

Managing Security Threat in SaaS: Essential “How To’s”

For Webinar Audio, Dial in:

Conference Line

US: 1 888 436 6494/ 1 866 581 2411 (Toll Free)

UK: 08000518866 (Toll Free)

Audio Conference ID: 22787970

Webinar ID: 259-924-097

Date : Thursday, August 13th, 2009

11:00 AM ET/ 08:00 AM PT/ 04:00 PM BST/ 08:30 PM IST

Panelists:

Alexey Lef

Chief Technical Architect, SciQuest

Jothi Rengarajan

Senior Technical Architect, Aspire Systems

Moderator:

Janaki Jayachandran

Business Manager – SaaS Specialization, Aspire Systems

About Aspire

- Thought leader in Outsourced Product Development
- 1050+ product releases to date
- 80+ customers; 475 producteers
- 63% CAGR over the last six years
- Offices in Chennai (India), San Jose, CA, and London, UK
- ISO 9001:2000 certified

Awards



Ranked in the top 500 fast growing technology companies in Asia Pacific for 3 years in a row

Ranked 7th in Business Today Survey featuring the Best Companies to work for in India in 2005

Housekeeping Instructions

- All phones are set to mute. If you have any questions, please type them in the Chat window located beside the presentation panel.
- We have already received several questions from the registrants, which will be answered by the speakers during the Q & A session.
- We will continue to collect more questions during the session as we receive and will try to answer them during today's session.
- In case if you do not receive answers to your question today, you will certainly receive answers via email shortly.
- Thanks for your participation and enjoy the session!

Panelist



Alexey Lef

Chief Technical Architect, SciQuest

- Alexey has over 20 years of experience in the Software Industry and has played various roles from System administrator, DBA, Programmer and architect
- Ever since 1998, Alexey has been one of the early contributors to SaaS by architecting and designing a successful on-demand procurement and supplier enablement solution for SciQuest.
- He was a System Administrator in IBM before SciQuest taking care of Network security and Database Administration.
- He holds a bachelor of computer science from New York University.

A Hypothetical Case Study

- EMR Anywhere – a fictitious company providing electronic medical records, scheduling, insurance billing and other services for medical offices as a SaaS solution.
- Founder: Bob. Background: Traditional Software Development.

Opportunity

- Doctors find it hard to:
 - Maintain servers in-house
 - Keep track of and maintain compliance with the latest electronic medical record keeping requirements.
- With an online solution, doctors can access patient information from anywhere

The Main Challenge

- Highly sensitive data
- Concerns over patient privacy and the security of medical records
- The question of Trust

Hosting solution

- EMR Anywhere placed their servers at the state-of-the-art data center of a Managed Hosting provider (e.g. Rack Space, Verio, SunGuard)
- Redundant power, UPS, multiple redundant internet connections, 24x7 monitoring, strict access controls
- Latest OS security updates, firewalls, intrusion detection
- Secure offsite backups (e.g. Iron Mountain)

Other Hosting Options

- Use a co-location facility but maintain the servers ourselves
 - Pros: hosting provider doesn't have access to the servers (other than physical access)
 - Cons: need highly skilled employees; not core competency
- Use a "cloud" provider (e.g. Amazon EC2, OpSource, Force.com, Google Apps)
 - Pros: fast startup; scalability; no capital expenditures; focus on core business
 - Cons: reduced flexibility; may be more expensive in some cases; physical location of the data vs. local laws; network latency; provider has access to the servers/data
- A hybrid approach (e.g. use managed hosting + store some data on Amazon S3)

Development & QA

- Data segmentation – one customer can't access another customer's data
- Awareness of common application vulnerabilities (e.g. SQL injection, cross-site scripting)
- Security safeguards at every layer of the application
- Standards-based encryption of sensitive data
- Encryption keys differ in development/test vs. production
- Every new feature has to undergo testing for security vulnerabilities

Security is Not Just Technology

- One day Bob was walking around the office and noticed
 - Passwords attached to screens on Post-It notes
 - Printouts of sensitive documents left at the printer
 - Screens are not locked
- Bob realized that security can't be solved by technology alone
- Social engineering may be a cheaper and easier way to gain unauthorized access
- Security is about people, processes and access control
- Every department will have to play a role in the overall security solution

Access Control

- Keep the number of people with access to customers' data to a minimum
- Developers have no access
- A separate Production Support department pushes code to the production environment and respond to defects and application vulnerabilities affecting customers. Have access to logs for problem determination.

