Delft University of Technology - Computer Science

Thesis BSc Project *IN3405*

Charon

The Pluggable Filtering Framework for the Fox-IT DataDiode

Project members:
Matthijs Amesz (4010620)
Erik Biemans (1179233)
Joris van den Oever (4002741)
Jasper Ruoff (4003055)

Company Project Supervisor:
Dr. W.

University Project Supervisor:
Dr. Z. Erkin

University Course Coordinator:
Drs. P.R. van Nieuwenhuizen

Delft University of Technology

Faculty Electrical Engineering,
Mathematics and Computer Science

FOX IT
FOR A MORE SECURE SOCIETY

Preface

At Delft University of Technology, Computer Science students finish the three year bachelor program by doing a BSc project. This thesis is the result of the BSc project of Matthijs Amesz, Erik Biemans, Joris van den Oever and Jasper Ruoff.

The project has been carried out for Fox-IT in Delft from May to August 2012. During this time we followed the complete process of designing, implementing and delivering a software product named Charon. This thesis covers all three phases of the software development process. Charon has been successfully tested and will most likely be integrated in one of the Fox-IT products.

We would like to thank dr. Zekeriya Erkin from the Information Security and Privacy Lab at Delft University of Technology, who guided us through the project and gave us feedback on several topics.

We also want to thank dr. W. for providing us with an interesting and challenging assignment, giving us the opportunity to work at Fox-IT and taking the time to answer our questions during the weekly meetings.

Finally we would like to thank C. MSc for reviewing our source code and providing us with with extensive feedback.

Delft, August 2012

Matthijs Amesz
Erik Biemans
Joris van den Oever
Jasper Ruoff

Abstract

The Dutch IT security company Fox-IT created the DataDiode, a product that connects two networks with different security levels providing a one-way data path. A new appliance of the DataDiode is currently under development. As part of our BSc project, we were given de assignment to develop Charon, a pluggable filtering framework for the new DataDiode appliance.

This thesis describes the complete process of the project and elaborates the choices we have made. In the introduction we explain what a Computer Science Bsc project is at Delft University of Technology and describe Fox-IT and the DataDiode. After this we give a detailed description of the assignment, define the requirements, explain the design methodology and why we consider Charon to be a suitable name for the project. In the next chapter we elaborate on the design choices we have made and illustrate these choices with UML-diagrams. The chapter that follows is about the implementation of the system; we describe the libraries, tools and system components. After this chapter we evaluate the implementation by comparing the implemented functionality with the requirements. We also explain in which way we tested our system to make sure it runs according to the specifications, about the Fox-IT challenge and the code evaluation. We reflect the process in the succeeding chapter where we compare the initial planning with the actual execution, and explain the collaboration between the group members. In the last chapter, we conclude the thesis and list several recommendations for Fox-IT. The appendices that are attached to this thesis contain a complete class diagram, several documents that are created during the orientation phase and a user manual.

Chapter 1

Introduction

In this chapter we give an introduction to the bachelor project. First we introduce the team members and explain what a Computer Science bachelor project means. After this we give a description about Fox-IT, the company we did our internship. This is followed by information about the DataDiode, the product that is extended by the system we have built.

1.1 Bachelor project

We are a group of four Computer Science students at Delft University of Technology: Jasper Ruoff, Joris van den Oever and Matthijs Amesz have a specialization in Media and Knowledge Technology while Erik Biemans is specialized in Software Technology. We have a shared interest in software development, software design and security.

The three year Computer Science bachelor program at Delft University of Technology is completed by a project where everything that has been learned during the bachelor can be used in practice. During this bachelor project students follow the complete process of designing, implementing and delivering a software product for a company or for Delft University of Technology. The duration of the project is ten to eleven weeks with 40 hour work weeks.

We considered several projects in different companies and decided to work on a project for the DataDiode at the Fox-IT Crypto business unit. We chose for Fox-IT because it one of the market leaders in IT-security and working for a company like this provides us with a better understanding of the security market. The project itself is intellectually challenging, feasible in the given time and matches our interests.

1.2 Fox-IT

Fox-IT is a company that specializes in cyber defence, IT Security, lawful interception and digital forensics solutions for government defence and intelligence agencies, systems integrators and commercial organizations worldwide. Fox-IT solutions maintain the security of government systems up to "state secret level" sensitivity, critical infrastructure and process control networks and other highly confidential data. The company also provides services including IT security audits, digital forensic investigations, training programs and managed security services.

