Functional Composition Security Threats and Requirements

Irfan Simsek[*], Abbas Siddiqui[§], Paul Müller[§], Erwin Rathgeb[*]
[*]Computer Networking Technology Group, University Duisburg-Essen, Germany
{irfan.simsek, erwin.rathgeb}@iem.uni-due.de
[§]Integrated Communication System, University of Kaiserslautern, Germany
{siddiqui, pmueller }@informatik.uni-kl.de

I. MOTIVATION

The current Internet is a packet based network of networks – based on the static layered protocol stack architecture. Protocols acting on the diverse layers specify the entire functionality and operate with each other only in a hierarchic manner. It is hard to introduce or to remove functionality from the static network stacks which results in an inflexible architecture. Furthermore, the current Internet security based on "fix it as you go" - approach results in multiple fragmented and complex solution concepts which are obviously inadequate – from a conceptual as well as from an operational perspective.

The Functional Composition (FC) which can be seen as an abstract concept for the Future Internet architecture splits entire layered functionality in modular and loosely coupled units, so-called Functional Blocks (FB), and composes in a flexible and a dynamic manner the desired functionality based on given application requirements. The FC approach can be applied on diverse operating levels, e.g. Service and Network level. Thus, we can distinguish the FCs acting on different levels from each other: Service level FC, e.g. the Service Oriented Architecture (SOA) [2], and Network FC [3]. In the recent years diverse FC approaches have been proposed, so the security for the FC itself must be considered while implementing a FC approach. Though several security requirements and methods for the Service level FCs, e.g. Web Service Security (WSS) [4] for the SOA Protocol (SOAP), are developed, but the security for the Network FCs is a complete new research area.

In this poster presentation, we discuss possible conventional and architecture-specific attacks against the FC and conceivable security requirements for the FC.

II. FUNCTIONAL COMPOSITION SECURITY

In the diverse FC concepts, we can find several common components operating in a FC Framework – which is important to analyse the possible security threats and requirements. One of such components is the so-called FB Repository where the available FBs are registered by the FB providers. Thus, each FB registered at the Repository must uniquely be described in a well-defined language. Workflow engine is the component for executing a workflow. The Workflow Engine execute the building blocks described in a composed workflow (i.e. workflow is composed by a selection and composition process). Thus, a workflow defines connection among FBs and their execution sequence. In case of a distributed FC, the selection and composition process will be distributed as well as the workflow engine across the frameworks residing on the network nodes. In this case, the Workflow Engine at the node executes only the partial workflow and rest is executed by the workflow engines on other nodes.

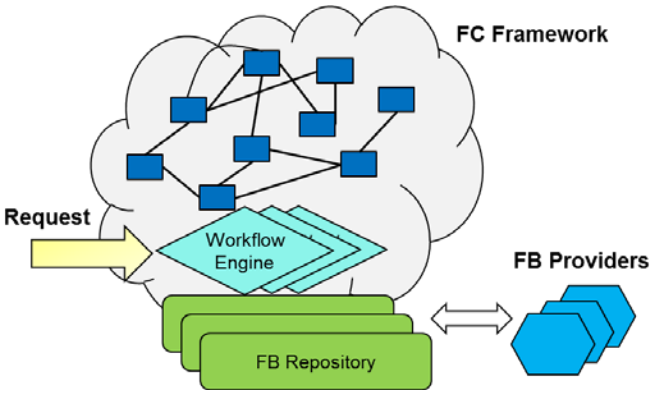

Figure 1. General Functional Composition Concept

A. Possible Security Threats

In the context of the common FC concept, we can specify the following possible threats:

- Against FC availability: By following manners, FC Framework can be attacked so that the requested FC cannot even be built up or the existing FC can be made unavailable for the users.
  - Cutting down the connection between the FB Repository and the Workflow Engine / FB providers.
  - Requesting the same service in a huge amount.
  - Requesting a specific service overloading one or multiple FBs in the FC Framework.
  - Alternating requests for different FCs so that the dynamic of the Framework is overloaded.
  - Infiltrating malicious FBs in the FC. Such as FBs can contain infinitive loops so that the entire FC cannot complete the requested service.

- Interrupting the workflow signalling so that a part of the entire FC cannot be built up.
- Interrupting the communication between the FBs.

- Against FC Integrity and Confidentiality: The goal of such kind of attacks is to sniff the data traffic between FBs or to build up a faulty FC so that the requested service cannot be provided or the user data operated by the FC can be forwarded to a third party.
  - Manipulating workflow during workflow signalling.
  - An attacker can act as a legitimate Workflow Engine.
  - Infiltrating malicious FBs in the FC. Such FBs can produce incorrect results or forward the user data to a third party.

B. Conceivable Security Requirements

While diverse security requirements are specified for the Service level FCs, the security requirements for the Network FCs are rarely analysed. However, the requirements which we specify here are detached from the differentiation of level that the FC operates on, in that the FC on the both levels contains the common concepts. In this context, we can specify the following security requirements for the FC:

- FC common components security: These components can be seen as sensible points in a FC Framework. Therefore, the communication between them must be secure. The communication may not be sniffed, interrupted or manipulated.
- Functional Block security: A FC realising a requested service consists of multiple FBs so that an insecure FB can cause crucial security problems. Thus, the FBs must be authenticated by registering at the Repository. Furthermore, a FB must be verified before it is taken in the FC. In addition, the FBs already acting in the FC must be monitored for anomalies.
- FB Communication security: A secure communication between the FBs acting in a FC keeps the entire operability of the FC together. Therefore, the availability and integrity of the communication between the FBs acting in a FC must be guaranteed. Furthermore, the FBs exchange user specific data which the confidentiality must be ensured for.
- Workflow security: A workflow specifies the processing steps in the entire FC and the connecting the FBs with each other. By a workflow signalling, the workflow must be authenticated before the Workflow Engine builds up the FC according to the received workflow. Furthermore, the security mechanisms must make sure that a workflow is not manipulated during the signalling. In addition, the processing of the entire FC must be monitored to ensure that the FC achieves the requested service.
- Request security: A request control must authenticate and verify the requests and monitor the reaction of the FC for the requests in regarding of overloading cases.

III. OUTLOOK

In this work, we analysed the security threats and requirements for the FC and it represents the first steps in a new giant research area. The next step that we plan is to design FC security mechanisms on the basis of the presented analysis. The security system must be FC-oriented. Thus, the system must keep up with the common FC concepts; flexibility, dynamic, service orientation distributed characteristic.

IV. ACKNOWLEDGEMENTS

This work is funded by the German Federal Ministry of Education and Research within the scope of the G-LAB DEEP [1] project as part of the G-Lab project.

[1] BMBF Funded Project, G-Lab DEEP, [online] (last access 25.05.2012) http://www.g-lab-deep.de

[2] C. M. MacKenzie, K. Laskey, F. McCabe, P. F. Brown, R. Metz, and B. A. Hamilton. Reference Model for Service Oriented Architecture v1.0. OASIS, October 2006.

[3] C. Henke, A. Siddiqui, R. Khondoker. Network Functional Composition: State of the Art, IEEE ATNAC, November 2010.

[4] A. Nadalin, C. Kaler, R. Monzillo, and P. Hallam-Baker. Web Services Security: SOAP Message Security 1.1, OASIS, February 2006