Customer Service Department

- Provides phone and email support to customers
- Helps customers configure the application
- Has some access to customers data through the application interfaces
- Uses strict identity checks when interacting with customers

Internal Network Support Department

- Responsible for internal network security
- Establishes password strength and expiration policies
- Maintains up to date antivirus and anti-malware software
- Works with HR to grant appropriate access to new users / remove access from those who left the company

Remote Access / Working from Home

- On one hand, remote access has clear benefits
 - Quick response to customers' issues
 - Salespeople and remote users in other parts of the country/world
 - More flexible and friendly environment for employees
- On the other hand, a typical home computer may look like this:
 - Boots up right into an admin account with no password
 - Shared by multiple family members
 - Antivirus trial subscription expired a year ago
 - WiFi router with default password and wide-open wifi access
- How to balance convenience and security?

Remote Access / Working from Home

- Bob decides to
 - Provide company laptops to sales people and essential customer service and production support employees
 - Distribute old company laptops (> 3 years old) as they become available exclusively for remote access
 - Remote access is not allowed from personal computers

Sales

- Aware of security concerns and are able to talk intelligently about solutions
- To mitigate the risk of laptops being lost or stolen (In 2006 laptop stolen from Department of Veterans Affairs had unencrypted personal information about millions of veteran and active-duty military personnel)
- Keep sensitive data on laptops to a minimum
- Keep sensitive data encrypted

Professional Services Department

- Implement secure integration with the customer systems
- Implement single sign-on integration (a frequent request from larger customers)
- Educate customers on security and access control
- Partner with local companies to help customers secure and support their local networks

HR Department

- Communicates with Internal Network, Server support and Customer Support department whenever employees are hired or leave to modify access in a timely manner
- Facilitate security-awareness training for new and existing employees

Standards and Certifications

- **ISO/IEC 27001: Information security management systems**
 - 3-stage certification process including tests
- **SAS 70: Processing of Transactions by Service Organizations**
 - Commonly asked for
 - Related to Sarbanes-Oxley Act
 - Type I and type II audits are available
- **PCI-DSS: Payment Card Industry Data Security Standard**
 - Applicable to organizations processing credit/debit card information

How Much is Enough?

- Security costs money, time and effort
- There is no such thing as perfect security
- Factors to take into account
 - Sensitivity of the data
 - Applicable laws (e.g. Sarbanes-Oxley Act)
 - Impact to the customers affected
 - Affect on future sales
 - Value to a potential intruder
- Goals:
 - Build customer's confidence and trust
 - Make it difficult enough for a potential intruder to be not worth the effort

Culture of Security

- Information security awareness has to become a part of the corporate culture
- There is always a conflict between security and something else:
 - Developing more features vs. making sure the application is secure
 - Hiring a security specialist vs. recent college graduate
 - Convenience of working from home vs. security of the office network
 - Security audits and certifications are expensive
- Executive support is essential
 - Without executive support, implementing effective information security in the organization is difficult if not impossible

Resources

- [ISO 27000 Standards](#)
- [Information Security Forum's The Standard of Good Practice](#)
- Social Engineering Fundamentals
 - [Part I: Hacker Tactics](#)
 - [Part II: Combat Strategies](#)

Panelist



Jothi Rengarajan

Senior Technical Architect, Aspire Systems

- Successful in building enterprise SaaS solutions specifically in the fields of SCM, HRM and Education
- Plays a key role in the R&D and development of “**Propel SaaS**” – Aspire’s proprietary infrastructure framework that enables quick development of SaaS solution
- As part of the Aspire’s Advanced Technology Group (ATG), Jothi’s current interests include SaaS, SOA, PaaS and IaaS.

Key Areas in Application Security

- Data Security
- Access Control Security
- Security in Cloud

Data Security

Typical questions SaaS providers face on Data Security

- How is people centric access to the data handled?
- How is data privacy maintained between different clients?
- Is the data encrypted?
- Who has access to the data? How are the employees accessing my data screened and how their access is logged and audited?
- How the backup of data is handled and where is it stored?

