genua.

cyber-diode

Technical Information
(Security Measures)

Version 1.1

Edition June 19, 2024

Chapter 1

Management Overview

The genua cyber-diode separates a network with valuable assets from the rest of the Internet. It ensures unidirectional communication by design: Data leaves the assets only through rigorously controlled channels while the cyber-diode prevents any changes from the outside to the protected network. The configuration allows for a strictly regulated data flow and can be used to restrict it even further.

As a software solution running on dedicated hardware the cyber-diode is:

- more convenient than an air gapped system
- more secure than a firewall
- more reliable than an optical fiber diode
- based on the same technology stack as its BSI-approved variant for level “SECRET”.

The cyber-diode is always active and provides unmaintained and automated data flow. By separating hardware and software into independent components the attack surface is drastically reduced in comparison to common firewalls that use an operating system with a monolitic kernel. The layered defense mechanisms of the cyber-diode follow the “castle and moat” principle and provide a very high level of security. By providing controlled and reliable interfaces between the separated components within the cyber-diode, data loss is either prevented or reported. Every successful transfer is acknowledged.

Chapter 2

Technical Overview

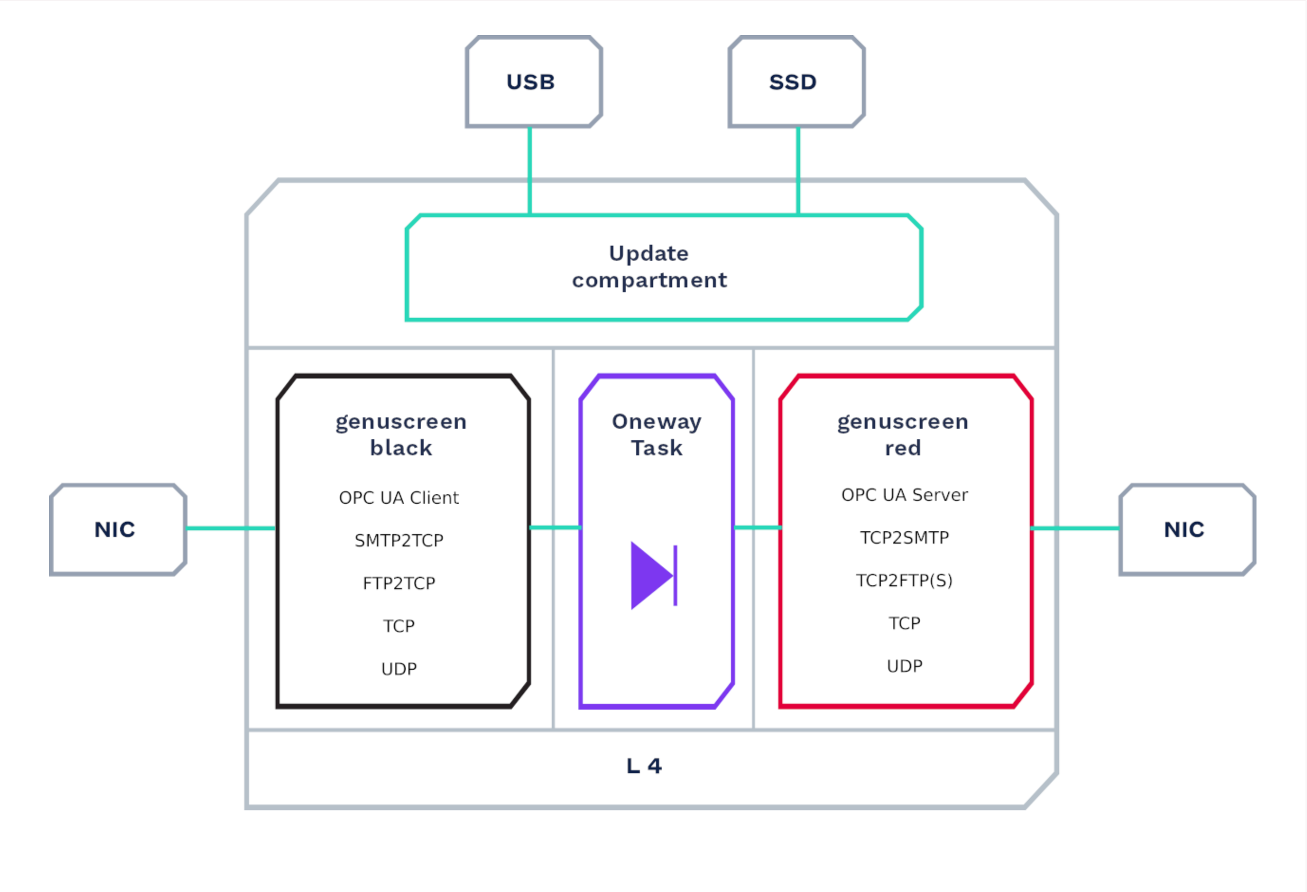

Figure 2.1: cyber-diode schematic

The cyber-diode runs on a L4 microkernel. Because of its structure and small size, this highly specialized “miniature operating system” is easier to defend against abuse. The L4 microkernel creates strictly separated runtime environments called compartments. These compartments allow a tight control over all resource accesses. Thanks to the microkernel even the communication between the compartments only takes place over clearly defined and secured interfaces. This ensures the secure separation of critical services.

The cyber-diode uses four compartments. Three of these compartments run their own hardened OpenBSD-based operating system. The fourth compartment is a native L4 task:

1. genuscreen black compartment (GS black)
2. genuscreen red compartment (GS red)
3. Update compartment
4. Oneway Task

2.1 genuscreen compartments

Each of the two genuscreen compartments **GS black** and **GS red** contains a genuscreen firewall and transforms TCP and UDP streams or higher level protocols into L4 internal data communication. The kernel of each firewall is paravirtualized and restricted to a dedicated CPU core. In addition, it is permitted only to use a dedicated part of the RAM.

