CELTIC
Telecommunication Solutions
www.celtic-initiative.org

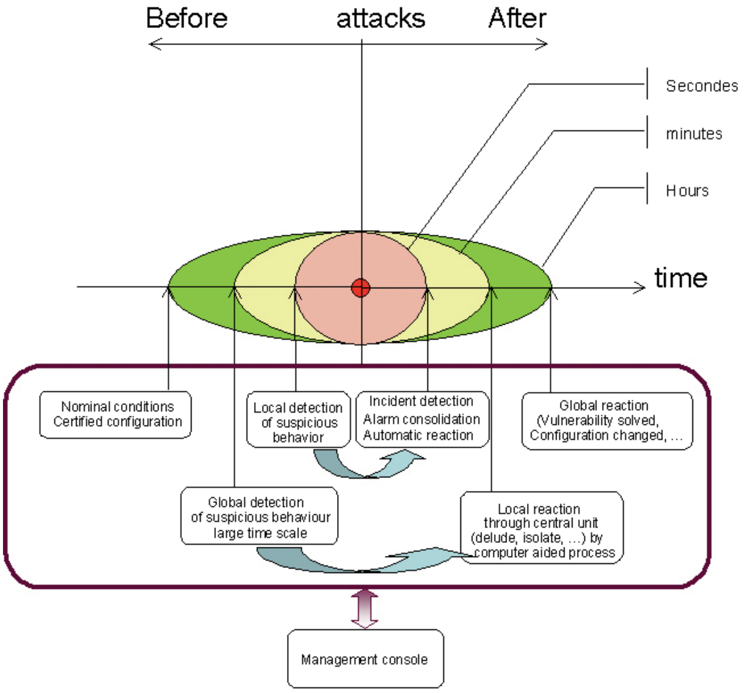
REaction after Detection

RED manages the security of information systems through a global approach, focusing on the reaction phase. By ensuring both accuracy of the reaction mechanism and efficiency of the reaction propagation, RED will develop a global security management platform which integrates the different techniques in a unique management console.

Main focus

Today, IP-based telecommunication and information systems constitute a widespread and inter-connected system, linking heterogeneous systems into a mesh of ever-increasing complexity. This situation implies an increasing number of vulnerabilities exploitable by a wide range of threats, as well as an increasing number of low-tech and high-tech attacks. Due to these increasingly common phenomena, it is now vital to have innovative solutions to react accurately to the detected attacks. The RED project defines, designs and tests innovative solutions for telecommunication IP networks in order to ensure an accurate detection/reaction process by developing tools and techniques to:

- Enhance the management of alerts by improving the diagnosis accuracy,
- React automatically and accurately to detected and well-characterized attacks,
- Define and dynamically deploy new equipment configurations to enhance security protection,
- Manage efficiently and coherently all of the above-mentioned through a security console which ensures information presentation and action possibilities in an understanding manner to take easily and – most of the time – independently appropriate reaction decisions.



RED

Project ID: CP3-024
Start Date: 1 November 2006
Completion date: 30 April 2009

Partners

Alcatel CIT, France

CRP Henri Tudor, Luxembourg

EADS DCS, France

Exaprotect Technology, France

France Télécom R&D, France

GET/ENST Bretagne, France

GMV Soluciones Globales Internet S.A., Spain

Innovae, Spain

Telindus, Luxembourg

Thales, France

Univ. Politécnica de Madrid, Spain

UPVLC - Universidad Politécnica

de Valencia, Spain

Co-ordinator

Cécile Herbault
EADS DCS, France
E-mail: cecile.herbault@eads.com

Project web site

www.celtic-initiative.org/projects/red

Approach

The first step of the RED project defines use cases that are the base lines of the project and which validate the RED success through the final demonstrator. From those use cases, requirements and a global architecture are elaborated. The definition of a detailed glossary and terminology is one of the key successes of this preliminary phase.

The approach adopted by RED is split into three technical axes, each focusing on one innovative aspect: alert management, automatic counter measure, and policy based configuration management, which are integrated in a unique security console. Each of these aspects follows a similar process from a study of the state of the art to specification, design, development, and test. Then, in order to promote our global approach to security management, those technical outputs are integrated and interfaced through a unique security console in the RED prototype. This console manages all the reaction processes: from automated and hot reaction to reconfiguration which requires a validation process.

To validate the proper operation of security products, and particularly intrusion prevention devices and security information management consoles, the RED prototype has been and will be tested in a test environment. This test bed replicates the operation of the core IP network of a telecommunication provider, using the same hardware platforms and configuration as a commercial network. This test bed has been in operation for several years and has been successfully been used for product evaluation and selection. It can reliably re-create test conditions to measure improvements in the experimented equipments.

Main results

The major project achievements that are targeted can be summed up as the specification, development, integration and testing of:

1. Enhanced alert management components to collect and aggregate a large amount of information coming from different sources, and harmonize them to a standard format in order to be analysed.
2. Automated reaction mechanisms implemented through new and innovative techniques for launching automated, trustworthy, efficient, and accurate reactions inside a complex, multi-organisational system in order to counter any form of unexpected, abnormal action.
3. Policy based counter-measure functionalities to improve and update the configuration of a complex telecommunication system according to detected attacks. These updates will be done through a computer-assisted process in order to ensure efficient deployment and to guide the administrator in the jungle of security components to reconfigure.
4. A security console on a demonstrator platform: the project will implement the previous components and mechanisms in a centralised security console that can manage all the reaction processes. The RED proof of concept will be demonstrated on a test bed platform hosting the RED security console.

Impact

There is a strong need for security mechanisms to ensure system protection not only at design time, but also during all of its operational life. System management operators do not have any integrated solution to execute their emergency plan, and there are no security products on the market, which propose solutions to react quickly and efficiently to the threat.

One of the direct results of RED is to improve the resilience to attacks of core IP networks and large information systems, which form a critical infrastructure for communication and services today. RED will provide tools for reacting automatically to threats, deploying the appropriate configuration changes, and verifying that threat response is appropriate. This will allow the deployment of security-adaptive networks and information systems, which can harden in the presence of threats while servicing users at the maximum of their capabilities under normal conditions.

About CELTIC

Celtic is a European research and development programme, established as Eureka cluster, to strengthen Europe's competitiveness in telecommunications through short and medium term collaborative R&D projects. Celtic is currently the only European R&D programme fully dedicated to end-to-end telecommunication solutions. Launched in November 2003, Celtic (Cooperation for a sustained European Leadership in Telecommunications) was founded and has been supported by major European telecommunication players, both vendors and operators. Celtic fills the gap between public R&D programmes not specifically focused on telecoms and short-term R&D efforts by the telecoms industry

Timeframe: 8 years, from 2004 to 2011

Total budget: in the range of 1 billion euro, shared between governments and private participants

Participants: companies from the telecommunications industry (small, medium and large), universities, research institutes, and local authorities from all 35 Eureka countries may participate in Celtic projects.

CELTIC Office

c/o Eurescom,
Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989 405,
e-mail: office@celtic-initiative.org
www.celtic-initiative.org

EUREKA
Σ! 3187