Data Security - Storage Architecture

Data Schema	Pros	Cons
<p>Isolated Database Each tenant gets an individual database computing resource</p>	<ul style="list-style-type: none"> • High security • High Performance • Supports different backup policy for each tenant depending on SLA • Supports individual restore of tenant's data 	<ul style="list-style-type: none"> • High maintenance cost and Hardware cost
<p>Shared Database, Isolated Schema Each tenant having access to their own set of tables that are grouped into individual schemas created specifically for the tenant in the same database</p>	<ul style="list-style-type: none"> • High security • Supports different backup policy for each tenants depending on SLA 	<ul style="list-style-type: none"> • Harder to restore tenant's data in the event of a failure where an incomplete recovery is required • Relatively less performance compared to isolated database
<p>Shared Schema, Shared Database A single table includes records from multiple tenants stored in any order</p>	<ul style="list-style-type: none"> • High Scalability • Lower hardware and maintenance cost • Security addressed by good design schemes 	<ul style="list-style-type: none"> • Relatively less performance compared to isolated database • Very hard to have different backup policy for each tenant • Very hard to restore tenant's data in the event of a failure where an incomplete recovery is required

Data Security – Shared Schema Environment

Design scheme for Security in a multi tenant shared schema environment

- Tenant Data Segregation
 - Uses The concept of Fine Grain Access control at row level
 - Enforces that tenants get access only to their data no matter how they happen to log into the database even though multiple tenant's data are sitting in the same table.
 - Need to be controlled at the database level as the tenants can get access to the database for maintenance
 - Eg) Oracle VPD, MSSQL – Tenant Based Views

- Tenant Data Encryption
 - Last gate in data security.
 - Ensures that data will remain secure even if it falls into the wrong hands.
 - Important in situations involving high-value data or privacy concerns.

Data Security - Audit Trails

Audit trails are records showing who has accessed the product and what operations he or she has performed during a given period of time.

What to audit?

- Important events in the database like User Login, Database connection
- Data access and changes

Where to audit?

- Application level auditing
- Database level auditing

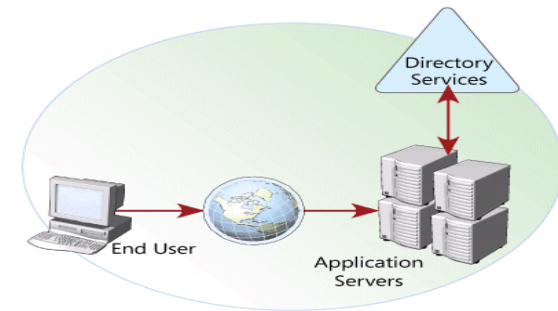
Access Control Security

Typical questions providers face on Access Control Security

- Can you integrate your product with the employee data that sits in my premises?
- Can you provide Single sign on with the other applications that reside in my premise?
- How easy is it to define roles in the system based on our organization structure?
- Can I customize the access control policy based on my need in the product?

Access Control Security - Authentication

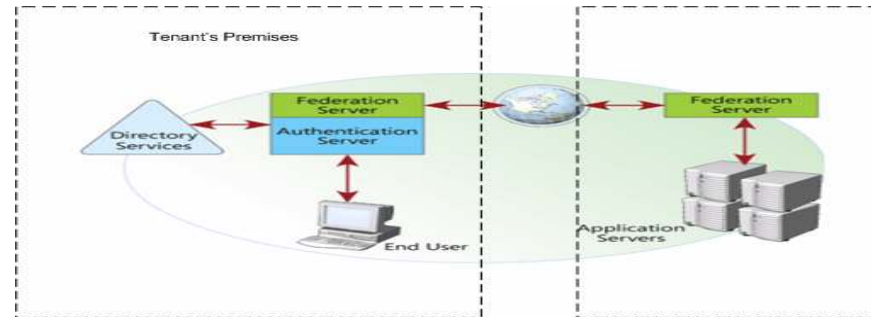
- Authentication
 - Centralized Authentication
 - The provider manages a central user account database that serves all of the application's tenants. Each tenant's administrator is granted permission to create, manage, and delete user accounts for that tenant in the user account directory or database



Access Control Security - Authentication

- Decentralized Authentication

- The tenant deploys a federation service that interfaces with the tenant's own user directory service.

