**Basic Network Pump with Data Diodes**

Security Target

Common Criteria - BANPUMP

Author: Eugenia Ana CAPOTA

**Table of Contents**

[**1.** **Security Target Introduction (ASE\_INT.1)** 3](#_Toc167373193)

[**1.1** **Security Target Reference** 3](#_Toc167373194)

[**1.2** **TOE Reference** 3](#_Toc167373195)

[**1.3** **TOE Overview** 4](#_Toc167373196)

[**1.4** **TOE Description** 6](#_Toc167373197)

[**1.4.1** **Physical Scope** 6](#_Toc167373198)

[**1.4.2** **Logical Scope** 8](#_Toc167373199)

[**1.5** **Document Overview** 10](#_Toc167373200)

[**2.** **Conformance Claim (ASE\_CCL.1)** 10](#_Toc167373201)

[**2.1** **CC Conformance Claim** 10](#_Toc167373202)

[**2.2** **Protection Profile Claim, Package Claim** 10](#_Toc167373203)

[**2.3** **Conformance Rationale** 10](#_Toc167373204)

[**3.** **Security problem definition (ASE\_SPD.1)** 11](#_Toc167373205)

[**3.1.** **Threats** 11](#_Toc167373206)

[**3.2.** **Assumptions** 11](#_Toc167373207)

[**4.** **Security Objectives (ASE\_OBJ.2)** 12](#_Toc167373208)

[**4.1** **Security objectives for the Target of Evaluation** 12](#_Toc167373209)

[**4.2** **Security objectives for the Operational Environment** 12](#_Toc167373210)

[**5.** **Security Requirements (ASE\_OBJ.2)** 13](#_Toc167373211)

[**5.1** **Security Assurance Requirements (SARs)** 13](#_Toc167373212)

[**5.2** **Extended Component Definition (ASE\_ECD.1)** 14](#_Toc167373213)

[**6.** **TOE Summary Specification (ASE\_TSS.1 / ASE\_TSS.2)** 14](#_Toc167373214)

[**APPENDIX** 14](#_Toc167373215)

[**A.** **Security Objective Rationale** 14](#_Toc167373216)

[**References** 21](#_Toc167373217)

**List of Figures**

[Figure 1. Data diode using mediaconverters with separate transmit (xmt) and receive (rcv) ports [2]. 4](#_Toc167373218)

[Figure 2. Essential part of a Data Diode [2]. 4](#_Toc167373219)

[Figure 3. Original US Navy Lab Network Pump model [5]. 5](#_Toc167373220)

[Figure 4. Original Network Pump Block Structure [6]. 6](#_Toc167373221)

[Figure 5. Proposed architecture of the TOE with strict Bell and LaPadula security properties always holding. 7](#_Toc167373222)

[Figure 6. Proposed architecture of the TOE when High needs to communicate with Low with strict Bell and LaPadula security properties always holding. 8](#_Toc167373223)

[Figure 7. Algorithm for the TOE functioning to send files from Network Level A (bottom) toward Network Level B (top) via Bunker Jails FTP Servers. 9](#_Toc167373224)

**List of Tables**

[Table 1. Threats to the TOE. 11](#_Toc167373225)

[Table 2. Assumptions. 11](#_Toc167373226)

[Table 3. Security Objectives of the TOE. 12](#_Toc167373227)

[Table 4. Security Objectives of the TOE Environment. 12](#_Toc167373228)

[Table 5. Assurance Requirements. 13](#_Toc167373229)

[Table 6. Mapping Threats/Assumptions to Objectives. 15](#_Toc167373230)

[Table 7. Threats/Objectives Rationale. 15](#_Toc167373231)

[Table 8. Assumptions/Objectives Rationale. 18](#_Toc167373232)

# **Security Target Introduction (ASE\_INT.1)**

## **Security Target Reference**

|  |  |
| --- | --- |
| **ST Title** | Basic Network Pump with Data Diodes Security Target |
| **ST Version** |  |
| **ST Status** | Final |
| **ST Classification** | Public |
| **Author** |  |
| **Evaluation Assurance Level** |  |
| **Publication Data** |  |
| **Number of pages** |  |
| **Common Criteria Version** |  |

## **TOE Reference**

|  |  |
| --- | --- |
| **Developer Name** |  |
| **TOE Name** | Basic Network Pump with Data Diodes |
| **TOE Version Number** |  |

## **TOE Overview**

The Target of Evaluation (TOE) is the Basic Network Pump with Data Diodes (BANPUMP) and will hereafter be referred to as the TOE throughout this document. The TOE is a new network pump architecture which guarantees the Bell-LaPadula [[1](#_ENREF_1)] confidentiality properties between the connected networks, even when software components of the pump are under total adversary control.

A data diode is a cybersecurity solution that makes sure that information can only travel in one direction. Data diodes guarantee one-way data flow based on the laws of physics. The most frequent implementation of a data diode is based on fiber optics, where the transmission (TX) and receive (RX) device ports are connected such that information can only go one-way around, from LOW network towards HIGH network, as shown in Figure 1, taken from [[2](#_ENREF_2)].

