TRIGENT

Addressing SaaS Security

Padma Krishnan
SaaS Practice Manager

Trigent ■ 2 Willow Street, Suite 201, Southborough, MA 01745 ■ 1-877-387-4436 ■ www.trigent.com

Introduction

This paper identifies some of the best practices and design principles followed by Trigent in developing SaaS applications to address inherent security challenges.

Security continues to be one of the biggest concerns for a SaaS based offering. In this paper we will examine three areas of possible information leakage which are:

- ❑ Saas Vendors
- ❑ SaaS Hosting Providers
- ❑ Co-tenants of the SaaS Applications deployed on the same Image

Information leakage mechanisms in these areas are:

- ❑ Information security with the SaaS vendor and SaaS Hosting Providers. How can unauthorized access to tenant data be prevented?
- ❑ What precautions and prevention practices can be used for protection against other co-tenants of the same application getting accidental access to each others' data due to application errors?

SaaS solution providers need to provide an appropriate security solution model that would help their customers feel confident about their data security, and that these are understood and addressed with the best practices available in the market today. Therefore, this paper will describe general design principles that can be used to best mitigate the data security concerns as applied to SaaS applications.

Security Principles

While there seems to be no silver bullet for solving all the security needs of complex enterprise grade SaaS applications, they require a well thought out interplay of both security architecture and security techniques. When Trigent develops enterprise grade applications, we follow a "Defense in Depth" principle. In short, the "Defense in Depth" principle prescribes building multiple complementary defense levels across the key layers of an application, such as: UI, Business and Data base.

In addition, we compliment this architecture with a wide range of best practice security techniques including physical security access, firewalls, appropriate network access, SSL certificates, two factor authentication, OpenID, etc. It is important to employ the best security techniques at appropriate levels. When done carefully and thoughtfully it will be extremely difficult to compromise your sensitive data either accidentally or on purpose.

In the following sections we describe design principles used by Trigent in development of SaaS applications.

Data Security and Encryption

Data Segregation - The most important principle in a SaaS application is that of data segregation which ensures that each Tenant's data is properly segregated and that no tenant is able to access another tenant's data. This is achieved by developing a filtering layer between the tenant and the data source so that data access via the filtering layer returns only the selected tenant's data. This is done by a enforcing a context based connection to the database, thus ensuring that only authorized data is returned. Such security blocks are implemented at common access points in the database layer and in the business layer ensuring that a tenant's data is always properly segregated.

Data Encryption - Another necessary initiative is encrypting selected sensitive database fields such as SSN, bank account details etc. This is to prevent users like administrators who have access to the database from viewing this sensitive information. We typically encrypt these fields by using a combination of keys or a key and an external random sequence of bits (called a "salt") which is used to further obscure the encrypted data. A commonly used scheme calls for one part of the key for decrypting the sensitive field to be programmed into the application itself, thus making it almost impossible for say, a database administrator to compromise the data. This ensures that data can be decrypted only by an authorized user running the very application itself and not by a database user who gets access to the database otherwise.

Database Encryption

Microsoft SQL Server 2008 provides TDE (Transparent Data Encryption) functionality which does encryption of the underlying data files of the database. Therefore if only the data files get compromised, it is not possible for the intruder to restore the database and access sensitive data. TDE therefore provides the ability to comply with many laws, regulations and guidelines established in various industries. For more information on TDE, please refer http://msdn.microsoft.com/en-us/library/bb934049.aspx.

Dual validation on Client side and Server Side

Applications making use of Java script to perform certain validations are vulnerable to security issues as scripts can be injected to change the behavior of the application. While java scripts are highly preferred for quicker UI response times, they do pose a security risk. Such vulner abilities should be assessed and another validation should be performed on the server side to ensure the correctness of the data.

Obfuscation of code assemblies

Obfuscation using proven techniques is recommended for development in environments such as Microsoft .Net applications. This is necessary so the code assemblies may not be otherwise be reverse engineered thus providing insight into how the application's security works. This also has the additional benefit of protecting the SaaS vendor's IP. An example of such an obfuscator tool is PreEmptive Dotfuscator for the Microsoft .Net platform. should be assessed and another validation should be performed on the server side to ensure the correctness of the data.

Conclusions

New security threats evolve, as SaaS model matures. These practices will also necessarily evolve or change to keep pace with such needs. The above methods are some of the recent practices we have established for developing SaaS applications. It is also important to standardize on many of these practices using reusable libraries or components to speed up such implementations and get reliable, repeatable performance.

About Trigent Software Inc.

Trigent is a privately held, professional IT services company and a Microsoft Gold Partner with its U.S. headquarters in the greater Boston area and its Indian headquarters in Bangalore. We provide consulting services in various technologies including Microsoft Solutions. Our operating model is to conduct sales, customer relationships and front-end consulting (e.g., business case, requirements, architecture) onsite with our clients and perform the detail design, development, integration, testing and quality assurance offshore at our world class development and support center in Bangalore. We are a SEI CMM Level 4 company and is ISO 9001:2000 TickIT certified organization.

For sales contact sales@trigent.com or call 508-490-6000.

CERTIFIED ISO 9001:2008 COMPANY

SOFTWARE 500

Microsoft Partner

Gold	Application Development
Gold	Collaboration and Content
Silver	Mobility