Project Achievements

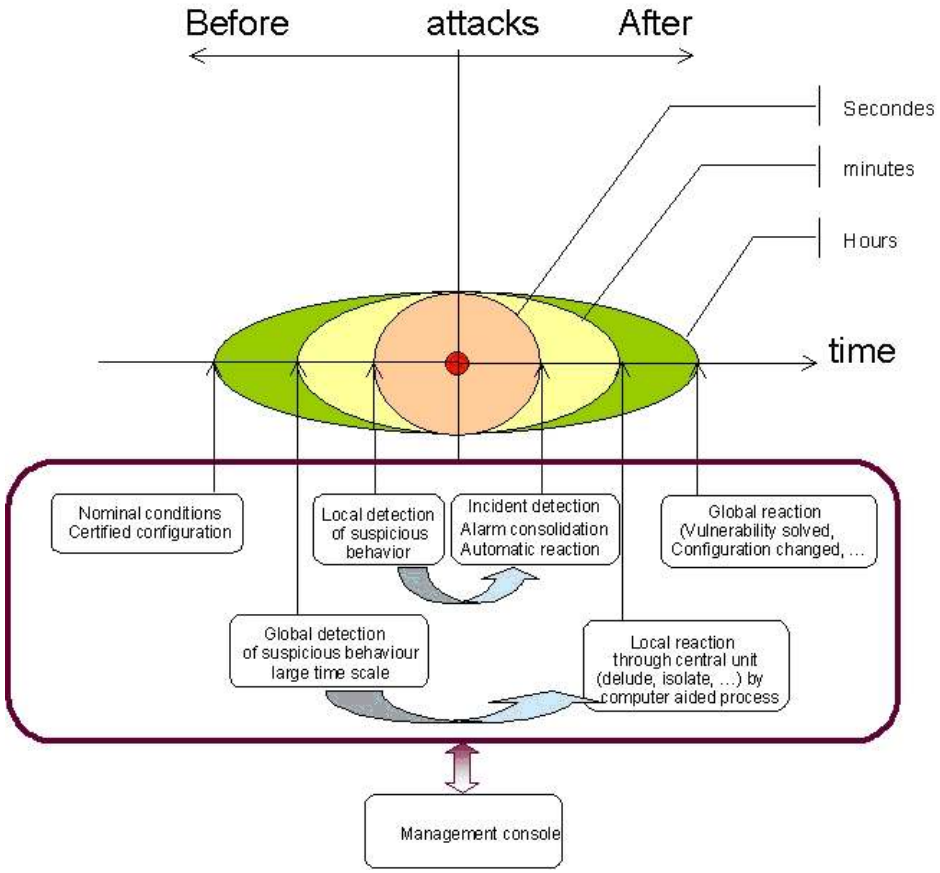
REaction after Detection

RED manages information systems security through a global approach and focuses on the reaction phase. By ensuring both accuracy of the reaction mechanism and efficiency of the reaction propagation, RED elaborated a global security management platform integrating the different policy-based response 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 exploitable vulnerabilities as well as an increasing number of low and high-tech attacks. Due to these increasingly common phenomena, it is now vital to have new and innovative solutions to react accurately to the detected attacks. The RED project defined, designed and tested 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,



RED

Project ID: CP3-024

Start Date: 1 November 2006

Closure date: 30 April 2009

Partners:

Alcatel-Lucent, France

CRP Henri Tudor, Luxembourg

EADS DCS, France

EPT INNOVATION - ExaProtect, France

GET/ENST Bretagne, France

France Télécom R&D, France

Innovae, Spain

Soluciones Globales Internet S.A., Spain

Telindus, Luxembourg

Thales, France

Universidad Politécnica de Madrid, Spain

Universidad Politécnica de Valencia, Spain

Co-ordinator:

Christophe Ponchel

EADS DCS, France

E-mail: christophe.ponchel@eads.com

Project Website

www.celtic-initiative.org/projects/red

- Define and dynamically deploy new equipment configurations to enhance security protection,
- Manage efficiently and coherently all these through a security console ensuring information presentation and action possibilities in an understandable manner to take easily, and most of the time, alone, appropriate reaction decision.

Approach

The first step of the RED project defined use cases that were the base lines of the project, and that validated the RED success through the final demonstrator. From those use cases, requirements and a global architecture were elaborated. A detailed glossary and terminology definitions have been key factors for the success of this preliminary phase.

Then the approach followed by RED was split into three technical axes, each one focusing on one innovative aspect: alert management, automatic counter measure and policy based configuration management which were integrated in a unique security console. Each of these aspects followed 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 were 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 that requires validation process.

To validate the proper operation of the RED components in different environments, these ones were tested on three testbeds with VoIP and adhoc infrastructures, providing attack replay and reaction enforcement capabilities.

Achieved results

Regarding standardization, RED partners have built part of their work on already existing standards (XML-based protocols, IDMEF for intrusion message exchange, Web services…) and studied possible extensions of the IDMEF format. By leveraging the experience of every participant in the form of use cases, a common vocabulary has been created early that has then guided the work.

The dissemination has been organized to support the exploitation of the project results and has mainly addressed potential end-users. Large efforts have been devoted toward future exploitation. For instance, EADS has disseminated results of the RED project to show the know-how and competence of European industrial companies into IP security market. Many publications and presentations were also done during the project (CRiSIS 2007 and 2008, IBC exhibition, IEEE International Conferences, Celtic Events 2008 and 2009...).

Fully adapted industrial products based on the defined framework are currently under development. For instance, EADS whose security is a key activity in Europe, is integrating new reaction components for its security management solution. Another example: Alcatel-Lucent benefits from the project by integration of detection and reaction mechanisms in network elements with enhanced sensors and mechanisms. ExaProtect is exploiting the results of the project by extending their correlation engine (reaction capabilities) and by improving the expertise of the R&D team.

Impact

One of the major impacts is that detection and reaction solutions for system management operators relying on concepts studied in the RED project are now close to be launched in the market. Another important aspect is that embedded components use the same protocols (e.g. Web services) and exchange formats, which offer a full interoperability with external tools. For instance, a customer can replace the ACE components used in the project and developed by the following companies, SGI, GET-ENST, ExaProtect, by any other ACE using the IDMEF exchange format and having equivalent capabilities.

About Celtic

Celtic is a European research and development programme, designed 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.

Timeframe: 8 years, from 2004 to 2011

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

Participants: small, medium and large companies from telecommunications industry, universities, research institutes, and local authorities from all 35 Eureka countries.

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