Project Information

Building Security assurance in Open Infrastructure, beyond

Security assurance is ground for confidence that a system security works as expected and is ready to face attacks against service infrastructures. As of today, there is no solution that monitors the security assurance for telecom infrastructures at the service level and builds up confidence that the involve network elements, infrastructures and services have the specified security working as expected.

Main focus

Open systems such as communication services are nowadays massively distributed. They rely on ubiquitous, evolving and multi-domain communication infrastructures composed of highly connected sets of managed products. Many products dedicated to security (such as firewalls, proxies, anti-virus, intrusion detection and prevention systems, and vulnerability scanners), act as deployed security safeguards at application or network level.

In a first phase of the project (BUGYO, Celtic project number CP2-002), we have already demonstrated the feasibility of federating the continuous monitoring of deployed safeguards. This was realized to gain objective confidence that the deployed safeguards meet the security policy by the means of distributed probes and a central assurance evaluation server.

The global aim of BUGYO Beyond is to build a global continuous security assurance methodology and framework that will federate security assurance tools and techniques for evolving communication service infrastructures relying on different technologies managed by multiple entities that need to share security assurance information.

Approach

Surveys indicate that most often security fails because the safeguards are either misconfigured or inadequately monitored. The continuous security assurance goal is to give a global assessment of the deployed safeguards' configurations and proofs that they comply with the security expectations stated in the security policy and the security risk analysis.

A specific methodology for continuous security assurance monitoring of communication services, developed during the first phase of the project, relies on a system of five assurance levels codified in a taxonomy, a security assurance model for static

BUGYO_Beyond

Project ID: CP5-003

Start Date: 1 November 2008

Closure date: 1 May 2011

Partners:

Alcatel-Lucent, France

B-Kyung System, South Korea

Centre Henri Tudor, Luxembourg

EADS DS, France

Innovalia Association, Spain

Itrust Consulting, Luxembourg

Nethawk Oyj, Finland

Nextel, Spain

Nokia Siemens Networks, Finland

Oppida, France

TELECOM ParisTech, France

TeliaSonera, Sweden

Universidad Politécnica de Valencia, Spain

Uphill Oy, Finland

VTT (Technical Research Center), Finland

Co-ordinator:

Samuel Dubus

Alcatel-Lucent, France

E-mail: samuel.dubus@alcatel-lucent.com

Project Websites:

www.celtic-initiative.org/projects/bugyo-beyond

http://projects.celtic-initiative.org/bugyo-beyond/

services and a six-step methodology.

The challenges in BUGYO Beyond are to enhance this methodology and demonstrate its applicability for multi-domain, ubiquitous and evolving communication service infrastructures.

To tackle these challenges, the project studies a modeling abstraction called “assurance profile”. Assurance profiles act as modeling patterns that can incorporate best practice knowledge into a real model of a service to reflect the impact on the security assurance of new parts of the relaying infrastructure or evolution of third-party’s network. Furthermore, the measurement infrastructure is improved to manage the dynamic collection of base measures used by metrics associated with assurance profiles.

Another focal point is the security cockpit that presents a synthetic view of the global security assurance level of each supervised communication service. It enables cockpit operators and decision makers to monitor and correct security assurance variations that could lead to breaches using correct priorities and relevant business related indicators.

Moreover, as security assurance needs to be widely accepted as a realistic source of confidence between communication service providers and third-parties, another challenge of BUGYO Beyond is to work towards proposals for standardization.

Main results

The major result expected is a **dynamic, multi-domain and continuous security assurance monitoring framework** including methodologies, best practices, tools, and a management cockpit.

The project will provide:

- The structure of service **security assurance profiles**, as the means to define security assurance needs for whole or part of service provider’s infrastructures. This will enable multi-domain monitoring in which service and third-party providers can agree within a security level agreement (SecLA) on commonly accepted service security assurance profiles.
- The dynamic **assurance measurement framework** aims to continuously gather the necessary base measures across the evolving communication infrastructure, produced by dynamically deployed probes, on which metrics of service assurance profiles rely.
- The **Security Assurance Cockpit** represents the interface for the service provider’s decision maker to prioritize necessary operations to maintain a targeted security assurance level.

The project will also **draft a proposal for standards and define a process for the certification** of security assurance profiles and metrics.

Impact

All actors involved in the operation of communication service look for methodologies and tools to manage in real-time the confidence they can have in the security of the services they provide to their customers. **Security is no longer an option** service providers can ignore. But, having a deployed security does not mean the security is effective.

Following the BUGYO approach, BUGYO Beyond will continue addressing a *better* security rather than a *larger* security.

The project will help clarifying operational security assurance at three interfaces:

- Between service providers and third-party infrastructure providers.
- Between service or infrastructure providers and infrastructure equipment vendors.
- Between end users and service providers.

BUGYO Beyond results will help building communication services in which deployed security is more reliable and sustainable along the life-cycle of the service infrastructure no matter it relies on third-party infrastructures. They will give service providers the ability to increase the confidence in the security effectiveness of the services their customers pay for.

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