Alexandre Buge

UID: 34028

Skyrecon Systems

WiViser: Global security

Abstract

Subject: A solution to the actual security problems in Information Technologies.

Internship from 03/01/2004 to 08/31/2004

1 Summary

2 Introduction

In the first part, I will explain the aim of the security solution WiViser by Skyrecon.

In the second part, I will describe my work:

- Multi-platform API.
- Self working agent system.
- Security policy server.
- Wireless network sensor.
- Network firewall.

Finally, I will illustrate my work in public presentations of the WiViser solution.

3 Presentation of the company

3.1 Activities

The Skyrecon sector of activity is exclusively the user desktop security.

The Skyrecon's objective is to secure information against lost of data with DataViser and against intrusion and virus with WiViser.

Skyrecon offers different services such as:

- Software development
- Product promotion
- Deployment and integration of solutions in customer's environment

Skyrecon is currently negotiating with several distributors for partnership. The goal is to centralize the Skyrecon activity on software development and let the distributors make the promotion of Skyrecon solutions.

3.2 History

Skyrecon is a young company created in November 2003. She was founded by 14 co-shareholders. Mr Ravy Truchot is the actual chairman.

Skyrecon is organized in three departments; a commercial department composed by three persons, one other person for the marketing, and a developer department with ten members.

The developer team is cut in three parts directed by one supervisor:

- The research and development division.
- The graphical user interface division.
- The artificial intelligence division.

The aim of the research and development division is to create the low level implementation of the software architecture and realize the security system based on new technologies.

The objectives of the graphical user interface division are to create user-friendly interface for the different Skyrecon softwares and create the basic graphical guideline of Skyrecon.

The artificial intelligence division goal is to implement complex algorithms in Skyrecon softwares like compartmental analysis and data correlation.

The Skyrecon headquarter address is 10, rue du Colisée, in the eighteenth district of Paris.
The Skyrecon development division address is 8, rue d'Argenteuil, in the first district of Paris.

Skyrecon also work with lawyers for juridical questions, patents pending and other licenses and copyright problems.

To manage administration needs, Skyrecon also works with a secretary firm and an accountancy agency.

4 Work realized

4.1 General Goal

Skyrecon created the software named WiViser to secure end-point user desktop.

WiViser software is an alternative to hardware security system. It's a complete security solution which includes:

- Network Intrusion Prevention System.
- WiFi Sensor and control of WiFi environment.
- Network Firewall.
- Application Firewall.
- System Firewall.
- And Compartmental Analysis

To help system administrators, the security policy configuration is centralized and managed by a unique user-friendly graphic interface. Alerts and logs are also centralized and viewable with this interface.

The WiViser solution deployment is managed by an automatic installation system.

I've integrated the research and development division to work on several parts of WiViser:

- The Architecture Abstraction Layer used to realize the agnostic Application Programming Interface.
- The Framework, used to easily segment the software development to obtain a multi-agent system.
- The Policy Server necessary for dispatching configuration to the end-point desktop computer secured by WiViser.
- The WiFi sensor which purpose is to analyze the Wireless environment.
- And the Network Firewall, required by the Intrusion Detection System and the WiFi Sensor to block attacks.

4.2 The API

The APIs (Application Programming Interface) are created to abstract the Operating System specificity. With these API, developers can create multi-platform compliant agents faster. APIs are already working on Operating Systems like Windows, UNIX, Linux, Mac OS-X...

WiViser is developed in C language. C is an old language which is not ‘object’ oriented like more recent languages. C doesn’t supply elementary structure containers and algorithms.

These missing elementary algorithms have been integrated in the APIs to provide a common interface to all Skyrecon agents and clarify their source code.

More complexes APIs were written as a second layer to bring more features to agents like tasks spooler, tasks scheduler and XML parser.

The Artificial Intelligence division also works on an API to create a multi pattern matching algorithm and an expert system.

One of my tasks in Skyrecon was to teach to other co-workers how to use the technologies brought by the APIs.

That’s why each API contains comments created by the Doxygen tool and illustrated by an example of use.

4.3 The Framework

The framework was created to enable developers to create independent parts of WiViser software. Each part is able to communicate to each other. All of them working together to make a complete software.

The multi-agent system is inspired from the CORBA architecture.

The framework purpose is to load agents, manage their tasks and allow the inter-agent communication with synchronous or asynchronous messages. It's the core of Skyrecon software and it's build on previously developed API layer.

4.4 WiViser Architecture

WiViser is divided in three parts:

- The Graphical User Interface.
- The Policy Server.
- The Client Probe.

The Graphical User Interface shows the alert stored by the server and lets the user set the security policy.

The Policy Server receives security policy from the Graphical User Interface and dispatches it on the end-point user desktop.

The Client Probe secures the desktop by applying the security policy. It also manages the attacks and intrusions detected by other agents and sends alerts to the server.

The Policy Server and the Client Probe are based on the framework architecture. They have a special agent to handle each action.

For WiViser, I am still in charge of several agents:

- An agent made to output messages from other agents and save them in a log file
- A server agent used to accept probe connections and send them the right security policy.
- A WiFi sensor agent scanning the neighborhood of the desktop to prevent wireless attacks like “man in the middle”.
- And finally the Network Firewall agent which block specific network connections when an attack is detected.

4.5 The Network Firewall

Building a driver for the Network Firewall agent was the main part of my work. The driver is loaded in the kernel land of the operating system. Developing drivers in kernel mode brings a lot of constraints. It's harder and makes the source code more accurate.

Another part of the software had to be created to enable the communication between the kernel driver and the firewall agent.

The Network Firewall following the filtering rules he received; have to destroy some network packets. The firewall has to optimize the filtering rules to run as quickly as possible.

4.6 WiViser's promulgating on information technology market.

To increase the presence of WiViser on the market I had to participate to a software presentation as a technical assistant.
I worked with the commercial team to explain the advantage of our technology to potential interested venture capitals, industry helper agency like ANVAR, and software distributors.

Then, I received more responsibilities in the presentation of our technology. I made a seminary organized by Skyrecon to sensibly the main actor of the IT industry to the modern security problematic.

5 Conclusion

My internship at Skyrecon gave me a great experience in software conceptions and analysis. Starting the internship at the same time of the WiViser software creation allowed me to have a great expression liberty that made my work more interesting.

I learned lot of different things, in kernel programming, marketing, and commercial domain. Little and young PME give the advantage to offer you a lot of responsibility and to work on several domains at the same time.

Working in a great team helped me to accomplish my tasks in the continuity of my Epitech studies.