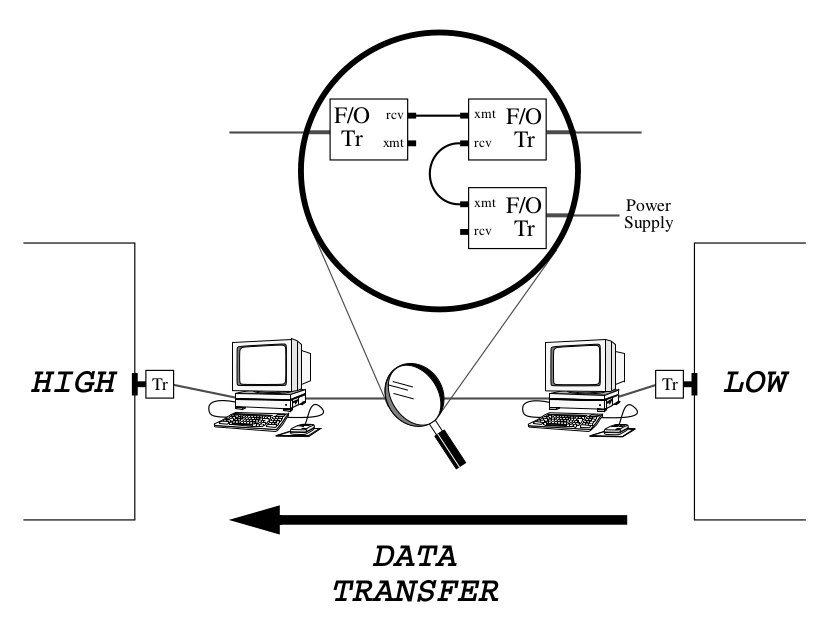


Figure 1. Data diode using mediaconverters with separate transmit (xmt) and receive (rcv) ports [[2](#_ENREF_2)].

The essential part of the data diode is shown in Figure 2 [[2](#_ENREF_2)] where the electrical symbol of a diode is used to indicate the unidirectional data flow of information. The missing optical cable from the transmit port (Xmt) on the left to the receive port (Rcv) on the right makes sure that there is no communication from right to left.

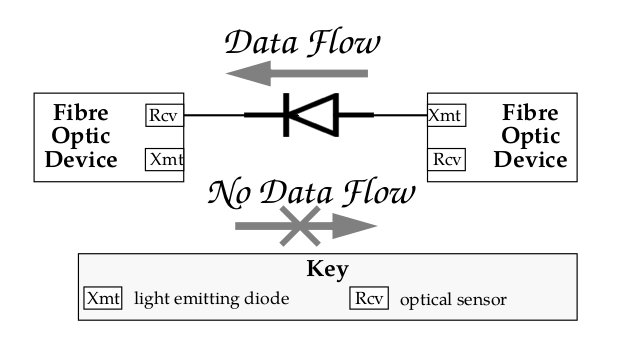


Figure 2. Essential part of a Data Diode [[2](#_ENREF_2)].

The Network Pump is another cybersecurity solution providing network domain separation through a failsafe and redundant security architecture. It performs high assurance validation, inspection, sanitization, and/or transliteration, as required, per data flow between networks of different classification levels [[3](#_ENREF_3)]. The Naval Research Laboratory (NRL) Network Pump, or Pump, is a standard for mitigating covert channels that arise in a multilevel secure (MLS) system when a high user (HU) sends acknowledgements to a low user (LU). The issue here is that HU can encode information in the timings of the acknowledgements [[4](#_ENREF_4)].

Critical infrastructure security standards recommend using these two network appliance types, namely the data diode and the network pump along with unidirectional routers(ie. based on electromagnetic induction for the physical one-way separation of networks in Siemens Data Capture Units) [[3](#_ENREF_3)].

The problem with current implementation of data diodes is that there is no feedback going back from the high network towards the low network in order to acknowledge the incoming information flow. That goes along with very expensive prices required for product certification. Network pumps solve this problem with a secure feedback loop; however, the pumps are scarcely used in securing critical infrastructures.

The Network Pump has a major design flawmaking it susceptible to violations of the Bell LaPadula [[1](#_ENREF_1)] security requirements. To be more specific, the original Network Pump allows the device to keep functioning regardless of how many times a file or message has failed the delivery. An unlimited number of retries are permitted for the same file or message, allowing for attackers on both networks to communicate through coded number of failures used to deliver the same message. Only time is mitigated as a side channel for sending signals backwards through the Pump [[4](#_ENREF_4)], reversing the direction of the data flow. This is done only in terms of „good enough” stochastic acknowledgments for the received messages. Figure 3 shows the original version of the Network Pump:

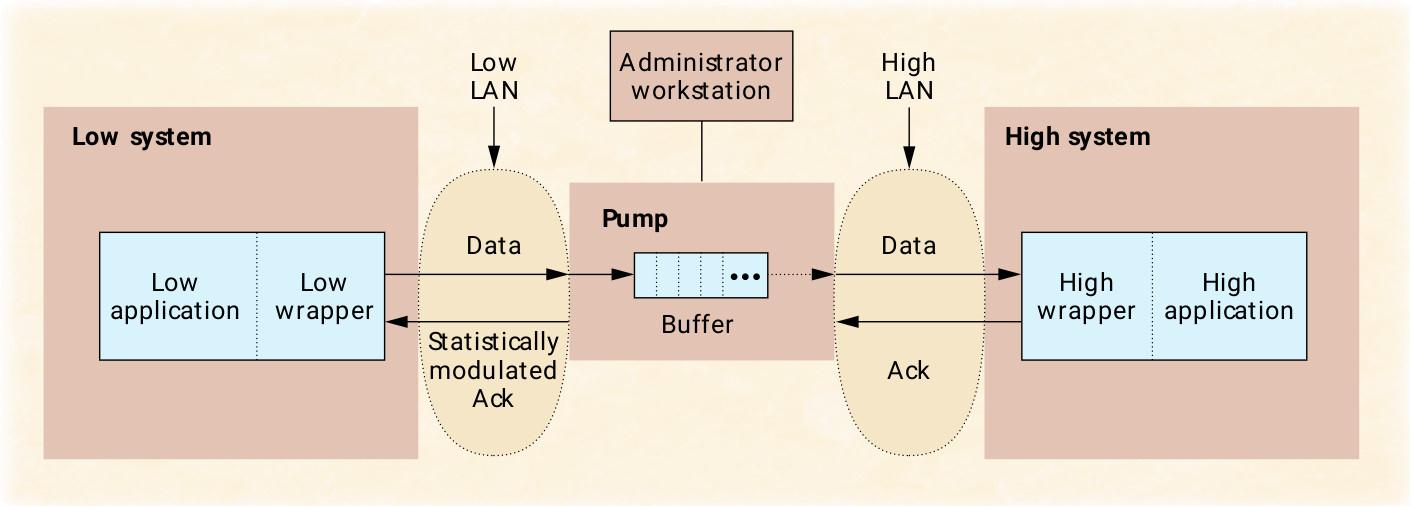


Figure 3. Original US Navy Lab Network Pump model [[5](#_ENREF_5)].

