BLËSK Interview

January 2018

Web SIte

www.cegep-ste-foy.qc.ca

Sector

School

Location

Sainte-Foy, Quebec

Solution

R&D for BLËSK Network Monitoring

BLËSK joins forces with Cegep de Sainte-Foy to develop a methodology.

CONTEXT

BLËSK is a tool that is constantly evolving and always on the cutting edge of technology thanks to integrated open source tools, but also thanks to its partnership such as with the Cegep de Sainte-Foy (Cegep)

We interviewed Mr. François Gagnon—Principal researcher at the Cyber Security Research Laboratory at the Cegep to learn about his experience in developing a methodology for monitoring in segmented networks.

WHAT WAS THE MANDATE REQUESTED OF YOU BY THE BLËSK TEAM?

F.G. : This project aimed at developing a methodology for monitoring on a segmented networks. More specifically, the project aimed to exploit different techniques to automatically **detect** components (eg computers, network equipment) and **identify** their characteristics (eg services offered, operating systems, manufacturer, version) on a segment computer network from an external point of view.

HAVE YOU WORKED ON A SIMILAR PROJECT BEFORE? IF YES, BRIEFLY DESCRIBE THE PROJECT YOU'VE WORKED ON.

F.G. : Yes, as part of my Ph.D., I did a project to identify the family and operating system version of a computer by listening to network traffic generated by it. Each system has small pecularities as to how it transmits data (or more broadly how it implements standard protocols), which distinguishes them from each other. On the other hand, the external point of view (segmented networks) on the new project brings a more realistic and more complex dimension.

WHAT WERE THE STEPS IN SOFTWARE DEVELOPMENT?

- Establishment of a test environment to experiment with different approaches and technologies.
- Study of the two main technologies (netflow and sflow) and their contribution towards the project objective (detection & identification)
- Develop proof of concept for component detection / idenfitication based on flow inspection.
- Exploration of alternative techniques for the identification of different Linux distributions.
- Preparation of a prototype for integration as aBLËSK module.

BLËSK Interview

January 2018

WHAT WERE THE BENEFITS FOR YOU TO PARTICIPATE IN THE DEVELOPMENT OF THIS EXTERNAL SOFTWARE ?

F.G. : An important advantage is the acquisition of new technical expertise (R&D) in the manipulation and analysis of the network flow communications. An expertise that opens several doors for future R&D projects. This is an element that should take more and more space in the management of medium and large networks.

Another advantage of this project was the contribution to the level of the research laboratory. A direct contribution in grants which made it possible to hire a student and to make available two teachers to work actively on the project. Any grant brings an more visibility to the laboratory, helping it to become better known. The addition of a new partner (BLËSK / PRIVAL) opens the door to a longer-term partnership. The fact that the partner company is based in Montreal, while the laboratory is in Quebec, demonstrates the uniqueness of the laboratory (and its expertise).

WHAT WHERE THE DIFFICULTIES FACING THIS PROJECT?

F.G. : Like any short-term R&D project (6-month project in this case) with an industrial partner, it is difficul to fully understand the general needs of the company (what will become a competitive advantage for them), but also what they already master (what is not worth exploring since equivalent solutions already exists within the company). For reasons of intellectual property protection and limited time, it is not clear what the company is already doing before starting the project.

Another challenge was that reality and needs change quickly. From the moment the grant application is written down to the middle of the R&D project, many things have time to change which make some of the originally planned tasks less relevant. Project planning / management is therefore more difficult in this sense since the R&D project does not always evolve independently of the other projects of the company.

WOULD YOU BE WORKING WITH BLËSK TO DEVELOP ANOTHER SOFTWARE?

F.G. : Absolutely. Although this year I am not in the research laboratory, I remain open to other collaborations with the BLËSK team for new R&D projects.

About BLËSK

BLËSK is a suite of applications for monitoring and network management, consisting of a mix of open source and proprietary tools. BLËSK helps you understand the behavior of your network and services. Anyone can now view and analyze problems before they affect your infrastructure.

Web site

w w w . b l e s k . c a

Headquarter

Brossard, Qc, Canada

T: 1-866-761-9973

Email: sales@blesk.ca

blësk network monitoring