Further, Intels virtualization technology VT-d is used as IOMMU to restrict network hardware access to the **GS black** and **GS red** compartments.

2.2 Oneway Task

The **Oneway Task** compartment is logically located between the two genuscreen compartments. The Oneway Task forwards data from the GS black compartment to the GS red compartment, only allowing TCP data success/fail messages from the GS red compartment back to the GS black compartment.

2.2.1 FTP(S), SMTP and OPC UA

The higher level protocols FTP(S), SMTP and OPC UA are converted to an unidirectional TCP stream which is then passed on through the Oneway Task. Relays in the GS black and GS red compartments transform these complex Internet protocols into TCP streams and their data direction is enforced by the Oneway Task.

For connection oriented protocols, data from the black network is accepted by the black relays and the Oneway Task provides the data for the red relays.

OPC UA is a special case: An internal client is implemented on a black-side relay and an internal OPC UA server is implemented on the red-side relay. The internal OPC UA client requests the overall data provided by the OPC UA server (source) in the black network and the internal OPC UA server provides it transparently for the receiving OPC UA client (target) in the red network.

2.3 Update Compartment

The **Update compartment** is necessary to change the configuration and the software of the cyber-diode. The compartment has access to the persistent storage and the USB controller. When a USB stick is inserted in the cyber-diode, the Update compartment verifies the signature of the software and checks the consistency of the configuration. If the verification is successful, the software and the configuration files are copied to persistent storage. After that, the cyber-diode is rebooted and the changes are applied.

Chapter 3

Security Measures

The design of the cyber-diode is based on several independent layers of defense.

- The cyber-diode uses the same technology stack as its technical equivalent, the **vs-diode**. The vs-diode is approved by the BSI (German Federal Office for Information Security) for use in a level **GEHEIM** restricted environment.
- Essential components as **GS black** and **GS red** are certified according to the Common Criteria version 3.1r5 and are also approved by the BSI.
- For all genua products a lifecycle process is established, maintained, and continuously improved.

3.1 Oneway Task Protection

The Oneway Task is protected using a "defense in depth" strategy: A single weakness is insufficient to circumvent the entire oneway property of the cyber-diode.