This network appliance uses two microprocessors as shown in Figure 4:

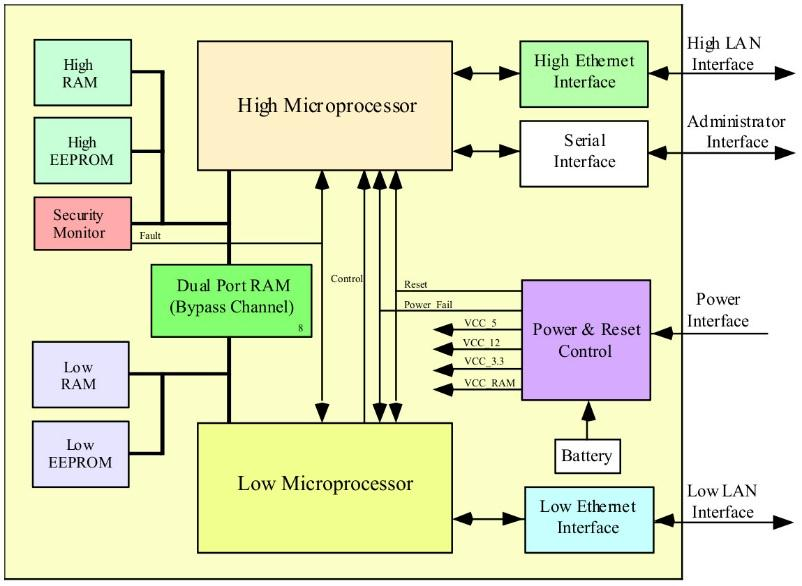


Figure 4. Original Network Pump Block Structure [[6](#_ENREF_6)].

Both High and Low microprocessors shown in Figure 4 run real Linux-based operating systems according to [[7](#_ENREF_7)]. It is critical to note that the threat model of the original Pump does not take into account the fact that any kind of operating system connected to a network can be hacked, hijacked and backdoored in order to circumvent the security of the device. The “basic Pump” serves only one sender and one receiver. The “network Pump” services many senders and receivers from different applications (e.g., file transfer, e-mail) simultaneously, increasing the likelihood of the High operating system and the Low operating system getting hacked.

## **TOE Description**

### **Physical Scope**

The TOE is a pump made of commercial off-the-shelf hardware data diodes, with the  
ability to accept simultaneous traffic from multiple users without the design flaws of the original Pump.

Figure 5 shows the design of the TOE when Low needs to communicate messages (files) with High with unhackable acknowledgements and without covert channels:

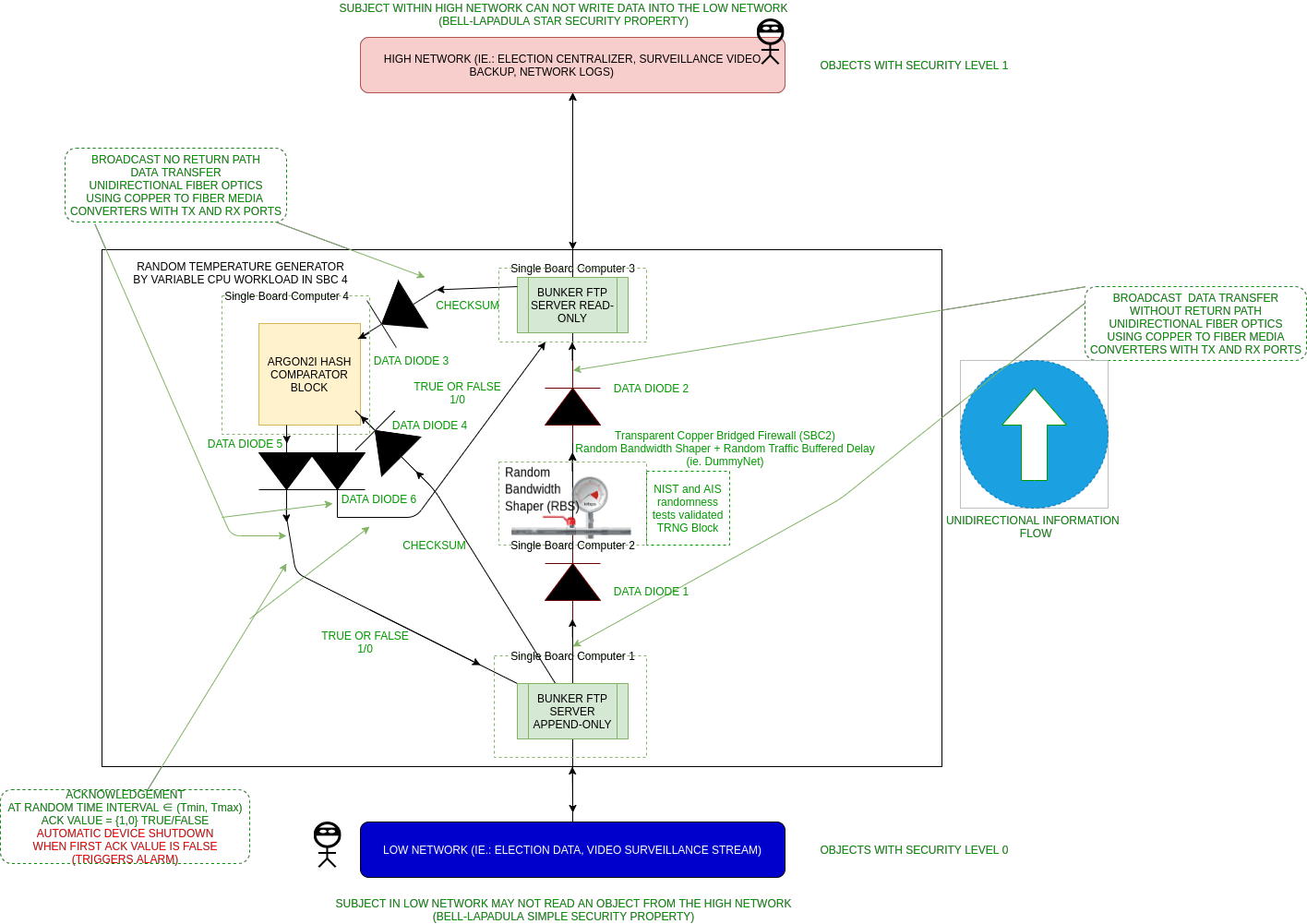


Figure 5. Proposed architecture of the TOE with strict Bell and LaPadula security properties always holding.

The reversed scenario for the TOE architecture is when High needs to communicate with Low using the same device, in Figure 6:

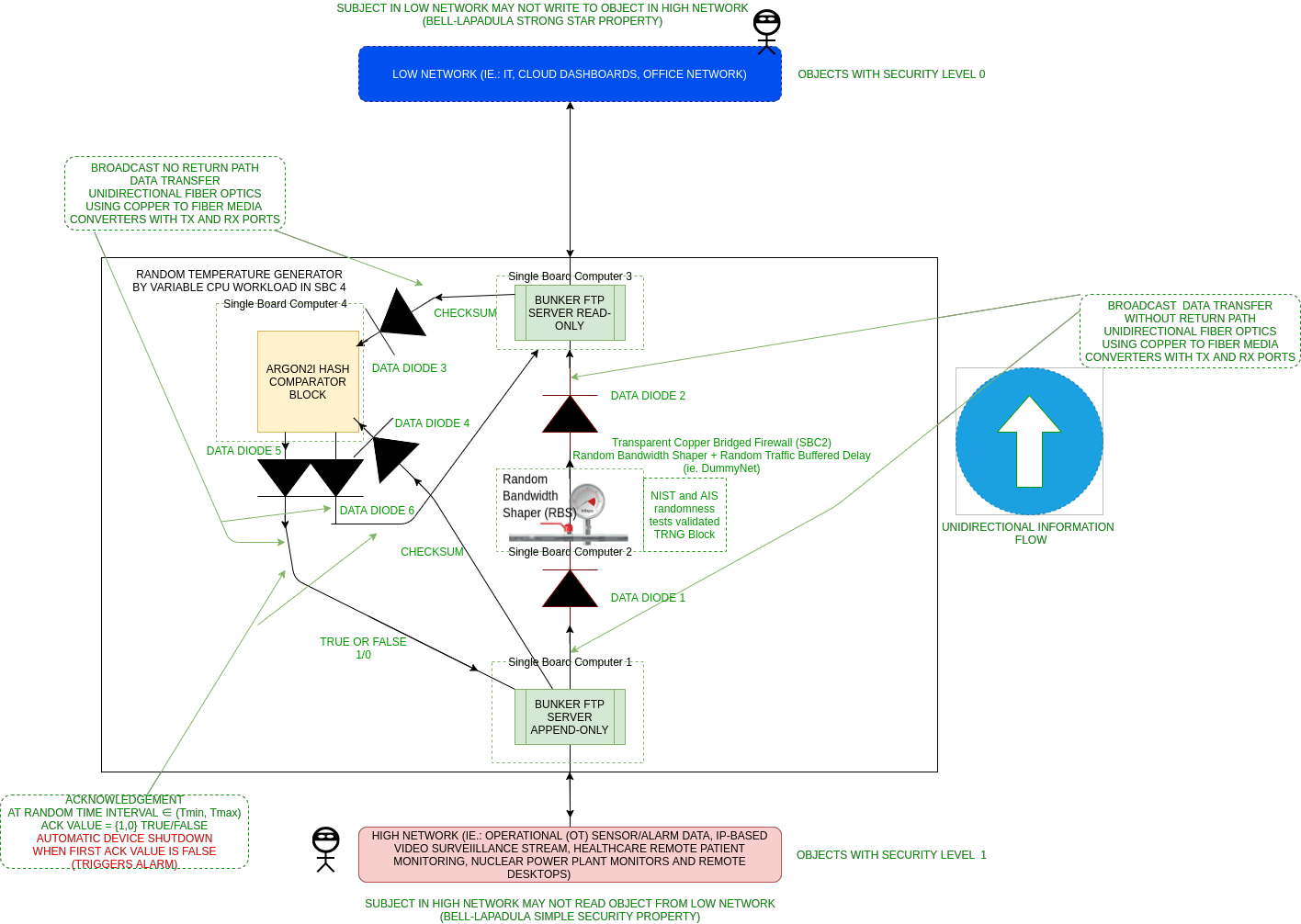


Figure 6. Proposed architecture of the TOE when High needs to communicate with Low with strict Bell and LaPadula security properties always holding.

The TOE design uses HardenedBSD Jail Bunkers which we developed earlier for running daemon services on the 4 Single Board Computers (SBC) [[8](#_ENREF_8)], similar to the two FTP servers for file transfer.