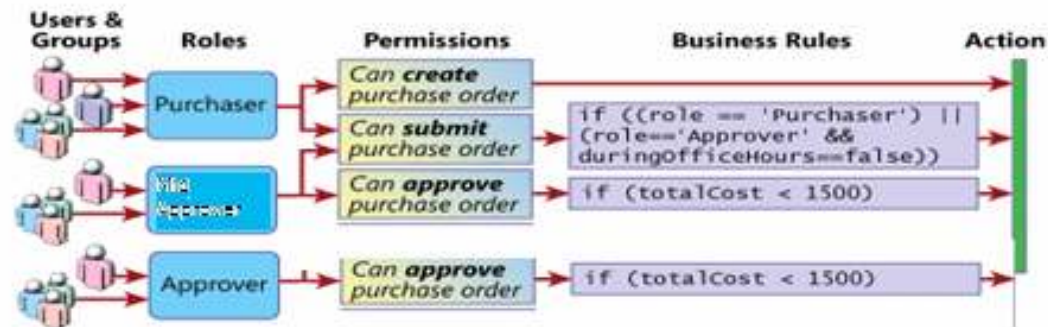


- The federation service authenticates the user locally and issues a security token
- The SaaS provider's authentication system accepts and allows the user to access the application.
- Standards - Saml, WS-Federation
- Central Identity Provider Services – Microsoft passport, OpenID

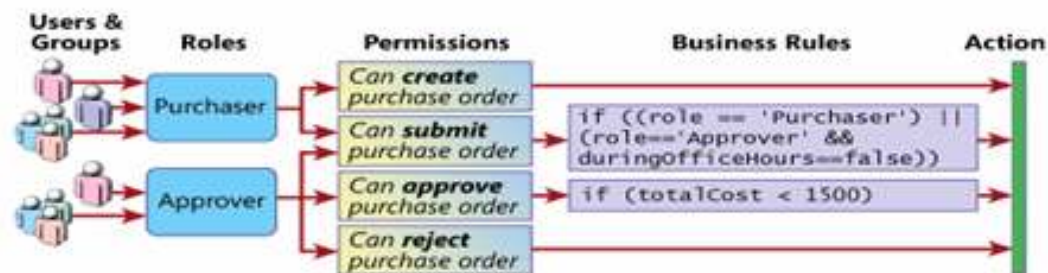
Access Control Security - Authorization

- Authorization : Managing user actions based on user's rights and permissions on a system

Tenant 1



Tenant 2



Cloud Security

Questions to be asked while considering public cloud

- Who is accountable if something goes wrong?
- What's the disaster recovery plan, including response to a pandemic?
- How to comply with Export and Privacy laws?
- What happens if my cloud provider disappears?
- How is the environment monitored for OS / DB / application failures and how are we notified?
- How difficult is it to migrate back to an in-house system? Is it even possible?
- Are there any regulatory requirements on my business that can prevent me from using the cloud?

Considerations for Public Cloud

- Back-up your cloud data periodically
- Secure private keys that are stored in the cloud
- Applications that involve extremely sensitive data, particularly where there is a regulatory or legal risk involved in any disclosure, will require special treatment if they are to be run on a public cloud (get legal advice before committing any applications of this type to public cloud)

Some Useful links

Google's Security Practice

http://www.google.com/a/help/intl/en/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf

Zoho's Security Practice

<https://www.zoho.com/security.html>

Amazon Web Services Security Practice

http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf

For more details



Alexey Lef
Chief Technical Architect
SciQuest
E-mail: alef@sciquest.com
Website: www.sciquest.com

For more details



Jothi Rengarajan
Senior Technical Architect
Aspire Systems

E-mail: jothi.rengarajan@aspiresys.com

Website: www.aspiresys.com

Ph. No: +91-44-67404000

For more details



Janaki Jayachandran
Business Manager – SaaS Specialization
Aspire Systems

E-mail: janaki.jayachandran@aspiresys.com

Website: www.aspiresys.com

Ph. No: +91-44-67404000

Questions?