Project Achievements

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 security measures deployed on network elements, dedicated entities, within infrastructures and parts of services function as expected.

Main focus

Nowadays, open systems such as communication services are massively distributed. They rely on ubiquitous, dynamic and multi-domain communication infrastructures composed of highly connected sets of managed products. Surveys indicate that most often their security fails because the deployed security safeguards (e.g. firewalls, AAA, anti-virus, IPS, vulnerability scanners etc.) are misconfigured or inadequately monitored.

The goal of the operational security assurance evaluation is to provide a continuous assessment that the deployed safeguards comply with the security expectations stated in the security policy and the security risk analysis.

In the first phase of the project (BUGYO, Celtic project number CP2-002), the feasibility was demonstrated to continuously monitor deployed safeguards to gain objective confidence that they meet the security policy.

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

Approach

During the first phase, a six-step methodology was developed for continuous security assurance monitoring of communication services. This methodology relies on a five levels of assurance taxonomy and a security assurance model for static infrastructures.

The challenges in BUGYO Beyond were to enhance this methodology and to dem-

BUGYO_Beyond

Project ID: CP5-003

Start Date: 1 November 2008

Closure date: 1 September 2011

Partners:

Alcatel-Lucent Bell Labs, France

B-Kyung System Co. Ltd, Korea

CASSIDIAN, France

Centre de Recherche Public Henri Tudor, Luxembourg

Innovalia Association, Spain

Itrust consulting, Luxembourg

NetHawk Oyj, Finland

Nextel, S.A.; Spain

Nokia Siemens Networks Oy, Finland

Oppida, France

Télécom ParisTech, France

TeliaSonera, Sweden

Universidad Politécnica de Valencia, Spain

Uphill Oy, Finland

VTT (Technical Research Center), Finland

Co-ordinator:

Samuel Dubus

Alcatel-Lucent Bell Labs, France

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

Project Websites:

www.celticplus.eu/projects/celtic-projects/call5/BUGYO-BEYOND/bugyo-beyond-default.asp

onstrate its applicability for multi-domain, ubiquitous and dynamic communication service infrastructures.

In particular, a modeling abstraction, called "assurance profile", was proposed and developed. It acts as patterns that systems owners may adapt to instantiate easily the security assurance models of their communication services. Furthermore, work on a measurement infrastructure was carried out to address the dynamic collection of base measures required by metrics associated with security assurance models.

The project also focused on the design of a security cockpit that should enable administrators and decision makers to monitor and correct security assurance variations which could lead to breaches using correct priorities and relevant business related indicators.

As security assurance needs to be widely accepted as a realistic source of confidence between third-parties, proposals for standardization were elaborated.

Achieved results

The major achievement of the project was an **Operational Security Assurance Assessment Framework** (OSA-AF) including the necessary assurance models, exchange formats, methodologies and a global architecture to continuously assess the security assurance of modern communication services relying on large-scale, multi-domain and dynamic infrastructures.

The **Assurance Profile** (AP), and its associated methodology, were defined as a structured format allowing a community of experts to establish a common set of assurance measurement needs on an agreed Target of Measurement (ToM) for recurring security design of a communication service. By defining Security Assurance Views (SAVs), several companies in a multi-domain environment might base a security level agreement (SecLA) on commonly accepted security and assurance requirements derived from APs.

Moreover, a standardization of this AP is on going within the ETSI TISPAN Security WG7.

Further achievements were a specification and implementation of a global architecture of an OSA-AF composed of two main modules:

- the secured, resilient and adaptable **Measurement FrameWork** (MFW), based on a combination of multi-agent and overlay network technologies, reliably gathers derived measures from deployed probes over the ToM.
- the **Security Assurance Cockpit** (SAC) manages, assesses and monitors the operational security assurance through different SAVs, so that system administrators, security managers, other SACs, or even end-users may take decisions based on the assurance level of whole or parts of a ToM.

It was demonstrated how the OSA-AF scales to modern network infrastructures by testing it with a communication service composed of several administrative domains, using virtualization technologies to simulate network dynamisms of the underlying infrastructure.

The project consortium achieved to publish a large number of articles and papers in both refereed conferences and journals (e.g. IARIA 2010, CRiSIS 2011), but also invited talks and tutorials (e.g. Enisa summer school 2010, Predict-11).

Impact

BUGYO Beyond results offer a framework to build communication services in which deployed security is more reliable and sustainable along the life-cycle of the service infrastructure, no matter whether it relies on third-party or dynamic infrastructures. By implementing the proposed OSA-AF, service providers can increase the confidence in the security *correctness* and *effectiveness* of the services their customers pay for.

A standardized Assurance Profile should also help security experts' communities to build libraries of security architecture models for operational assurance assessment.

Several partners already engaged exploitations. Alcatel-Lucent enhances its solution lifecycle with concepts and methodologies derived from the Assurance Profile. Cassidian plans to enhance its software solution dedicated to security monitoring with new features derived from BUGYO Beyond such as APs. Nextel is developing an operational security monitoring cockpit based on BUGYO Beyond specifications. Oppida and itrust develop tools to enhance their auditing and pentest process with operational measurements. Other partners, like Nokia Siemens Network and NetHawk, study the exploitation of specific parts of the project results. Several academic partners, like the CRP Henri Tudor, has tailored security assurance concepts and a tool (based on intelligent agents) to suit their current research interest.

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