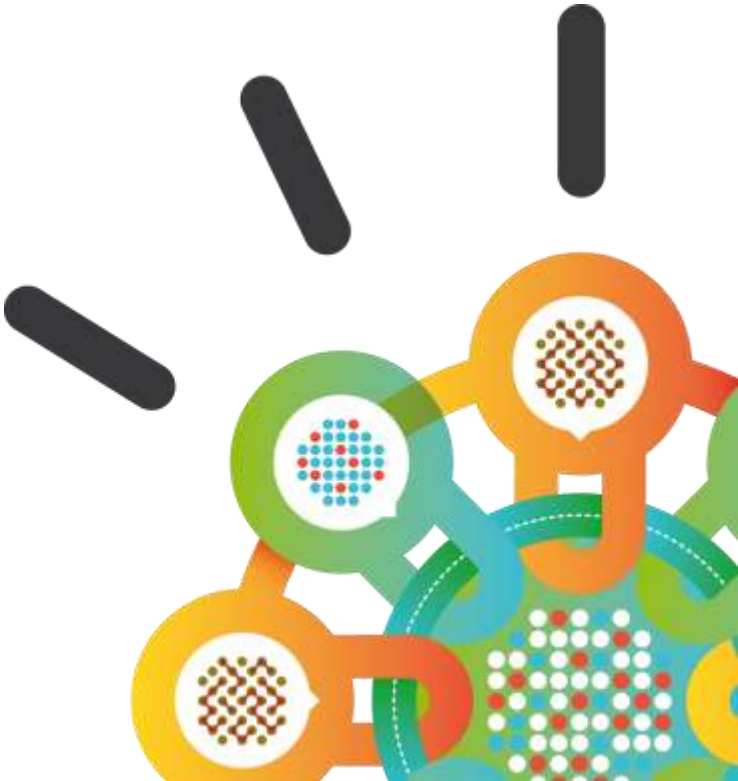
Security Intelligence.
Think Integrated.

Securing applications in the Cloud

Satish Sundar
IBM Security Systems
India Software Lab (ISL)



Agenda

- Software Security Matters – No Matter where the Application Resides
- De-Mystifying the Cloud
- Protecting Data in SaaS Applications
- Developing and Deploying Secure Applications in PaaS

Securing Applications is a Challenge

- Large and diverse application portfolios
- Mobile and cloud applications
- In-house and outsourced development
- External & internal regulatory pressure
- Pockets of security expertise
- Yet another task for developers

