Project Achievements

Building security assurance in open infrastructures

The Celtic BUGYO project has defined a framework to measure, document and maintain the security assurance level of telecommunication services. To build confidence that network assets are adequately protected, this framework has provided a methodology, specific metrics, and software applications through an easy-to-use graphical user interface: the security cockpit.

Main focus

As of today, there is no global solution that monitors the state of security countermeasures at service level for telecom infrastructures and build confidence that network assets, infrastructures and services are adequately protected. The challenge was to provide methodology, specific metrics and software applications that are providing security assurance monitoring. In BUGYO we defined an operational methodology that can be practically applied in particular by major telecom operators and service providers to gain confidence in the security deployed to protect their service and the associated business revenues. This operational methodology provides foundation for the security assurance framework development and deployment.

Approach

The project delivered a complete chain for the security assurance dimension of a telecom infrastructure: from an analysis/ modelling of security assurance needs for several service via an applicable methodology to a framework and a supervision tool.

All the work achieved has been a result of partners' involvement and collaboration in this project, as at the beginning very few elements existed on how to address security assurance in telecom infrastructures.

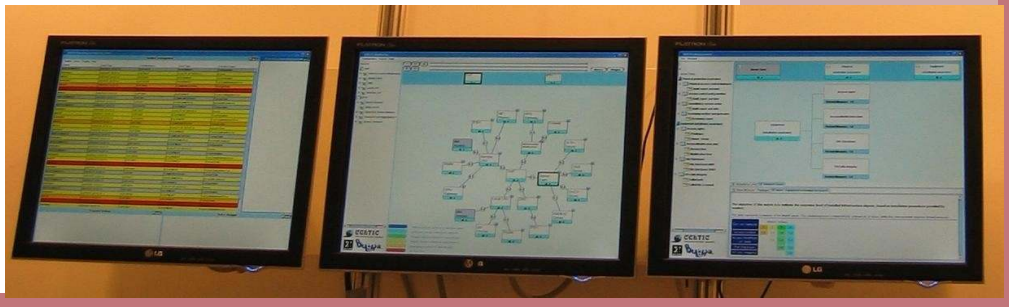
Complexity of the monitored services and infrastructures was a major challenge in the project.

This was resolved by modelling services regarding critical elements of the infrastructure for a dedicated service. Having a strong assurance on critical security functions of a service will be enough to have confidence that the service will face most of the security threats and, consequently, guarantee service continuity. The result is a robust low complexity system, the BUGYO system, that observes the complex system of the service infrastructure.

Achieved results

The BUGYO outputs can become an industrial product with a limited industrial and deployment effort. They can also be easily integrated in a security management solution or any network management system or operation support system.

The project delivered documents, software, prototypes, and a demonstrator. BUGYO provided a modular and open implementation of a complete measurement framework. Assurance



BUGYO

Project ID: CP2-002

Start date: 1 June 2005

Completion date: 1 July 2007

Partners:

Acotec, Spain

Alcatel-Lucent, France

Centre de Recherche Public Henri Tudor, Luxembourg

EADS-DCS, France

ENST, France

Karlstad University, Sweden

OnePutt Solutions, Sweden

Oppida, France

TeliaSonera, Sweden

Telindus, Luxembourg

Telefónica I+D, Spain

Co-ordinator:

Bertrand Marquet

Alcatel-Lucent, France

E-mail: bertrand.marquet@alcatel-lucent.fr

Project Website

www.celtic-initiative.org/bugyo

metrics have been specified for a VoIP infrastructure. A distributed and scalable multi-agent system has been developed in order to collect measures generated by probes implemented on critical equipments of the infrastructure. The initial and strong effort to build a development kit has been efficient as it allows fast development and integration of a specific agent. Existing open source probes as well as BUGYO-specific probes are included in the architecture.

This operational methodology, which represents the core of the BUGYO project, is composed of six main steps: first, the **modelling** allows decomposing the service in order to identify security critical components. In order to realise this phase, a dedicated security assurance model has been defined. The second step addresses the **selection of metrics** that defines what needs to be measured. The third step concerns **measurement** addressing network investigation by deploying specific probes implementing selected metrics. The measures are **aggregated** in the fourth step to express the assurance level of critical infrastructure objects and to derive an assurance level for the service. The fifth step provides an **evaluation** of the assurance status based on the result of the aggregation step. This step is crucial for the operated service as it measures deviation, evolution and by consequence determines management actions that need to be taken in order to maintain targeted security assurance level. In order to provide evaluation means, five assurance levels have been defined enabling the expression of the actual security assurance:

- **Assurance level 1**: Rudimentary evidence for parts
- **Assurance level 2**: Regular informal evidence for selected parts
- **Assurance level 3**: Frequent informal evidence for selected parts
- **Assurance level 4:** Continuous informal evidence for significant parts
- **Assurance level 5:** Continuous semi-formal evidence for the entire system

The last step provides means to the operator to **monitor** the security assurance status both at service and network infrastructure objects, to be able to determine the causes of assurance deviation and, consequently, to provide assistance for security management.

The description of this methodology is available on the project web site.

Impact

The provided framework aims to fill a gap for telecom security and risk management. It represents the last step in risk management. The first approach consists in a proactive and continuous monitoring of deployed security countermeasures within telecom and services infrastructures security in order to verify countermeasures correctness but also leverage security audits and certifications of infrastructures objects. The second addresses security assurance modeling of complex infrastructure, the complexity being managed by reducing the model by identification of critical elements.

The continuous assurance measurement is provided by definition of appropriate metrics as well as near real time aggregation of results. The provided framework is expected to provide effectiveness in managing security assurance in operation through three main functions: Monitoring, measurement and assistance. Those three functions represents the three screens of the developed security cockpit which includes interfaces to Network Management Systems (NMS) and Security Information Management (SIM) systems

The developed cockpit and associated three main functions can lead to several ways of industrial exploitation: the monitoring function, Service monitoring and or security monitoring, is the immediate possibility of industrial exploitation target NMS and SIM market. The measurement functions with metrics and probes developed technologies can enhance infrastructure based security management and expertise and therefore be applied to others critical infrastructures. The assistance functions can be exploited in alarm and incident management solutions as well as for the growing compliance management market.

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