Cloud & SOA
Application Security as a Service

Ulrich Lang
ObjectSecurity
Plug & Play Tech Center
530 University Ave, Palo Alto, CA 94301, USA
St John's Innovation Centre
Cowley Road, Cambridge CB4 0WS, UK
ulrich.lang@objectsecurity.com

Abstract

This paper introduces the concept of moving security and compliance policy automation for Cloud applications and mashups into the Cloud. This way, Cloud applications and mashups can be protected more seamlessly within the Cloud computing paradigm, and the secure software development lifecycle for Cloud applications is improved and simplified. The policy automation aspects covered in this paper include policy configuration, technical policy generation using model-driven security, application authorization management, and incident reporting. Policy configuration is provided as a subscription-based Cloud service to application development tools, and technical policy generation, enforcement and monitoring is embedded into Cloud application development and runtime platforms. OpenPMF Security & Compliance as a Service (“SeaaS”), a reference implementation using ObjectSecurity OpenPMF, is also presented. The paper argues that security and compliance policy management for agile distributed application landscapes such as Cloud mashups needs to be model-driven and automated in order to be agile, manageable, reliable, and scalable.

1 Cloud Computing

Cloud computing can be defined in simple terms as a style of computing where scalable and elastic IT capabilities are provided as a service to multiple customers using internet technologies [Gart09a]. NIST defines and categorizes Cloud computing in more detail (see [MeGr09]) Cloud computing is still a rapidly evolving landscape and there is considerable provider investment and hype around cloud computing, as many business models and ideas are rapidly emerging. It is becoming clearer that not all enterprise computing will move to the Cloud due to various constraints and requirements, but that suitable Cloud services will emerge that will replace the need for a number of in-house IT services. In the consumer world, this trend towards Cloud services is currently complemented by the uptake of thin client devices (e.g. tablets, netbooks, and smartphones). An important Cloud concept is that multiple Cloud services can also be integrated using so-called Cloud mashups. In simplest terms, a mashup is a way to obtain data from multiple sources and combine it in new ways to create a new solution. For example, using a mashup, internal company data of nearly any type can be combined and integrated with Web services, feeds, and just about any other outside information. A Cloud mashup shares many of the char-
acteristics of SOA and web applications, with the exception that Cloud services integrated using mashups are per definition always hosted as a Cloud service. Mashup tools are application and data integration platforms that allow users to create such mashups using numerous data sources and has a graphical user interface used to simplify integration. Cloud computing promises many benefits, including reduced cost, increased storage, high degree of automation, flexibility, mobility, and less need to deal with IT 'plumbing'. As a general rule, it needs to be assessed for each case whether the benefits of Cloud computing are significant enough to outweigh the current shortcomings. There is a general observation that the return on investment grows with increasing scale of the Cloud and decreasing migration time. Also, security and compliance will play a critical role for government Cloud adoption.

2 Cloud Security & Compliance

Security is currently often stated as an inhibitor for Cloud adoption. According to Forrester [Forr10], in Q3/2009, around half of all IT managers in North America and Europe decided against the use of Cloud services due to security concerns. But in general, Cloud computing does not necessarily have to be any more or less secure than most other current environments; as with many new technologies, it creates new opportunities, but also new risks. The Cloud provider argument that security is inherently better because the provider will have more pooled resources and expertise to do security better than the user organization could is as skewed as the argument that Cloud security is inherently unachievable – the truth is probably somewhere in the middle and depends on the particular use case [LaSc10]. The Cloud Security Alliance (CSA) has produced a publication [CSA09] that details various governance and operational aspects of Cloud security, and an alternative categorization can be found in [Gart08a].

A number of general observations can be made related to Cloud security: As far as the responsibilities for security and compliance are concerned, the lower down the stack the Cloud service provider stops (e.g. PaaS or IaaS), the more security is the consumers responsibility. Also, Cloud mashups have significant security implications because information flows and resource usage need to be controlled across logical and geographical boundaries. And multi-tenancy (i.e. several users sharing common resources) implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies. Compliance reporting will also be a necessary Cloud feature.

3 Cloud Application Security & Compliance

Just as with traditional application security, Cloud applications need to be secured. The CSA identified the a number major Cloud application security aspects [CSA09], which are in line with many identified security concerns associated with web apps and SOA [LaSc08a]: In particular, Cloud computing and security affect the complete Software Development Life Cycle (SDLC), for example because the SDLC security must support Cloud application dependencies and agility. Also, Cloud SDLC must support the complex ownership, provisioning and responsibility of tools and services used to develop, test, and manage Cloud applications. Identity and Access Management (IAM) also play an important role for Cloud application security, and includes identity provisioning, authentication, federation, and authorization management. And compliance, which