De-Mystifying the Cloud

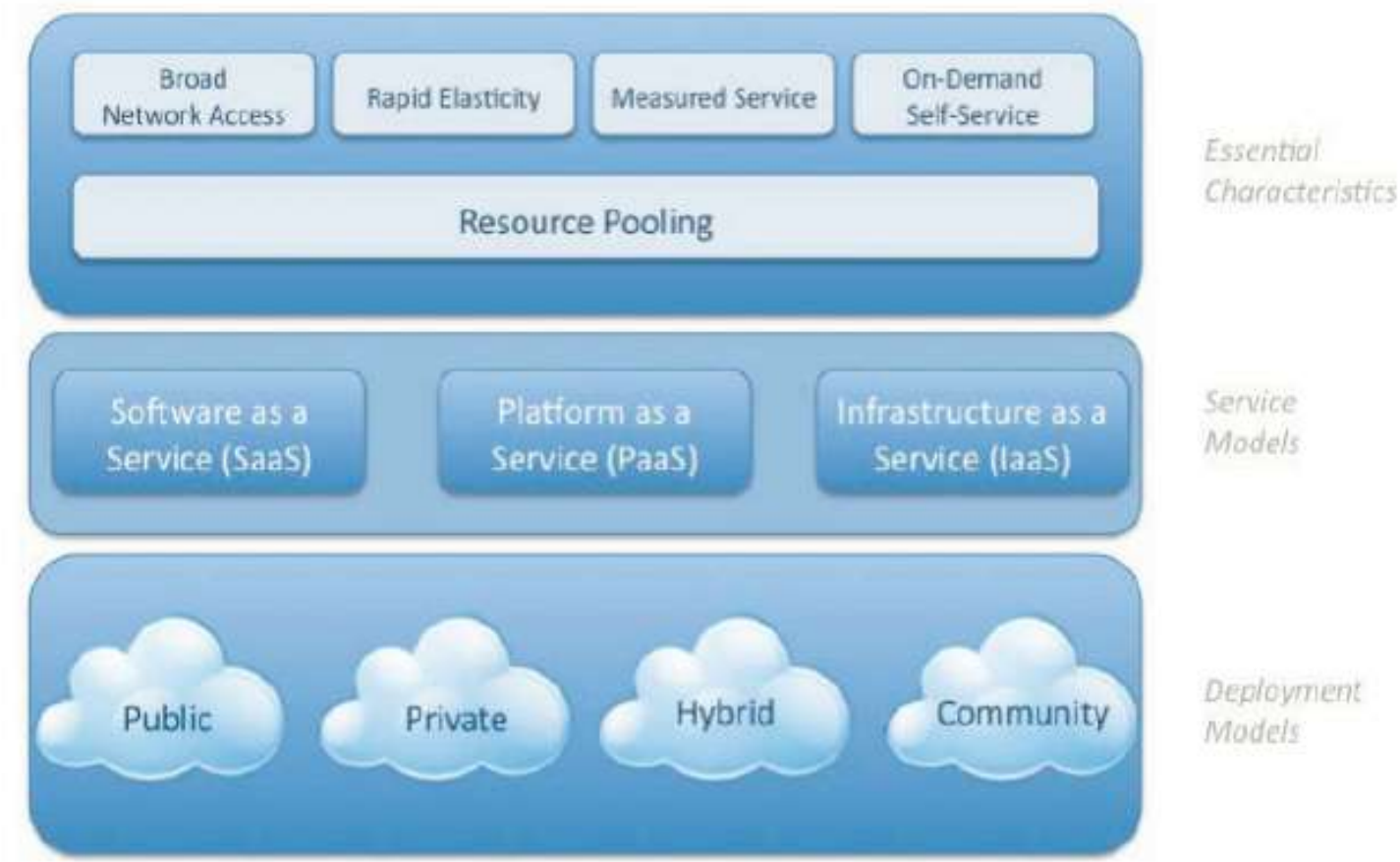
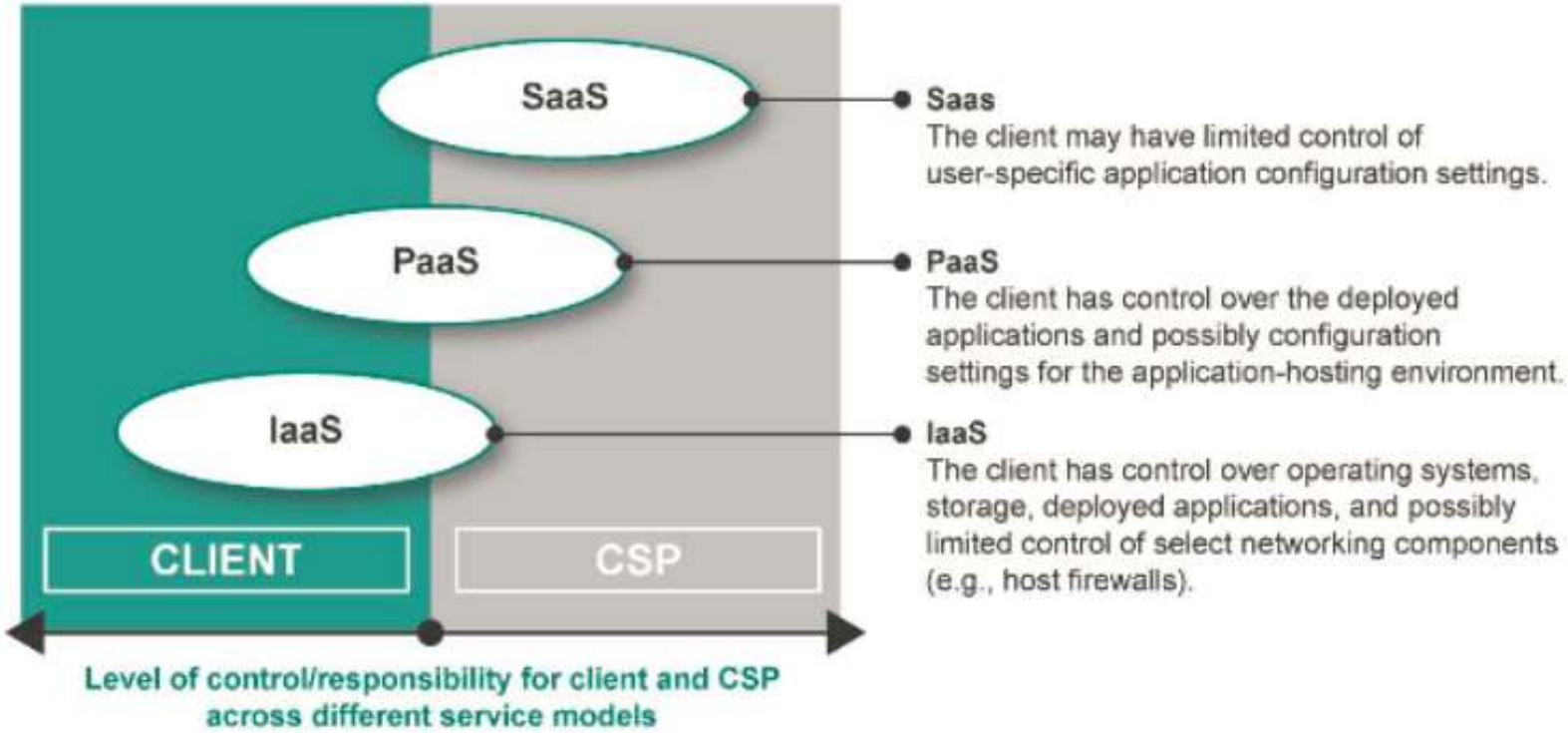