All our Single Board Computers are isolated from each other using 6 hardware commodity off-the-shelf data diodes. The data diodes are made from ordinary copper-to-fiber-optics mediaconverters as described in [[2](#_ENREF_2)], so a total of 18 mediaconverters are required.

### **Logical Scope**

Our threat model acknowledges that operating systems can be hacked and hijacked. The TOE design is engineered to be resilient when both SBC1 and SBC3 are hacked being under complete adversary control.

SBC4 is used as an isolated checksum checker that keeps sending a fountain code pattern for “TRUE/1” at random, delayed time intervals immediately shutting down the system when the first message failure is encountered. This is necessary in order to mitigate for attackers on both sides communicating via acknowledgements. Short-distance fiber optics is highly reliable and fountain codes are only used as a care taken in advance in order to mitigate for software issues on the receiver side, like full kernel buffers and CPU load. We plan on using fountain codes for all traffic that goes through data diodes. Argon2i is used as a modern checksum algorithm because it deals with side channel attacks and is designed to be resilient to botnets and ASIC crackers, also being public domain [[9](#_ENREF_9)].

SBC2 is a transparent isolated OSI Layer2 (ethernet) bridge using DummyNet [[10](#_ENREF_10)] for creating random bandwidth shaping and random buffered traffic delay. This is used to mitigate for the time channel being used as a covert side channel in order to send messages back from SBC3 to SBC1.

Figure 7 shows the flowchart of the algorithm governing the TOE model:

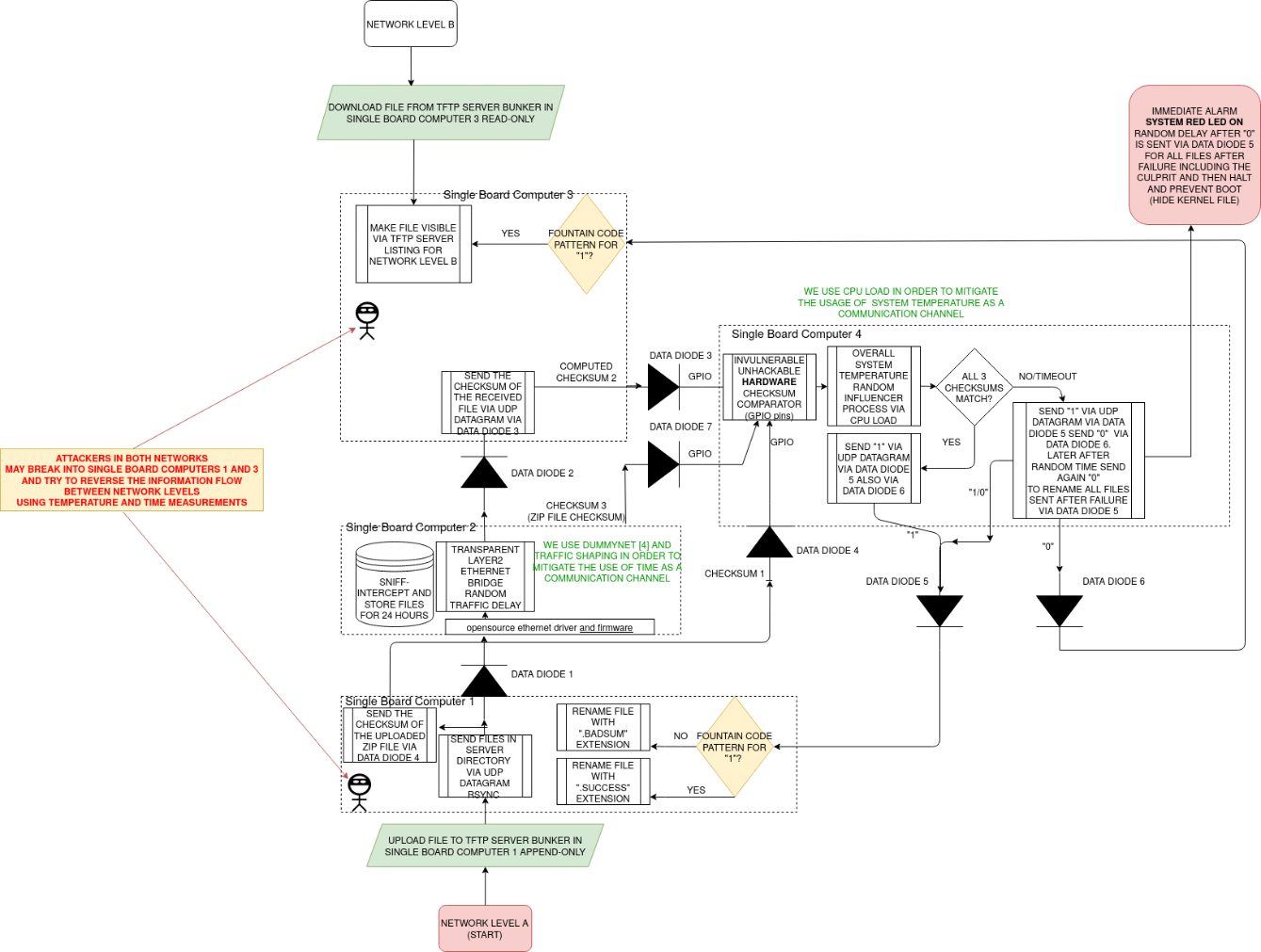


Figure 7. Algorithm for the TOE functioning to send files from Network Level A (bottom) toward Network Level  
B (top) via Bunker Jails FTP Servers.

The TOE model is TRL2 and we plan on constructing a fully working device at TRL3. Our design strictly imposes the Bell-LaPadula confidentiality and, implicitly, the BIBA integrity properties, mitigating for all possible covert channels even when an adversary takes full control over SBC1 and SBC3 (Figure 7).

