Low |
| 8 | Brute force attack | Avoid | High | Low |
| 9 | Virus and malwares | Transfer | Medium | Medium |
| 10 | Misconfiguration | Transfer | Medium | Medium |
| 11 | Failure in maintenance from the provider | Accept | Medium | Low |
| 12 | Sniffing | Accept | Low | Low |
| 13 | Social engineering | Transfer | Medium | Medium |
| 14 | Data credentials lost | Transfer | Low | Low |
| 15 | Data credentials theft | Transfer | High | High |

Table 5: Summary of countermeasures, risk level and residual risk.

3 Implementation

3.1 Simulation of the data diode

In this section, we will explain our implementation from scratch but also our network infrastructure. Because of costs reasons, we had to use virtual machines and virtual networks.

3.1.1 Machine installations

We firstly installed two virtual machines. As we said earlier the operating used is Ubuntu 16.04 LTS¹².

Once the OS installation was done, we created for each machine two virtual interfaces. Lets define the virtual network or internal network as the network between the two data diode machines (transmitter and receiver) and the outside network or external network as the network between a data diode server and computer's labs. Here is the schema of the virtual network used for the data diode.

Figure 11: Virtual network architecture.

As shown in Figure 11, within the data diode we used a virtual router to make the connection between the transmitter and receiver. We have set up the connection by specifying for each entity a static Ipv4 address.

- The transmitter Ipv4 virtual network address is : 10.37.129.5
- The receiver Ipv4 virtual network address is : 10.37.129.6

Once tested and approved, we continued by adding another router to simulate both external side of the data diode. This is illustrated in Figure 11 and is what we call the outside network. We have done this to be able to communicate with the transmitter but also with the receiver and without needing to change cable connection each time. Again we configured the outside network interface manually :

- The transmitter Ipv4 external network address is : 10.37.129.5
- The receiver Ipv4 external network address is : 10.37.129.6

3.1.2 simulation un seul sens

3.2 deployement de bftp

3.3 interface Web data diode

subsubsectionDjango pourquoi lié avec quelques contre mesure

¹²Long Time support.

3.3.1 interface de configuration

lien softlink de interface

3.3.2 ajout de vftp dans l'interface

3.4 control recommendation

4 Test and demo scenario

1 - Linux 2 - firewall iptables receiver 3 - deployment de bftp. joue avec pour comprendre comment ça fonctionne

4 - interface web 1 quoi et comment? Après des recherches on utilise Django 1 parce c'est python même que bftp, deuxième c'est un framework et simple à utiliser et qui implémente déjà certaines contre-mesures comme SQL, SRF XSS.... On fait les templates html et css 5 - interface config web - on crée comment modifier le ip serveur, avec un lien soft link interface ensuite on a créé système de alume bftp éteint bftp et ce avec des paramètres 6 - on a créé le code user normal et on a ajouté bftp dans l'implémentation

7 - on peut dire que control recommendation - ça serait bien que l'entreprise mette un anti DDOS, mais aussi que on peut pour ddos lancer en docker et docker monitoring

sifflant - j'https à configuration - si jamais une mauvaise config l'admin devrait pouvoir retourner en arrière - W utilisation d'un git un zip une fois que c'est bon config et après suffit de redéployer - système restore

failure in maintenance après une mise à jour, on peut par exemple essayer la data diode, un test temporaire, lancer en parallèle et dire au employé d'essayer de l'utiliser et une fois que c'est valide passer en master Virus malware - l'entreprise peut premièrement installer un firewall un système mais aussi elle pourrait dans la data diode installer un système de permission de fichier envoyé, pas d'exécutable seulement des fichiers normaux

entreprise politique de sécurité mot de passe par exemple admin change les mots de passe tous les x temps, surtout les mots de passe machines de data diode Chaque utilisateur doit changer son mot de passe tous les 3 mois ! ou tous les 6 mois par exemple

References

- [1] DEEP SECURE, *How Does a Data Diode Work?* Discussion Paper, February 2017.
- [2] SANS Institute InfoSec Reading Room, *Tactical Data Diodes in Industrial Automation and Control Systems*, January 2015.
- [3] CS Risk Management and Compliance Ltd, *Data Diode vs Firewall Feasibility*, September 2016. [Online]. Available: <https://csriskmanagement.co.uk/data-diode-vs-firewall-feasibility/> [Accessed: 30- Oct- 2017]
- [4] BlindFTP, *Blind ftp protocol*[Online]. Available: <https://www.decalage.info/fr/python/blindftp> [Accessed: 30- Oct- 2017]
- [5] David Basin AND Patrick Schaller AND Michael Schlapfer, *Applied Information Security, A hands-on Approach*, Springer.