Figure 1—NIST Visual Model of Cloud Computing Definition[2]

Image Source: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
Original data: The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Application Responsibility and the Cloud

Figure 1: Level of control/responsibility for client and CSP across different service models



Source: https://www.pcisecuritystandards.org/pdfs/PCI DSS v2 Cloud Guidelines.pdf

Cloud Control Considerations that Impact Application Security

- Access control
- Access to log files
- Patching and upgrades
- Networking zoning
- Multi-tenancy considerations
- Vetting of administrative staff
- Cost control of utilities
- Upgrades and patching
- Right to audit
- Breach disclosure

Application Security for SaaS

- What are the requirements for an application of this type on premise?
  - Can that be matched or exceeded in the cloud?
  - What security controls has the provider built in?
  - Look at both the applications and the APIs
- At a minimum, confirm with the CSP (cloud service provider)
  - Required application log data and access to the data
  - Authorization and Authentication
  - Vulnerability and patch management
  - Key management
  - Physical access to the data center
  - Breach notification and alerting
  - Escalation path
  - Reporting
  - Right to audit

Build and Deploy? Or Deploy Only?

- Platform as a Service
  - Operating systems, databases, middleware, web servers, tools
  - Testing and deployment support
- Customers can use tools from the PaaS provider for development and services for deployment
- Or use PaaS for deployment only
  - Develop applications in-house
  - Port legacy applications
- Burden of control for implementing application security – shifts to the developer/customer
- Define requirements
  - Authentication
  - Authorization
  - Data protection/encryption

Extend Secure by Design to PaaS Applications

- Build security into your application development process
- Efficiently and effectively address security defects before deployment
- Collaborate effectively between Security and Development
- Don’t forget training
- Provide Management visibility

X-Force Threat Analysis – Software still Isn't Secure

IBM researches and monitors latest threat trends with X-Force

Provides Specific Analysis of:

- Vulnerabilities and exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

Most comprehensive vulnerability database in the world

- Entries date back to the 1990's

Event Name	2012 Rank	Trend	2011 Rank	Trend	2010 Rank	Trend
SQL_Injection	1	Up	1	Up	2	Down
SQL_SSRP_Slammer_Worm	2	Slightly Down	3	Slightly Down	1	Down
PsExec_Service_Accessed	3	Slightly Up			3	Slightly Up
HTTP_GET_DotDot_Data	4	Up	5	Up		
Cross_Site_Scripting	5	Slightly Up	6	Slightly Up		
SNMP_Crack	6	Down	4	Down		
SSH_Brute_Force	7	Slightly Up	7	Slightly Up	4	Slightly Up
HTTP_Unix_Passwords	8	Up	8	Up	8	Slightly Up
Shell_Command_Injection	9	Slightly Up	9	Up		
JavaScript_Shellcode_Detected	10	Up				