The Bell-LaPadula confidentiality model:

* **The Simple Security property:** A subject in the Low network may not read an object from the High network (no read-up, Figure 5 and Figure 6).
* **The Star security property:** A subject in the High network may not write to object in the Low network (no write-down, Figure 5).
* **The Strong Star property:** A subject in Low network may not write to object in the High network (no write-up, Figure 6).

The BIBA integrity model:

* **BIBA Simple integrity property:** Subject in the High network may not read an object from the Low network (Figure 5 and Figure 6).
* **BIBA Star integrity property:** Subject in the Low network may not write to object in the High network (Figure 5).

## **Document Overview**

The ST has been developed in accordance with the requirements of the Common Criteria (CC) Part 3, Class ASE: Security Target Evaluation and ANNEX A: Specification of Security Targets, of the CC Part 1. The ST contains the following sections:

|  |  |
| --- | --- |
| **Section 1** | ST introduction, contains an overview and description of the TOE. |
| **Section 2** | Conformance claims, describes how the ST conforms to the CC. |
| **Section 3** | Security problem definition, defines the security problem that is to be addressed. |
| **Section 4** | Security objectives, provide the intended solution to the problem. |
| **Section 5** | Security requirements, contains the Security Assurance Requirements (SARs). |
| **Section 6** | TOE summary specification, describes how the TOE satisfies all the SARs. |

# **Conformance Claim (ASE\_CCL.1)**

## **CC Conformance Claim**

This Security Target complies with the following:

|  |  |  |
| --- | --- | --- |
| CC | | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5:   * Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Revision 1, November 2022. * Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Revision 1, November 2022. * Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Revision 1, November 2022. |
| Conformance claim | Part 2 Security functional components | Conformant |
| Part 3 Security assurance components | Conformant |

## **Protection Profile Claim, Package Claim**

This Security Target claims conformance to assurance package EAL7 augmented by ASE\_TSS.2 and ALC\_FLR.3.

## **Conformance Rationale**

None

# **Security problem definition (ASE\_SPD.1)**

## **Threats**

The security problems addressed by the TOE and the TOE environment are identified and detailed in the following table:

Table 1. Threats to the TOE.

|  |  |
| --- | --- |
| **Threat name** | **Threat definition** |
| T.UnauthorizedSBCAccess | An unauthorized party may attempt to access the equipment within a Single Board Computer. |
| T.CompromisedTemperature | An unauthorized party may attempt to reverse the information flow between network levels by using temperature measurements. |
| T.CompromisedTime | An unauthorized party may attempt to reverse the information flow between network levels by using time measurements. |
| T.CompromisedPowerConsumption | An unauthorized party may attempt to reverse the information flow between network levels by using power consumption measurements. |
| T.CompromisedAcoustics | An unauthorized party may attempt to reverse the information flow between network levels by using acoustics (using a hard disk as a microphone). |
| T.CompromisedNetworkIntegrity | An unauthorized party may attempt to overwrite files from Network Level A (Low) to Network Level B (High). |

## **Assumptions**

This section describes the assumption made in the process of identifying the threats and security requirements. The assumptions made for the TOE are defined in the following table:

Table 2. Assumptions.

|  |  |
| --- | --- |
| **Assumption name** | **Assumption definition** |
| A.Physical | The intended operation environment must store and operate the TOE in accordance with the highest of each of the requirements below. The internal and external connections of the TOE are implemented correctly. No unauthorized party has direct physical access to the TOE or any of the TOE components. |
| A.PhysicalSideChannel | Two unauthorized parties cannot communicate in any other way (e.g. through light signals), unless they attempt to reverse the direction of communication inside the TOE. |
| A.Power | The TOE shall be powered such that an unauthorized party or process on the transmitter and/or receiver side cannot evaluate the power fluctuation and consumption. This prevents an unauthorized party from using the power input as a covert channel. |
| A.NetworkFlow | The only method of interconnecting Network Level A and Network Level B is by using the TOE, where all of the units are operating in the same data flow direction. This prevents an unauthorized party from circumventing the security provided by the TOE through an untrustworthy product or by reversing the data flow direction of the TOE. |
| A.NetworkIntegrity | Files cannot be overwritten from Network Level A (Low) to Network Level B (High). |

# **Security Objectives (ASE\_OBJ.2)**

## **Security objectives for the Target of Evaluation**

This section identifies and describes the security objectives of the TOE.

Table 3. Security Objectives of the TOE.

|  |  |
| --- | --- |
| **Objective name** | **Objective definition** |
| O.Confidentiality | The information on Network Level A is kept confidential from Network Level B. |
| O.Integrity | The information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party. |

## **Security objectives for the Operational Environment**

The security objectives for the TOE Environment are defined in the following table.

Table 4. Security Objectives of the TOE Environment.

|  |  |
| --- | --- |
| **Objective name** | **Objective definition** |
| OE.Physical | The intended operational environment shall be capable of storing and operating the TOE. The TOE components are only accessible to authorized parties. |
| OE.Power | The intended operational environment shall provide power to the TOE such that the TOE power cannot be evaluated or interfered with through Network Level A and/or Network Level B. |
| OE.NetworkFlow | All the TOE components shall operate in the same data flow direction, from Network Level A to Network Level B. |
| OE.NetworkIntegrity | The TOE Network shall respect the BIBA Integrity Model. |

# **Security Requirements (ASE\_OBJ.2)**

## **Security Assurance Requirements (SARs)**

The security assurance requirements for the TOE are the Evaluation Assurance Level 7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE\_TSS.2 – TOE summary specification with architectural design summary and ALC\_FLR.3 – Systematic flaw remediation. For a detailed description of these components, please refer to the Part 3 of the Common Criteria directly. These requirements are listed in the following table:

Table 5. Assurance Requirements.

|  |  |
| --- | --- |
| **Assurance Class** | **Assurance Component** |
| ADV: Development | ADV\_ARC.1 – Security architecture description |
| ADV\_FSP.6 – Complete semi-formal functional specification with additional formal specification |
| ADV\_IMP.2 – Complete mapping of the implementation representation of the TSF |
| ADV\_INT.3 – Minimally complex internals |
| ADV\_SPM.1 – Formal TOE security policy model |
| ADV\_TDS.6 – Complete semiformal modular design with formal high level design presentation |
| AGD: Guidance documents | AGD\_OPE.1 – Operational user guidance |
| AGD\_PRE.1 – Preparative procedures |
| ALC: Life-cycle support | ALC\_CMC.5 – Advanced support |
| ALC\_CMS.5 – Development tools CM coverage |
| ALC\_DEL.1 – Delivery procedures |
| ALC\_DVS.2 – Sufficiency of Security Measures |
| ALC\_FLR.3 – Systematic flaw remediation |
| ALC\_LCD.2 – Measurable life-cycle model |
| ALC\_TAT.3 – Compliance with implementation standards – all parts |
| ASE: Security Target evaluation | ASE\_CCL.1 – Conformance claims |
| ASE\_ECD.1 – Extended components definition |
| ASE\_INT.1 – ST introduction |
| ASE\_OBJ.2 – Security objectives |
| ASE\_REQ.2 – Derived security requirements |
| ASE\_SPD.1 – Security problem definition |
| ASE\_TSS.2 – TOE summary specification with architectural design summary |
| ATE: Tests | ATE\_COV.3 – Rigorous analysis of coverage |
| ATE\_DPT.4 – Testing: implementation representation |
| ATE\_FUN.2 – Ordered functional testing |
| ATE\_IND.3 – Independent testing - complete |
| AVA: Vulnerability assessment | AVA\_VAN.5 – Advanced methodical vulnerability analysis |

## **Extended Component Definition (ASE\_ECD.1)**

All security requirements in this ST are based on components from CC Part 2 and CC Part 3,  
therefore there are no Extended Component Definitions.

# **TOE Summary Specification (ASE\_TSS.1 / ASE\_TSS.2)**

The TOE protects itself against interference and logical tampering by:

* Ensuring that all TOE components operate in the same data flow direction, from Network Level A to Network Level B.
* Having only two interfaces that are accessible to unauthorized parties, which allows for very limited interactions:
  + The transmitter interface: the TOE sends data through here without interpreting the data.
  + The receiver interface: the TOE does not permit any tampering of the transmitted data.
* Ensuring that the information on Network Level A is kept confidential from Network Level B.
* Following the BIBA Integrity Model, which prevents data modification by unauthorized parties, and unauthorized data modification by authorized parties.

The TOE protects itself against bypass by:

* Not allowing any unauthorized party direct physical access to the TOE or any of the TOE components.
* Being the only connection between Network Level A and Network Level B, (thus preventing bypass around the TOE through other communication channels, such as temperature and time measurements, power consumption monitorization, acoustics, light signals, etc.).

# **APPENDIX**

# **Security Objective Rationale**

This section presents the rationale behind the security objectives addressing the threats and assumptions associated with the TOE.

Table 6 demonstrates how all threats and assumptions are covered by at least one of the security objectives of the TOE, and that each security objective covers at least one threat or assumption.

Table 7 demonstrates how the objectives of the TOE and the TOE environment counter the threats  
identified in section 3.1.

Table 8 demonstrates how the objectives of the TOE and the TOE environment address the assumptions  
identified in section 3.2.

Table 6. Mapping Threats/Assumptions to Objectives.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Threats and Assumptions** | T.UnauthorizedSBCAccess | T.CompromisedTemperature | T.CompromisedTime | T.CompromisedPowerConsumption | T.CompromisedAcoustics | T.CompromisedNetworkIntegrity | A.Physical | A.PhysicalSideChannel | A.Power | A.NetworkFlow | A.NetworkIntegrity |
| **Objectives** |
| O.Confidentiality |  |  |  |  |  | X |  | X |  |  | X |
| O.Integrity |  | X | X | X | X | X |  |  |  | X |  |
| OE.Physical | X | X | X | X | X | X | X | X | X | X | X |
| OE.Power |  |  |  | X |  |  |  | X | X |  |  |
| OE.NetworkFlow |  |  |  |  |  |  |  |  |  | X |  |
| OE.NetworkIntegrity |  |  |  |  |  | X |  |  |  |  | X |

Table 7. Threats/Objectives Rationale.