The L4 microkernel manages CPU and RAM to separate the Oneway Task from the other compartments. Regions of shared memory are used for communication between the compartments, and PCI devices are connected only to specific compartments enforced by the IOMMU. Due to this design, the trusted codebase is reduced to the L4 microkernel and the Oneway Task. In addition, neither the L4 microkernel nor the Oneway Task have a direct connection to peripheral devices.

A remote attacker would be forced to utilize the communication data stream, due to the non-existent management interface. Hence, the attacker would have to break out of the relay, which is running in unprivileged and restricted mode. Afterwards, the attacker would have to gain root permissions to access the shared memory of the Oneway Task or the system calls to the L4 hypervisor. Furthermore, the attacker would have to find an exploit of the Oneway Task or the L4 microkernel. This is highly unlikely, as both were implemented in a very minimalistic and secure way.

3.2 Vulnerability and Patch Management

For the handling of vulnerabilities, third party vulnerabilities, and security patches a process is defined and documented. The vulnerability and patch management process guarantees that all upcoming vulnerabilities of essential cyber-diode components are detected, analyzed, and fixed if an exploit of the component is possible somehow.

- There are several sources for vulnerability reports for products and third party components, including the BSI. In addition, genua software developers are active members of the OpenBSD and OpenSSH community and receive information on vulnerabilities before publication.
- Third party software is integrated as source code and code reviews are conducted the same way as for source code by genua developers.
- All code is structured in privileged and less privileged parts.

3.2.1 Secure Update Process

Supply Chain Review Process and Guidelines are approved and tested by BSI (this includes the development infrastructure):

- When inserting a USB stick containing a software patch or software release, the cyber-diode verifies its signature before installation.
- Configuration updates are checked for consistency. In addition, misconfigurations that circumvent the oneway property are impossible.
- Even with physical access to disk or USB, the BIOS boots cyber-diode software only if signed by genua due to UEFI SecureBoot (a BIOS password must be set to prevent disabling SecureBoot).

3.3 Security Tests

Security related tests are conducted both for the genuscreen and the L4 product family as required for certification according to Common Criteria and approval for classification level RESTRICTED by the BSI. These tests include pen tests and vulnerability analysis by an external laboratory which is accredited by the BSI.

Dynamic code analysis enforces secure execution of the relays.

Static code analysis is conducted.

In general, all code is reviewed internally.

3.4 Functional Tests

Each component is tested during the continuous integration with unit tests. After that, the relays, the genuscreens, and the L4 are tested. The final product is run in the hardware testing lab.

This product contains software based on the OpenBSD operating system.

genua GmbH
Domagkstrasse 7
85551 Kirchheim/Munich
Tel.: +49 89-991950-0
Fax : +49 89-991950-999

All trademarks and licenses indicated in the user manual are the property of their respective owners and are mentioned for information purposes only.

Registered trademarks of genua GmbH are listed on this website:
https://kunde.genua.de/en/imprint/trademark.html

Please note that in accordance with current legal requirements, all owners of waste electrical and electronic equipment (WEEE) may not dispose of WEEE together with unsorted municipial waste. In addition, the following icon of a crossed out trash bin depicted on WEEE devices denotes the requirement to collect and dispose of all WEEE arising separately:

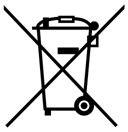

Figure 3.1: Do not dispose of with municipial waste

You as the end user bear the sole responsibility for deletion of all personal information from WEEE devices before their disposal.

For disposal of WEEE devices, please contact genua as the manufacturer at +49 89-991950-0 with the reference “waste electrical and electronic devices”.

A Bundesdruckerei Company

About genua

genua GmbH is a German IT security specialist and has been securing networks and providing top-quality security solutions since the company was founded in 1992. Our business activities cover securing sensitive interfaces in both public authorities and industry, securely connecting highly critical infrastructure, reliably encrypting data communication over the Internet, providing remote maintenance systems for machines, plants and IT systems and providing remote access solutions for mobile employees and teleworkers. Our solutions are developed and produced in Germany and many companies and security-conscious authorities rely on solutions from genua to protect their IT.
genua is a member of the Bundesdruckerei Group.

genua GmbH, Domagkstrasse 7, 85551 Kirchheim, Germany
tel +49 89 991950-0, info@genua.eu