The Crypto business unit provides IT-security solutions for clients where state secrets or large commercial interests are at stake. The standard products are for storage, communication, and encryption but it delivers custom solutions as well. These solutions are developed, implemented and maintained by the unit. The Fox Data Diode is one of the communication security products provided.

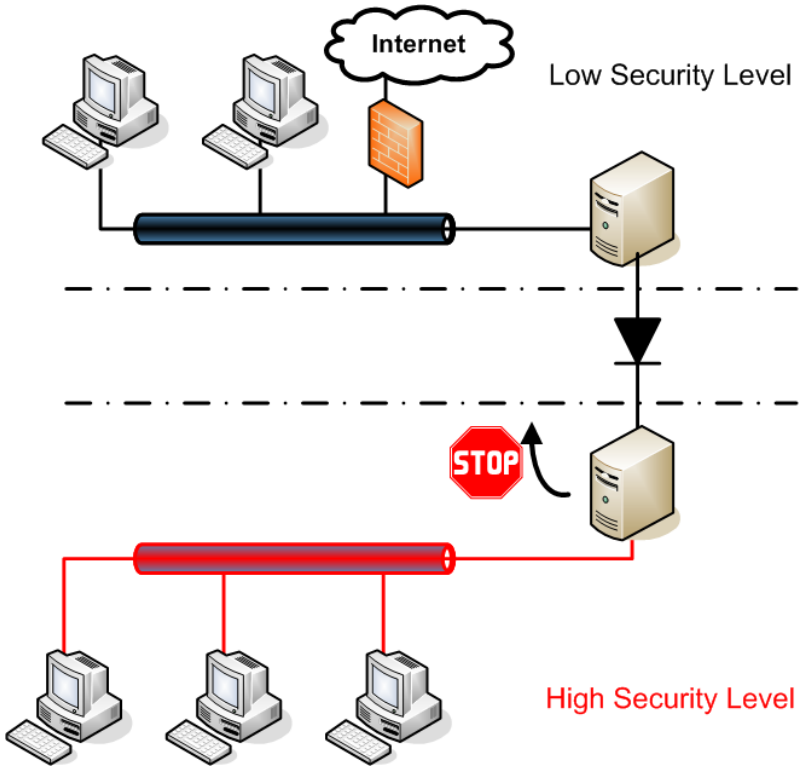

Figure 1.1: The Data Diode facilitates one-way traffic from the Black to the Red network.

1.3 DataDiode

In many cases a network is connected to an external source, like another network, to transfer electronic data. In high-security environments, it is often forbidden to make a physical connection between different networks. The present form of data transfer (using USB sticks, CDs or humans) is never real-time and creates security risks. However, it is used in order to prevent data leakage from the High Security Level (Red) network to the Low Security Level (Black) network. The reception of email or browsing the internet on the Red network is also impossible. Fox-IT created the Data Diode as a solution to this problem. The Data Diode connects two networks with different security levels providing a one-way data path. It prevents information from being transferred from the High Security Level network to the Low Security Level network. The Data Diode uses hardware components that make it impossible for data to be transferred from the Red side to the Black side.

A common DataDiode setup consists of two proxy servers. One of the proxies is placed in the Black network (which can be directly connected to the Internet). The other proxy is placed in the Red network. A one-way physical connection is made between the two proxies to prevent data leakage and guarantee the security of the Red network. Each proxy has a web interface that allows authorized users to configure what is to be transferred from where (Black side) to where (Red side). A transfer can contain files, streaming video, or incoming email.

As the physical hardware connection between the Red and Black network is one-way, any software malfunction (possible bug or tampering) will never compromise the security of the Red network. In addition, all transfers are logged. Error detection and correction will further enhance data integrity and security.

The Data Diode was originally developed for use by governmental organizations, especially those that have to assure a certain security level. Commercial organizations with critical infrastructures like airports, public transport systems or (nuclear) power plants can also make use of the Data Diode.

1.4 Confidentiality

The rest of this report contains detailed information about the design and implementation of Charon. The DataDiode, and by extension Charon, is used in many high security environments. They handle highly confidential data, and are used by clients ranging from major companies to governmental organizations. Because of this, the details about Charon disclosed in this report can not be made publicly available online. A physical copy of the full version of the report is kept by the Computer Science Bachelor Project Coordinator of the TU Delft. To access the full report, please contact the current coordinator.