Table 1: Top MSS High Volume Signatures and Trend Line - 2012 H1

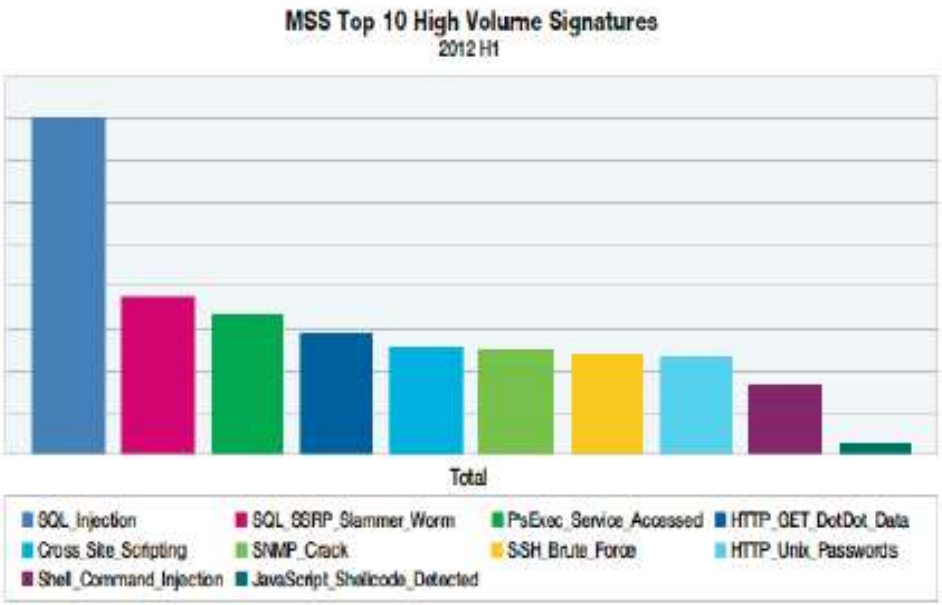
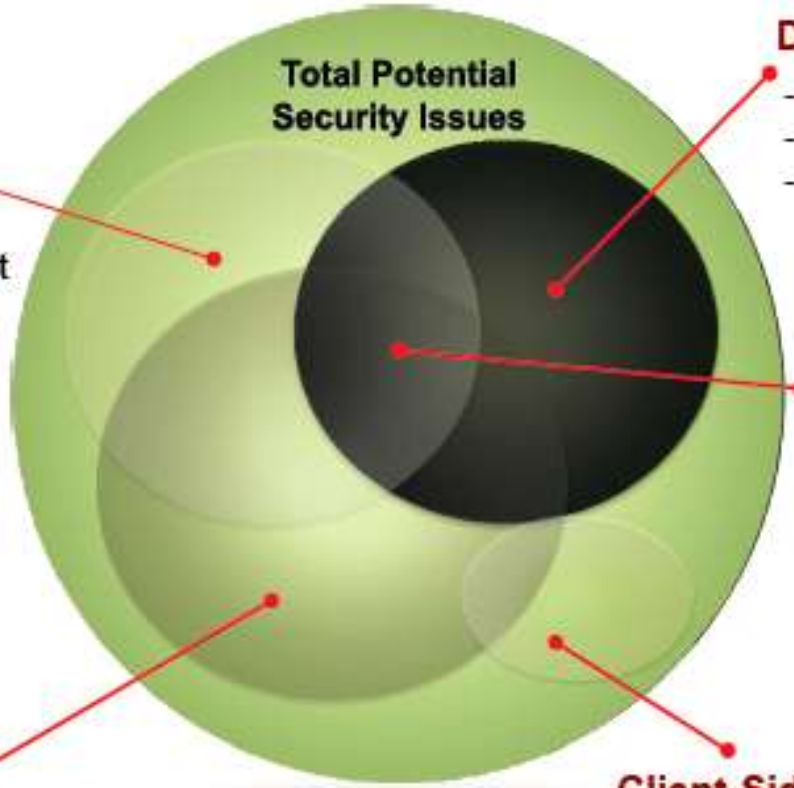


Figure 3: MSS Top 10 High Volume Signatures - 2012 H1

Test Applications before and after deployment



Static Analysis

- Analyze Source Code
- Use during development
- Uses Taint Analysis / Pattern Matching

Dynamic Analysis

- Analyze Live Web Application
- Use during testing
- Uses HTTP tampering

Hybrid Analysis

- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

Run-Time Analysis

- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

Client-Side Analysis

- Analyze downloaded Javascript code which runs in client
- Unique in the industry

Differences between SAST and DAST approaches

	Static Analysis (White Box testing)	Dynamic Analysis (Black Box testing)
Scan input	Scans source code and bytecode for security and quality issues. Requires access to source or bytecode	Scans running web applications. Requires starting point URL, and login credentials where relevant
Assessment techniques	Uses "taint analysis" and pattern matching techniques to locate issues	Tampering of HTTP messages to locate application and infrastructure layer issues
Role in application development lifecycle	**Development:** Scan code and work remediation from IDE **Build:** Scan nightly or weekly build to highlight defects for developers to correct **Security:** Define & customize security best practices for developers; Execute pre-production scans and audits	**Build:** Scan as part of build acceptance tests before releasing build to testing team **Test:** Execute security test scripts as part of quality plan **Security:** Define test scripts for quality plan; Execute pre-production scans and audits
Results & Output	Results are presented by line of code, source to sink functions flow	Results are presented as HTTP messages (exploit requests)

Summary

- Application security in the cloud requires a layered approach
  - Test, Assure, Protect
- Control for application security shifts depending on the model
  - Either way, organization must define application security requirements
- Less control with SaaS, CSP has a higher burden
  - Get it in writing from the provider
- More control with PaaS, CSP has a lower burden
  - Follow secure design processes

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

ibm.com/security