Project information

CELTIC
Telecommunication Solutions
www.celtic-initiative.org

Building security assurance in open infrastructures

Bugyo aims to define a security framework to measure, document and maintain the security assurance level of services based on telecommunication system. The project intends to fill the current gap of a general way to measure the confidence that operators and end customers can have in the security of the infrastructure, in end-to-end security services and in the security of end-to-end services above those architectures.

Main focus

Open systems such as telecommunication infrastructures are massively distributed. They are composed of highly connected sets of managed products. Products dedicated to security are numerous in this field of application, such as intrusion detection, vulnerability discovery, overall measure, analysis, and counter-measure applications.

Bugyo will federate tools, techniques and a global topology view in a framework in order to offer a complete and realistic picture of the overall confidence level for a telecommunication network that every telecommunication manager needs.

The Bugyo cockpit will display real-time dynamic indicators as well as present reports that take into account combinations and the composition of different elements. Bugyo aims at being the first security assurance measurement and security events monitoring product at network scale.

Bugyo

Project ID: CP2-002
Start Date: 1 June 2005
Completion date: 30 June 2007

Partners

Acotec, Spain
Alcatel CIT, France
Centre Henri Tudor, Luxembourg
Telefonica, Spain
EADS-DCS, France
GET-ENST, France
Ericsson, Sweden
Karlstad University, Sweden
OnePutt Solutions, Sweden
Oppida, France
TeliaSonera, Sweden
Telindus, Luxembourg

Co-ordinator

Jose Araujo / Bertrand Marquet
Alcatel, France
E-mail: jose.araujo@alcatel.fr / Bertrand.marquet@alcatel.fr

Project web site

www.celtic-initiative.org/projects/bugyo

Approach

The technological innovation consists of the development of security assurance assessment on an operational telecommunications system by launching tests and collecting results within distributived systems. Mobile agent technology in the middleware domain will act as a test vector that will gather the required results. Bugyo will provide guidelines and methods as well as software applications to assess the overall confidence that can be obtained. The framework will be based on a specific middleware, using technologies, such as mobile agents, to collect information within infrastructures in a non-disturbing and non-intrusive way.

Information will be collected by applications such as an automatic vulnerability research engine and a protocol security analyser. Bugyo will include information on configuration management (linked to databases of certified configuration) for automatic security testing.

The focus point will be a system cockpit that analyses all the results and provides an assurance level synthesis similar to the one produced by Common Criteria Evaluation Assurance Level.

Bugyo monitoring will need to provide a clear and high-level view of the security assurance of the network, which can be used by operators without strong security knowledge. Bugyo will integrate the different types of security assessment tools and methodologies. This will be the necessary pre-condition for providing a correlated synthetic view to the operator, especially when he is facing the management of a large and interconnected network.

Main results

One of the main results will be a system **security assurance framework** including methodologies, best practices, tools and a system security cockpit.

Bugyo will provide:

- **security assurance characterization** for the operation of **telecom services** addressing specificities of the underlying infrastructure.
- an **integration framework** providing the necessary means to integrate and coordinate different security tools as well as different security abstraction models in order to define different security profiles for the assessment of the security assurance of a determined service.
- the **System Security Cockpit** representing the interface for the operator or the service provider to perform necessary operations in order to obtain and maintain a security assurance level for a specified service.

The **Security Cockpit** should be able to give the necessary information to operators and service providers about the security assurance of the deployed infrastructure. Based on the displayed information, the operator will be able to take necessary and suitable actions without the knowledge of a security specialist and will support decisions to maintain operations at the necessary security level that is required.

Impact

Operators will directly benefit from all results, as they are building, maintaining, or managing the implemented system. Evaluation facilities will have more performing tools and methodologies to evaluate the security of products and systems.

Equipment providers will benefit from better methodologies and test platforms to produce highly secure network elements that can provide the necessary foundation to provide secured carrier infrastructure systems. The project will help clarify the two following interfaces: the first one between end user and service provider and the second interface between services/telcos and network equipment vendors. The goal of this project is to achieve security assurance at the first interface level. The way to achieve it will impact the second interface.

The Bugyo partners are already major actors in managing and securing telecommunications infrastructures. Their intent is to complete their security tools to be more relevant and cooperative in order to focus on their telecommunications infrastructure. The project will give to its participants real environment feedback and allow them to adapt the framework to real needs very quickly after the project completion. Fully adapted industrial products based on the defined framework will be possible, contributing to highly secured telecommunications infrastructures.

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 the only European R&D programme fully dedicated to end-to-end telecommunication solutions.

Timeframe: 5 years, from 2004 to 2008

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

Participants: small, medium and large companies from the telecommunications industry, universities, research institutes, and local authorities from 33 countries

CELTIC Office

c/o Eurescom,
Schloss-Wolfsbrunnenweg 35,
69118 Heidelberg, Germany
Phone: +49 6221 989 372,
e-mail: office@celtic-initiative.org
www.celtic-initiative.org

EUREKA
Σ! 3187