|  |  |  |
| --- | --- | --- |
| **Threats** | **Objectives** | **Rationale** |
| T.UnauthorizedSBCAccess | OE.Physical | OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. This mitigates the risk that unauthorized parties have access to the TOE at any given time. |
| T.CompromisedTemperature | O.Integrity  OE.Physical | O.Integrity ensures that the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party through temperature readings.  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. This mitigates the risk that unauthorized parties have access to the TOE at any given time to read or tamper with the temperature measurements of the TOE. |
| T.CompromisedTime | O.Integrity  OE.Physical | O.Integrity ensures that the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party through time readings.  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. This mitigates the risk that unauthorized parties have access to the TOE at any given time to read or tamper with the time measurements of the TOE. |
| T.CompromisedPowerConsumption | O.Integrity  OE.Physical  OE.Power | O.Integrity ensures that the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party using power consumption measurements.  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. This mitigates the risk that unauthorized parties have access to the TOE at any given time to read or tamper with the power consumption measurements of the TOE.  OE.Power ensures that the TOE power fluctuation and consumption cannot be evaluated or interfered with through Network Level A and/or Network Level B by an unauthorized party. |
| T.CompromisedAcoustics | O.Integrity  OE.Physical | O.Integrity ensures that the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party using acoustics (using a hard disk as a microphone).  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. This mitigates the risk that unauthorized parties have access to the TOE at any given time to tamper with the acoustics of the TOE. |
| T.CompromisedNetworkIntegrity | O.Confidentiality  O.Integrity  OE.Physical  OE.NetworkIntegrity | O.Confidentiality ensures that the information on Network Level A is kept confidential from Network Level B. This mitigates the risk of an unauthorized user overwriting files from Network Level A (Low) to Network Level B (High).  O.Integrity ensures that the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party through overwriting files from Network Level A (Low) to Network Level B (High).  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. This mitigates the risk that unauthorized parties have access to the TOE at any given time to overwrite files from Network Level A (Low) to Network Level B (High).  OE.NetworkIntegrity ensures that the TOE Network follows the BIBA Integrity Model. This prevents data modification by unauthorized parties, and it also prevents unauthorized data modification by authorized parties. |

Table 8. Assumptions/Objectives Rationale.

|  |  |  |
| --- | --- | --- |
| **Assumptions** | **Objectives** | **Rationale** |
| A.Physical | OE.Physical | This assumption is upheld by objective OE.Physical because it ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized party has direct physical access to the TOE or any of the TOE components. |
| A.PhysicalSideChannel | O.Confidentiality  OE.Physical  OE.Power | This assumption is upheld by the following objectives:  O.Confidentiality ensures that the information on Network Level A is kept confidential from Network Level B. This mitigates the risk of an unauthorized user attempting to communicate in any other way (e.g. through light signals).  OE.Physical ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized party has direct physical access to the TOE or any of the TOE components. This can effectively prevent an unauthorized party from attempting to communicate in any other way (e.g. through light signals).  OE.Power ensures that the TOE power cannot be evaluated or interfered with through Network Level A and/or Network Level B. This prevents two unauthorized parties from using the power fluctuation or consumption in order to communicate with each other. |
| A.Power | OE.Physical  OE.Power | This assumption is upheld by objective OE.Physical which ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized party has direct physical access to the TOE or any of the TOE components. This can effectively prevent an unauthorized party from evaluating the power fluctuation and consumption of the TOE.  The assumption is also upheld by objective OE.Power which ensures that the TOE power fluctuation and consumption cannot be evaluated or interfered with through Network Level A and/or Network Level B. |
| A.NetworkFlow | O.Integrity  OE.Physical  OE.NetworkFlow | This assumption is upheld by objective O.Integrity, which ensures that the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party.  Additionally, the assumption is upheld by OE.Physical, which ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized party has direct physical access to the TOE or any of the TOE components. This can effectively prevent an unauthorized party from circumventing the security provided by the TOE through an untrustworthy product.  OE.NetworkFlow ensures that all the TOE components shall operate in the same data flow direction, from Network Level A to Network Level B. The objective prevents any unauthorized party from reversing the data flow direction of the TOE. |
| A.NetworkIntegrity | O.Confidentiality  OE.Physical  OE.NetworkIntegrity | The assumption is upheld by objective O.Confidentiality, which ensures that the information on Network Level A is kept confidential from Network Level B. This mitigates the risk of an unauthorized user overwriting files from Network Level A (Low) to Network Level B (High).  Another objective which supports this assumption is OE.Physical, which ensures that the environment meets the requirements to operate and store the TOE in a secure manner. No unauthorized party has direct physical access to the TOE or any of the TOE components. This can effectively prevent an unauthorized party from overwriting files from Network Level A (Low) to Network Level B (High).  Objective OE.NetworkIntegrity also upholds the assumption by ensuring that the TOE Network follows the BIBA Integrity Model. This prevents data modification by unauthorized parties, and it also prevents unauthorized data modification by authorized parties. |

# **References**

D. E. Bell and L. J. La Padula, "Secure computer system: Unified exposition and multics interpretation," MITRE CORP BEDFORD MA 1976.

M. W. Stevens and M. Pope, *An implementation of an optical data diode*: DSTO, 1999, ISBN:

IEC, "Security for Industrial Automation and Control Systems—Part 4-2: Technical Security Requirements for IACS Components," ed: Standard, International Electrotechnical Commission (IEC) Geneva, Switzerland, 2019.

S. K. Gorantla, S. Kadloor, N. Kiyavash, T. P. Coleman, I. S. Moskowitz, and M. H. Kang, "Characterizing the efficacy of the NRL network pump in mitigating covert timing channels," *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 1, pp. 64-75, 2011.

M. H. Kang, A. P. Moore, and I. S. Moskowitz, "Design and assurance strategy for the NRL pump," in *Proceedings 1997 High-Assurance Engineering Workshop*, 1997, pp. 64-71.

A. Kern, "Advanced features for enterprise-wide role-based access control," in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 333-342.

M. H. Kang, I. S. Moskowitz, and D. C. Lee, "A network version of the pump," in *Proceedings 1995 IEEE Symposium on Security and Privacy*, 1995, pp. 144-154.

A. Anton and R. Cioargă, "Bunkers: Jail Application Level Firewall for the Mitigation and Identification of Service Takeover Attacks on HardenedBSD," in *Computer Security: ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26–27, 2019, Revised Selected Papers 2*, 2020, pp. 242-257.

A. Biryukov, D. Dinu, and D. Khovratovich, "Argon2: new generation of memory-hard functions for password hashing and other applications," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, pp. 292-302.

M. Carbone and L. Rizzo, "Dummynet revisited," *ACM SIGCOMM Computer Communication Review,* vol. 40, no. 2, pp. 12-20, 2010.